Enterasys Converged Networks

Deploying, Optimizing, and Securing a Network for Unified Communications

Table of Contents

enterasys® Secure Networks™

Enterasys Secure Convergence

Executive Summary

Deployments of converged voice/video/data communications are increasing as new applications support interactive business communications anytime, anywhere over wired and wireless networks. This white paper explains the Enterasys open-architecture, standards-based approach to supporting any convergence application from any vendor. New applications and business efficiency through unified communications are the primary drivers behind deploying converged networks today. Enterasys® Secure Networks™ solutions for convergence enable your organization to answer the following questions in a way that is practical, achievable, and delivers rapid time to value:

- Can the network meet the availability expectations for voice, video and data services?
- Are there ways to architect for reliability and automatically prevent problems?
- Does the network support open-architecture, multi-vendor interoperability?
- Is the network performance suitable for all converged communications requirements?
- Is the network intelligent enough to discover, classify and prioritize separate application traffic with easy-to-deploy, effective QoS?
- Are there enough physical ports with power-over-Ethernet capabilities to which new convergence devices, such as IP phones and security cameras, can attach?
- If a phone, camera and desktop are all connected off of a single switch port – can the voice, video and data traffic be secured and prioritized separately?
- Is the network secure enough to automatically protect the confidentiality, integrity and availability of the convergence application content?
- Is there management software to deliver a simple operational model for prioritizing and securing business-critical converged services end-to-end across multiple locations?

Let us show you how our connectivity, security and management solutions for the access, distribution and core layers of your network enable you to easily and effectively deploy convergence applications and avoid being locked in to a single vendor approach. Enterprises around the world rely on their Enterasys networks to support IP telephony and video solutions from 3Com, Alcatel, Asterisk, Avaya, Cisco, LifSize, Mitel, NEC (Sphere), Nortel, Panasonic, Polycom, Shoretel, Siemens, Tandberg, and others. Schedule a time to see how our unique approach to simplifying the deployment, operation, and securing of *any* convergence application from any vendor while leveraging your existing investments. Call us at 877-801-7082 in North America, +1-978-684-1000 worldwide, or visit www.enterasys.com/demo.

Introduction

This paper addresses challenges IT organization face when designing, implementing and operating a converged network and proposes a unique architectural approach to meeting the performance, availability and security requirements of a network infrastructure that supports converged and unified communications.

Today's Ethernet-based IP networks are the principle framework for the vast majority of companies' critical communications. Application data, textual communications and information retrieval have all become fundamental requirements of an enterprise network. Now, IT organizations are looking to the same workhorse network to deliver a number of additional business-critical services that have historically been delivered through separate infrastructures.

It is important to understand why you may move toward a converged network and the benefits and challenges associated with this significant undertaking. The convergence of voice services, video services and data services has historically been positioned as a method for significant cost and resource savings. But recent evaluation of organizations that have embarked on convergence projects clearly show that while some expected cost savings have been achieved —the main driver has shifted to business process efficiency improvements. Advances in application technology have led IT organizations down a converged network road designed to enhance interaction with stakeholders and significantly improve access to information and collaboration with customers, partners and employees.

According to a recent survey by IDC and InfoWorld, there are a variety of applications driving future investments in a company's data and telephony network budget. There are clear indications that many of these applications will rely on a single, converged infrastructure to deliver critical business services. More than half (52.3%) of the respondents indicated that unified messaging will drive future investment, and videoconferencing (36.9%), dual-mode (WLAN/mobile) phones (35.7%), and audio services (24.2%) are all applications that will be delivered through the single, converged Ethernet / IP network infrastructure.

But along with this sharing of the common Ethernet / IP network for these critical services, comes a new set of requirements for the IT organization. Traditional metrics for network performance and capacity may be completely inadequate for the converged network. Network service assurance (which may be perfectly adequate for traditional data communications) may not reflect the needs of unified voice, video and data communications. Security requirements of the converged network may also require additional technology deployments.

The Benefits and Challenges of the Converged Network

There has been much industry discussion about the benefits of deploying a converged network infrastructure. New application technology is driving significant IT requirements to support business process improvements. Business solutions are increasingly taking advantage of the possibilities of integrating data, voice and video services to deliver more robust capabilities. Consider the advances in instant messaging applications and how it is used to enhance employee communication and collaboration. Web-enabled call centers can keep a company closer to its customers enabling faster, more effective response to their needs. Ask any corporate end user what applications would likely have the biggest impact on improving their job function. More often than not the answer will be an application enabled by the integration of data, voice and video. While deploying a converged network infrastructure may not deliver immediate cost savings, the long-term effects of converging multiple, distinct networks into one should maximize the effectiveness of technical support resources and reduce long-term infrastructure build-out costs.

But what are the challenges associated with converging traditionally separate, as well as new and evolving applications, onto the same IP infrastructure? Ask yourself these questions:

- Was the infrastructure architected with high-availability in mind?
- Will it provide the level of availability that end users are accustomed to with services such as the traditional voice network or the traditional broadband television system?
- How many and what type of applications will now be sharing the same underlying infrastructure and data center services?
- Will the network support every application's performance, quality and accessibility requirements?
- Is the network secure enough to ensure the safe and consistent transport of converged application traffic?
- Is the network open enough to support future converged applications from any vendor?

The bottom line is that the availability, performance and security characteristics designed into traditional data networks may not be well suited for the converged network; and proprietary technologies that may be deployed in the data network today can inhibit the ability to deploy voice, video and other converged applications important to the business.

Ultimately, any business can benefit greatly from a convergence solution. Business processes and efficiencies can be improved and long-term total cost of ownership can be reduced. But in order to ensure the solution is a benefit and not a burden, new requirements of the common network infrastructure must be considered, and appropriate technology must be implemented.

Meeting the Demands of a Converged Network

In order to ensure an effective implementation of a converged network solution there are several requirements that should be met.

A well-architected solution for a converged network will support the variety of services that will share the single communications infrastructure. It is also important to build an **open architecture**. The network infrastructure should be able to provide the required performance, availability and security to support *any application from any vendor*. If the network only supports (or more significantly supports) a single vendor's IP phones or video application, it is a poorly designed convergence solution. Good networks are flexible and adaptable to be able to meet the company's current and future needs. As new business applications become increasingly important, the well-architected network will adapt to support them. When looking at voice and video services running over the converged IP network,

Requirements

- Open architecture – support of any convergence application
- Network infrastructure capacity
- Highly available network communications path
- Security of application services
- Application traffic detection / classification
- End-system detection / classification
- Network access control
- Enforceable quality of service

they should be viewed simply as additional IP-based applications which the network must support. Every application has its individual needs, but when running applications on a converged network, it is important that there are no proprietary dependencies between the applications and the communications network. A recent report from Gartner (ID Number: G00136673) supports this concept by stating: *"As voice is an application, the selection of a voice vendor should be independent from the selection of a network infrastructure vendor."* An open approach to deploying a secure converged network enables a company to select any voice or video application from any vendor and run it effectively and efficiently. This ensures the company can implement the best applications or solutions to meet its business needs without having to factor in network infrastructure dependencies - and potential indirect costs.

The **infrastructure capacity** requirements are likely to be very different in a converged network than a data-only network. Think about the different types of end systems and the numbers of these systems that could connect to a converged network - IP phones, IP cameras, facilities access systems (badge readers). Even devices such as Internet TV systems, vending machines and self-service cafeterias significantly increase the number of Ethernet ports that the infrastructure must contain. In addition to the need to resize the capacity of the network access layer, increased bandwidth requirements from all of these additional end systems and related applications may require upgrading the uplinks to the distribution layer and the network core. Bandwidth to the data center may also need to be increased to support new application services. Think about how much additional bandwidth may be required in the data center to support a streaming video business service. Some converged end points also are able to gain power from the network infrastructure itself without relying on the building electrical supply. The best example of this is an IP phone or video camera gaining network communications and power over the same Ethernet cable. For the network to support the IEEE 802.3af Power-over-Ethernet (PoE) standard, additional Ethernet switches with this capability may be required in the converged network. Additional power requirements in the wiring closets also may be needed to support PoE implementations.

Providing a **highly available network communications path** is critical to ensuring that mission-critical services meet end-user usage and availability expectations. Think about how the typical end user feels about the availability of telephony services using a traditional PBX-based system. If you asked the end user how often they did not hear a dial tone when they picked up the phone, they would say "almost never." End users have preconceived opinions about the expected availability of certain applications and services. Even if end users accept that there sometimes will be availability issues with business data applications, it does not mean they would accept the same from a voice or video service now running on the converged network. IT organizations must ensure that the network infrastructure to be leveraged as the converged network can meet the most stringent availability requirements of the individual applications. All aspects of network redundancy and resiliency must be carefully reviewed to ensure that faults and failures will not cause a loss of service to the end user. Proper use of Layer 2 and Layer 3 high-availability protocols can create an infrastructure that can survive major faults and still allow users to communicate with their required services. Intelligence within network infrastructure devices enables dynamic topology reconfiguration and rerouting of communication flows to maintain service availability.

It is critical to **secure application services** in a converged network. Once an application service such as voice is deployed in the converged network, there will be centralized services attached to the network (typically in the data center). Application servers such as soft PBXs, messaging servers, voice/fax gateways, video servers, etc. must be tightly secured against attack and misuse. Since these application services are now housed on servers attached to the IP network, they are potential targets of attack and are also potentially vulnerable to collateral impact from other undesirable activity on the network. If, for example, a video conferencing gateway service application is circumvented in the converged network, the company might lose significant training, messaging and collaboration capabilities. Traditional services such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) become increasingly important in a converged environment. If convergence endpoints need dynamic IP addresses and name services, the servers hosting these services must be highly available and protected against compromise. IT organizations must leverage the network infrastructure and specific security applications to protect all critical application services. Network communication policies must be enforceable where the application servers attach to the network to ensure the filtering of undesirable traffic. Appropriate intrusion prevention and behavioral analysis technologies must be implemented to detect both malicious and non-malicious attacks on critical application servers. A well-architected solution should automatically react to dangerous or threatening behavior targeting a critical applications server, and contain the threat quickly and effectively to ensure service integrity.

Application traffic detection / classification are important capabilities to ensure the appropriate operation of critical business applications. In a converged network environment, many distinct applications rely on the network. Each application has its own importance to the business. A voice call on the converged network might be more important to the business than a corporate video-cast, which in turn may be more important than a user viewing an external website. To establish communication policies for individual applications, it is necessary to identify the traffic associated with a particular application. The converged network infrastructure must be able to detect a specific flow of traffic and classify the traffic as belonging to a particular application. Once traffic flows are classified, security and quality of service policies can be enforced to ensure the associated application will function properly and be secure. Detecting and classifying individual application traffic in the network enables a very granular approach to enforcing priority and security to the individual business services running on the converged network.

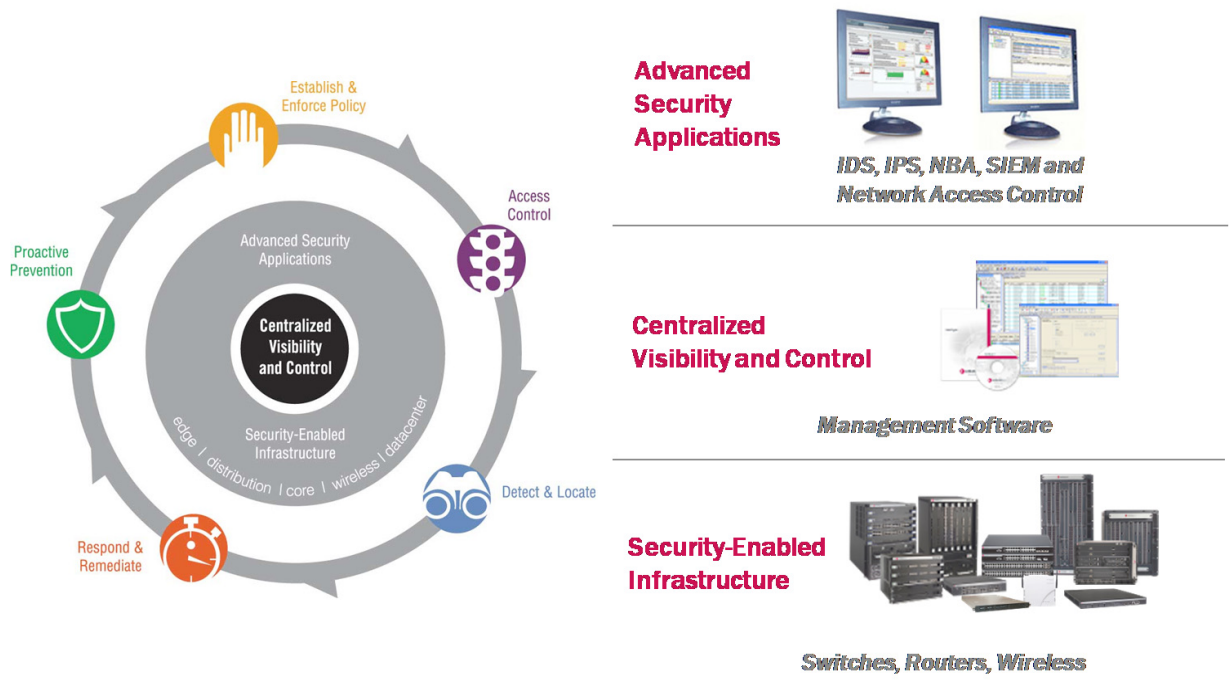
Having **end-system detection / classification** is a critical capability for identifying what types of devices are connecting to the network. Understanding the difference between end systems allows for communication policies that are specific to the device to be enforced. For example, the communication allowed to and from a typical laptop might be very different than the communication allowed to and from an IP-based surveillance camera. A solution that recognizes the differences between end systems attaching to the network is essential to ensuring appropriate services are available to the users and systems that need them. The converged network infrastructure must recognize when an end system attempts to connect and then use various technologies to automatically determine the type of device that is connecting. Device authentication, standard and vendor-specific discovery protocols, and even snooping initial communications should all be used to help determine the type of end system attaching to the network.

Providing **access control** for all end systems is an important component of securing the network environment and also for authorizing appropriate services. In a converged network environment it is important not only to control access to the network infrastructure, but also to control access to services on that network. An IP phone or IP camera should be authenticated to communicate on the network just as a user on a PC should be authenticated. Once an end system is authenticated and allowed to communicate on the network, access to required applications and services should be controlled based on criteria such as type of device, user credentials, organizational role, location, and time of day. The infrastructure devices to which end systems connect must be able to challenge an end system when it first attempts to connect. Several methods of authentication challenge should be available to support both human-centric and machine-centric end systems. The converged network infrastructure must restrict access to services based upon end-system identity. Network communication rules must be enforceable at the end system's point of entry, allowing it to communicate with the services it should be able to access, but restricting communication with services it should not be allowed to access.

Enforceable Quality of Service (QoS) is an important requirement for certain applications in a converged network environment. Consider the prioritization and bandwidth requirements to support voice or video services on a converged network infrastructure. If signaling between the IP phone and the call manager or gateway is affected by packet loss or simply delayed due to network congestion, a user might not get dial tone when they pick up their handset or open their soft phone interface. If the required bandwidth is not available to support a video stream, a user may experience choppy or complete loss of a video playing on their computer. QoS parameters must be enforceable at the point of entry of an end system, and then throughout the network between the end system and the service. Granular enforcement is important to ensure appropriate quality of service parameters for different services being utilized by a single end system. The converged network infrastructure must be able to recognize packets associated with a particular application, and prioritize those packets appropriately to support the requirements of the specific application service. In addition to prioritizing the traffic at the point it enters the network from the end system, the infrastructure device must be able to tag the specific traffic to prioritize communication with the service throughout the entire path of the network from end system to application server. Bandwidth usage must be controllable based on traffic type. The ability to restrict the amount of bandwidth used by any specific application on the network ensures that business-critical applications will have sufficient bandwidth to provide service.

An Architectural Approach

Enterasys provides an architectural approach to deploying, optimizing and securing a converged network. Unlike other vendors' approaches, Enterasys fully integrates a security-enabled infrastructure, advanced security applications and centralized visibility and control to enable IT organizations to very easily deploy networks that will adapt to any converged application and will provide secured and highly available services to business users.



This architectural approach to delivering optimized and secure converged networks delivers significant capabilities. The architecture enables network usage **policies** for users and devices to be **established** centrally and **enforced** throughout the converged network environment. These policies for network communication enable an IT organization to easily ensure the quality of service (QoS) needed for convergence applications, and also ensures secure access for all business-critical services in the converged network environment. Service quality and security policies can be applied to communication from any convergence endpoint from any vendor.

The architecture will enforce **access control** of users and devices attempting to communicate to specific service on the converged network. Each end systems can be detected and identified when they connect to the converged network. Once an end system is identified, access to the network as well as to specific services required can be controlled based on the type of end system, the organizational role of the end system and/or the person who may be using it, the location of the connection, the time of day, and other criteria important to the business. This allows convergence endpoints (IP phones, IP cameras, etc.) to be identified when they show up in the converged network, and their communication on the network controlled to ensure the appropriate QoS levels and security to deliver reliable and robust services.

The architecture will **detect** threats, anomalies, and other relevant events anywhere on the converged network and locate the exact source. Because of the increased business importance of a converged network infrastructure, it is critical that events which could threaten critical services are detected and contained in real-time. Enterasys leverages patented technology to deliver a unique capability of detecting network security, quality, and reliability problems as they occur and isolating the exact source of the problem. In a network of thousands of end systems and convergence endpoints, the exact source of a threat or network problem can be determined in just seconds through the use of intelligent and automated systems.

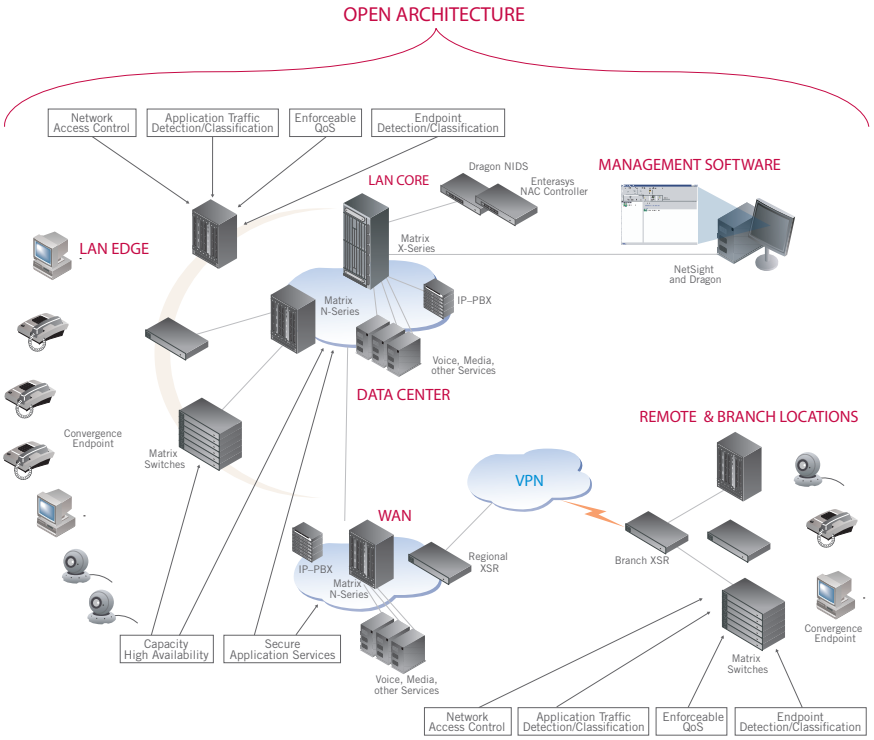
The architecture will **respond** to any threat to critical services with specific and measured action and will enable users to self-**remediate** when appropriate. The architecture's ability to locate the exact source of a threat to the environment enables an appropriate response to be taken. The response might vary based on the type of threat, or the source end system's type, location, user, etc. The Enterasys solution allows for measured response options including disabling a port, changing a VLAN, enforcing a specific set of communication policy rules, notification, and quarantine. In cases where the problem being addressed involves a user, the architecture allows for the enforcement of specific policy rules to completely protect all critical network services, but still enable the user to self-remediate so they can quickly start working productively.

The architecture will **proactively** protect the converged network from vulnerable and dangerous end-systems, preventing them from compromising critical business services, other users and end systems. Defenses are established to protect the environment from known threats and network misuse. In addition, end-systems of all types (including convergence endpoints such as IP phones and cameras) can be identified, located, and assessed for vulnerability and threat posture before they are allowed to communicate on the network. Because dangerous worms and viruses can infect and be spread by many different types of end systems, it is crucial that the architecture be able to proactively protect the converged network environment from any dangerous end systems infected with malware.

With the advantage of the architectural approach to a converged network, IT organizations can easily deploy an Enterasys solution to optimize and secure voice/video/data communications to align the network with the needs of the business.

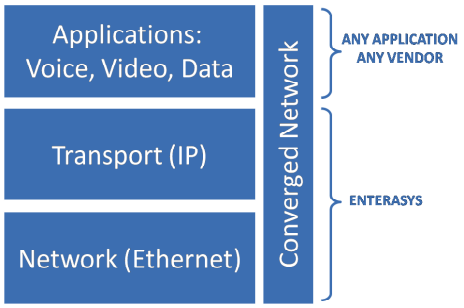
Enterasys Solution Principles

An Enterasys solution for convergence delivers all of the critical requirements to ensure business continuity and efficient operations. Key technologies are leveraged to provide a highly available, secure and application-focused communications environment that can deliver all of the converged services necessary to support the next-generation business environment. The following diagram represents the scalability and comprehensive nature of an Enterasys solution for a converged network.



Open Architecture

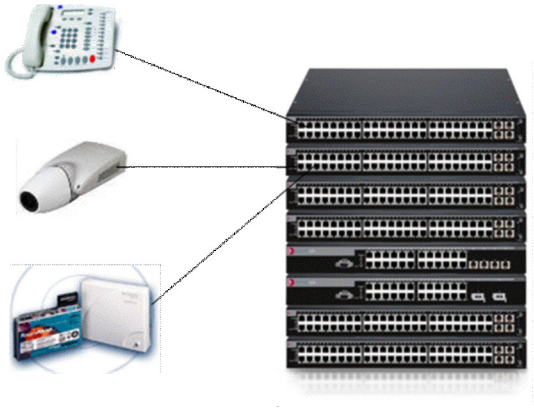
Leveraging Enterasys' long-standing commitment to standards-based technologies and open-architected systems, a converged network can be deployed that will work with any convergence application from any vendor. An Enterasys solution can identify and control convergence applications such as voice and video running on the network and ensure they are secured and prioritized based on the business requirements. This is accomplished through the use of packet classifiers embedded in the infrastructure hardware that can differentiate traffic using Layer 2, 3 and 4 attributes (from the industry standard OSI model). Specific convergence applications can be controlled through hardware-based priority queuing right at the point of entry to the converged network and also with industry-standard packet tagging such as IEEE 802.1Q, 802.1p and RFC 1349 Type of Service (TOS). An Enterasys solution can recognize and enforce communication policies against convergence endpoints from leading vendors. Leveraging the IEEE 802.1X authentication protocol, MAC-based authentication technology, standards-based convergence endpoint discovery protocols such as Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED), and several vendor-specific discovery protocols, an Enterasys solution can detect, authenticate and control access to any convergence endpoint.



This open architecture enables organizations to deploy the right business application at the right time, for the right reasons. There is no dependency in the network architecture restricting the converged applications that can be deployed.

Infrastructure Capacity

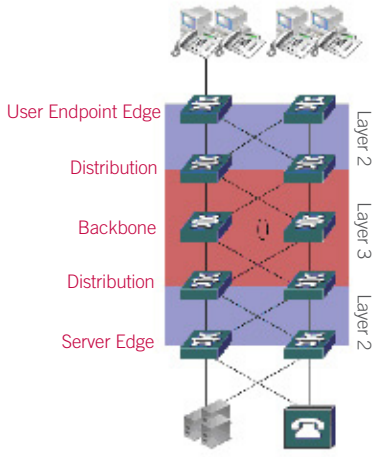
Enterasys infrastructure products are well positioned to scale to the capacity needs of the modern and future converged network. Leveraging the modularity of Enterasys Matrix® N-Series flow-based switches, additional port density can be added quickly and seamlessly where it's needed to support convergence endpoints. The Enterasys SecureStack™ family of switches offers a stackable design so additional ports can be added simply by expanding the stack. The modularity and variety of uplink technology in Enterasys switches for the access layer, distribution layer and network core allow for bandwidth to be increased where required, without major overhauls to the network infrastructure. Enterasys also offers the unique ability to gather real-time capacity-planning information from the network infrastructure. Using the Enterasys application NetSight Inventory Manager, reports show the used and unused ports in a network providing the network administrator with a clear view of the current infrastructure's ability to accommodate additional convergence endpoints.



To provide power to convergence endpoints through the network infrastructure, Enterasys offers standards-based 802.3af Power-over-Ethernet (PoE) technology in its Matrix and SecureStack lines of network switches.

High Availability

In a converged network, availability of services is absolutely critical. As additional mission-critical applications are converged onto a single infrastructure, the fault tolerance and resiliency of the network become increasingly important. Converged networks should be designed according to the principals of the traditional hierarchical network model. Most campus networks can be segmented into three tiers, although smaller environments may be composed of two. Each tier is configured to handle specific services within the environment. Users and end systems, including converged endpoint devices, are attached to the network at the edge tier. Edge-tier switches are connected to the campus by distribution-tier switches. Distribution-tier switches are connected to the campus backbone-tier switches. Server systems and other systems that provide application services such as IP telephony gateways and IP Video controllers connect to the campus through an edge tier specifically deployed to support these systems. A server edge tier generally will not provide user connectivity.



Switches that comprise the edge tier are generally configured as Layer 2 forwarding devices. Layer 2 topology protocols such as IEEE 802.1w, 802.1s and 802.3ad are essential to provide rapid recovery in the event of the failure of a link or a fault in the network components. Enterasys Matrix and SecureStack edge switches support these critical topology standards as well as additional high-availability features such as link flap detection, SpanGuard and backup root bridge to ensure rapid recovery of the network topology in the event of a fault.

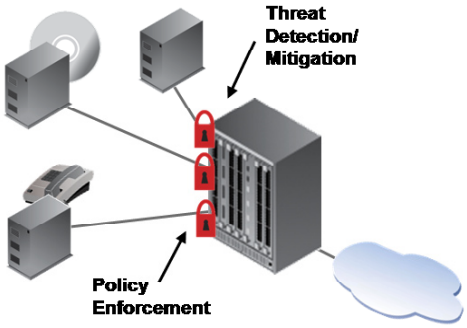
The distribution-tier switches should be configured to route to the backbone and isolate each Layer 2 domain. Distribution switches should support the same Layer 2 redundancy and fault tolerant

functionality as the edge switch, and also support Layer 3 redundancy protocols to interact with the routed backbone tier. Enterasys Matrix distribution switches support Layer 3 redundancy protocols such as Open Shortest Path First (OSPF) and Virtual Router Redundancy Protocol (VRRP) to ensure highly redundant network design.

The backbone tier interconnects large segments in the campus network. Backbone switches should be configured to operate as Layer 3 routers and will connect to distribution switches. The backbone tier should support redundancy and fault tolerance through standard protocols such as OSPF and VRRP. The Enterasys Matrix X secure core switch/router is an advanced next-generation core platform supporting critical redundancy and high availability features including Layer 3 redundancy protocols.

Secure Application Services

In a converged network there will likely be servers hosting specific applications that support the converged service. It is critical that these servers are fully protected from attack and misuse. If, for example, a call manager application or a voice gateway is attached to the converged network infrastructure, it must be secure and available in order for users to have telephone service. If these application servers are compromised or impacted by a denial-of-service attack, there is widespread loss of an essential business service.



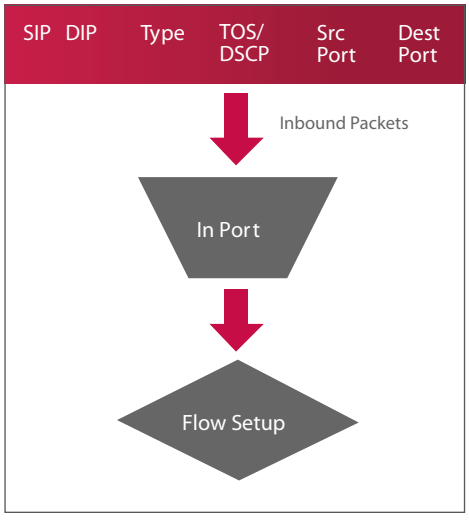
Enterasys policy-enabled Matrix and SecureStack switches and NetSight Policy Manager software protect application servers from attack or compromise by establishing and enforcing security policies that prevent extraneous and undesirable communication to and from the application server. Policy rules also can be configured to prevent the spoofing of critical servers' IP addresses. This ensures that essential application servers cannot be hijacked and the integrity of the converged application service is maintained. This use of an advanced policy framework protects against the misuse of converged business services. Security camera video cannot be intercepted or copied; voice call eavesdropping is not possible; unauthorized devices cannot attach to the network and access critical services. Additional protection of critical services such as DHCP and DNS can be established through policy rules. A policy profile can be enforced at all points of the network to ensure no rogue DHCP or DNS server is allowed to communicate on the network and that the connection points of valid servers are protected against unexpected traffic patterns.

Outbound rate shapers can be configured on Enterasys switch ports as part of the specific policy profile for critical application servers. This will ensure that services such as call managers cannot be overloaded by either malicious attack or a collateral effect from a network anomaly.

In addition to enforcing security policies on the switch ports where critical convergence application servers attach to the network, Enterasys Dragon® Distributed Intrusion Prevention uses host-based sensors residing on the critical convergence application servers to detect attacks and other security events in real time. Once a sensor residing on an application server detects a security event, Enterasys NetSight® Automated Security Manager software can eliminate the traffic associated with the threat, locate the exact source of the attack and take corrective action right at the source port in the network.

Application Traffic Detection/Classification

In order to enforce granular communication policy rules for critical application usage, the ability to detect and classify individual application traffic on the converged network is vital. An Enterasys solution provides advanced capabilities for dynamically identifying application traffic as it appears on the converged network, and classifying the traffic based upon the service type and the criticality to the business.



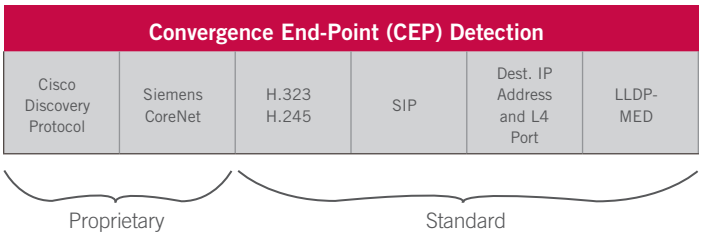
Packets entering Enterasys switches are analyzed and classified as a traffic flow based on a set of variables:

- Source IP address
- Destination IP address
- IP type
- TOS field / DiffServ code point
- Source port
- Destination port

These variables enable the identification of specific application traffic flows so communication policies can be enforced upon the traffic flow. This means each packet entering the switch can be examined as part of the forwarding process to determine what application it belongs to. Because this technology is embedded in the Matrix and SecureStack switch hardware, there is no performance penalty for packet classification services in an Enterasys solution.

End-System Detection/Classification

A critical aspect of a well architected converged network solution is the ability of the network infrastructure to detect end systems when they attach to the network and determine what type of system it is, including Convergence End Points (CEPs). Knowing the type of end system is important in determining the appropriate application prioritization and security policies that should be enforced at the point of network connectivity.

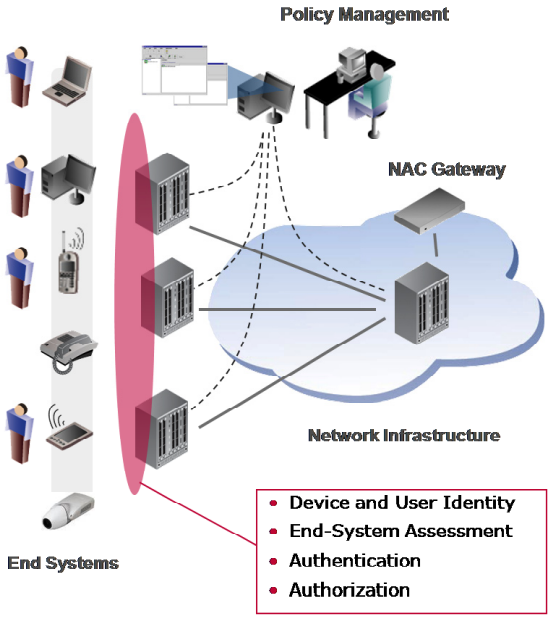


Enterasys Matrix and SecureStack switch products have advanced end-system detection and classification capabilities. End systems can be detected attaching to the secure converged network by forcing authentication and/or CEP detection on the access layer switches. Credentials can be passed to a directory service using the standard IEEE 802.1X protocol where an end system can be classified based on pre-established data. End systems also can be classified by passing their MAC address as the credential in the authentication process. In addition to these options using an authentication service, convergence endpoints can be detected and classified using the unique CEP detection technology embedded in the Matrix and SecureStack switch. Standards-based methods for CEP detection in Matrix switches include: LLDP-MED, destination IP address and Layer 4 Port, SIP, and H.323 / H.245. In addition, the switches can use vendor-specific methods for CEP detection: Cisco Discovery Protocol and Siemens CoreNet.

An important aspect of endpoint detection in a converged network environment is the ability to identify multiple end systems on a single Ethernet port. This is important, for example, when a PC is connected through an IP phone, with both devices connecting to the network switch through a single Ethernet cable. Enterasys Matrix switches have unique multi-user authentication ability so multiple devices can be authenticated separately on a single Ethernet connection into the secure converged network. Using authentication methods for end systems with credentials as well as being able to detect an end system through various signaling protocols enables the network to dynamically classify the end system and adjust the communication policies based on the type of device and its role in the converged network environment.

Network Access Control

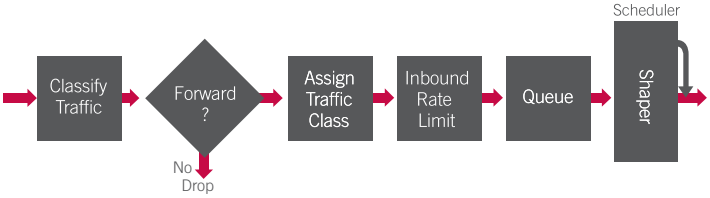
Once an end system is detected connecting to the converged network, a determination must be made on what access the end system should have to the communications infrastructure and the available services. In a well-architected solution, there are several parameters used to determine whether or not an end system can access the network and each of the services it supports.



Enterasys uses several unique technologies to control access to the communications infrastructure as well as the individual services that are available. Leveraging the Enterasys Network Access Control (NAC) solution, access policies are enforced against all types of end systems (including convergence endpoints). The Enterasys NAC solution fully integrates with agent-based and network-based end-system assessment technologies to determine the potential vulnerability and possible threat of an end system attempting to attach to the secure converged network. This is especially important in a network that includes convergence endpoints to ensure that those endpoints (IP phones, IP cameras, etc.) are not vulnerable to attack, or somehow have been compromised and may pose a threat to the entire network environment. Before any end system can communicate on the network, it is assessed. If an end system is determined to be vulnerable or dangerous, it is not allowed to communicate with business services in order to protect the environment. If an end system is deemed safe and secure, it is allowed to communicate to the appropriate services as determined by parameters such as end-system identity, business role, location and time. Access to specific network applications and services is enforced through Layer 2, 3 and 4 related policy rules for containing (VLANs), filtering, rate limiting, and prioritizing network traffic from the end-system.

Enforceable Quality of Service

Historically, data networks have been designed to provision enough bandwidth to support all business applications and circumvent the need to use QoS technologies. This may suffice for networks supporting only data applications, but this is not sufficient for converged networks. Data applications can usually compensate for the occasional dropped packet or variable delays that occur even on underutilized networks. IP telephony traffic, on the other hand, requires that no packets are lost and that



all communication is transmitted with minimal variation in delay to avoid jitter in the voice transmission. Streaming video requires significant and consistently available bandwidth resources for an end-to-end service. Convergence applications can be very sensitive to available bandwidth, packet loss, packet delay and delay variations in its packet streams. Because of the bursty nature of data applications, and the use of single network paths for both data applications and convergence applications, congestion can occur. This network congestion situation can result in packet loss, causing unacceptable service quality of a convergence application. To compensate for these periods of congestion, Enterasys Matrix switches provide a set of QoS and traffic shaping services that can ensure the viability of voice, video, and data traffic on the converged network.

Enterasys Matrix and SecureStack switches support advanced multi-layer packet classification, granular ingress and egress rate limiting and highly accurate queue schedulers.

Enterasys switches use multi-layer classification to associate received traffic with one of several priority levels. These priority levels are related to defined classes of service. Each priority level is mapped to a physical transmit queue. Different scheduling algorithms are used to manage how traffic is forwarded from a switch's queues. Enterasys switches support three types of queue scheduling algorithms. Every switch supports a strict priority scheduling algorithm and a weighted scheduling algorithm. Strict priority is the simplest algorithm and ensures that data stored in the high-priority queue is transmitted before data stored in lower priority queues. Enterasys switches also support the bandwidth-shaping algorithms Weighted Fair Queuing or Weighted Round Robin schedulers. Weighted Schedulers provide a mechanism to guarantee a minimum percentage of bandwidth to a specific queue.

Enterasys switches along with NetSight software use a role-based model to associate traffic with appropriate QoS. Roles are established in policy profiles that can be associated with individual users, systems, services or ports. Enterasys policy profiles enable network administrators to write a set of rules that can control and prioritize various types of network traffic. The rules that make up a policy profile contain both classification definitions and actions to be enforced when a classification is matched. Classifications include Layer 2, Layer 3 and Layer 4 fields. Policy actions that can be enforced include VLAN assignment, filtering, inbound rate limiting, outbound rate shaping, priority class mapping and logging.

The benefit of the Enterasys QoS model is the ability to establish role-based prioritization and rate-limiting policies from a central command console and allow the switches to enforce the appropriate policies automatically when specific end systems and specific applications are identified on the network.

Enterasys switches use multi-layer classification to associate received traffic with one of several priority levels. These priority levels are related to defined classes of service. Each priority level is mapped to a physical transmit queue. Different scheduling algorithms are used to manage how traffic is forwarded from a switch's queues. Enterasys switches support three types of queue scheduling algorithms. Every switch supports a strict priority scheduling algorithm and a weighted scheduling algorithm. Strict priority is the simplest algorithm and ensures that data stored in the high-priority queue is transmitted before data stored in lower priority queues. Enterasys switches also support the bandwidth-shaping algorithms Weighted Fair Queuing or Weighted Round Robin schedules. Weighted Schedulers provide a mechanism to guarantee a minimum percentage of bandwidth to a specific queue.

Enterasys switches along with NetSight software use a role-based model to associate traffic with appropriate QoS. Roles are established in policy profiles that can be associated with individual users, systems, services or ports. Enterasys policy profiles enable network administrators to write a set of rules that can control and prioritize various types of network traffic. The rules that make up a policy profile contain both classification definitions and actions to be enforced when a classification is matched. Classifications include Layer 2, Layer 3 and Layer 4 fields. Policy actions that can be enforced include VLAN assignment, filtering, inbound rate limiting, outbound rate shaping, priority class mapping and logging.

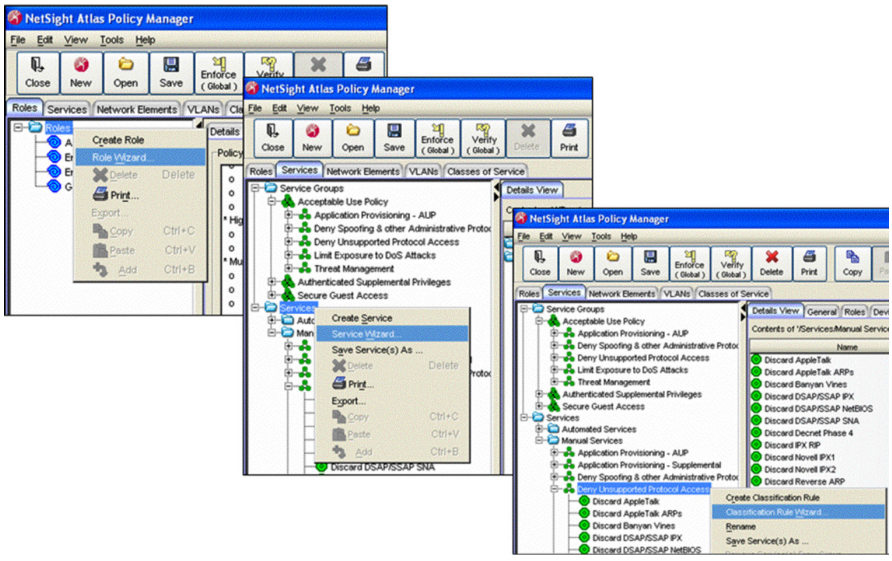
The benefit of the Enterasys QoS model is the ability to establish role-based prioritization and rate-limiting policies from a central command console and allow the switches to enforce the appropriate policies automatically when specific end systems and specific applications are identified on the network.

Enterasys delivers a comprehensive set of technologies to enable the next-generation converged network environment. The table below shows the technologies required to meet the needs of a secure converged network, and the Enterasys products that deliver them.

Secure Convergence Requirement	Technologies/Features		Enterasys Products
Open Architecture	•IEEE •Software Open APIs •3rd Party Event Integration •Support and CEP Type	•IETF •Distribution Layer Policy •3rd Party Security Enforcement	•Matrix SecureStack Switches •NetSight Management Software •Dragon IDS/IPS •Enterasys NAC
Infrastructure Capacity	•Modular Chassis •Modular Uplinks •Stackable Switches •Trunking	•Port Density (24 to 500+ ports per switch) •PoE •Capacity Reporting	•Matrix N-Series Switches •Matrix X Switch/Routers •SecureStack B- and C-Series Switches •NetSight Inventory Manager
High Availability	•Redundant Power •Distributed Switch Fabric •IEEE 802.1w •IEEE 802.1s	•IEEE 802.3ad •Enterasys Span Guard •OSPF •VRRP	•Matrix N-Series Switches •Matrix X Switch/Routers •SecureStack B- and C-Series Switches •NetSight Console
Secure Application Services	•Policy - Traffic Filters •Policy - Rate Limits •Policy - Service Spoofing Prevention •Flow Setup Throttling	•Intrusion Detection •Flow Isolation •Threat Mitigation	•Matrix N-Series Switches •SecureStack B- and C-Series Switches •NetSight Management Software •Dragon IDS/IPS/SIM
Application Traffic Detection/Classification	•Layer 2/3/4 Inspection •Priority Tagging •Policy-Role Association	•Per port/wire speed •Inbound/Outbound Inspection	•Matrix N-Series Switches •SecureStack B- and C-Series Switches •NetSight Management Software
End-System Detection/Classification	•IEEE 802.1X •MAC-Based Authentication •Multi-user Authentication •CEP Detection - SIP	•CEP Detection - H.323/245 •CEP Detection - LLDP-MED •CEP Detection - CDP •Dest. IP + Source Port	•Matrix N-Series Switches •SecureStack B- and C-Series Switches •NetSight Management Software
Network Access Control	•MAC-Based Authentication •Agent & Network Based Assessment •Quarantine/Self Remediation	•Network/Application Usage - Policy Enforced •Location Database •Compliance Reporting	•Matrix N-Series Switches •SecureStack B- and C-Series Switches •NetSight Management Software •Enterasys NAC
Enforceable Quality of Service	•Ingress & Egress Rate Shapers •Packet Tagging (TOS/802.1p) •Policy Routing	•Priority Queuing - Hardware •Application Class of Service	•Matrix N-Series Switches •Matrix X Switch/Routers •SecureStack B- and C-Series Switches •NetSight Management Software

Simple Deployment and Operation

Deploying and operating a converged network from Enterasys is simple. It is important that potentially complex technologies for application optimization and security are not overwhelming to the IT resources available to implement and maintain the network. Using the architectural approach, software-based tools and automatic network functions must be fully integrated to allow for simple and effective administration of the converged network.



With the Enterasys solution, configuration of the network infrastructure devices is easily performed with the use of template-based tools and one-click actions. If an IT administrator wants to configure all ports on the network to dynamically detect Convergence Endpoints (CEPs), it is a simple action which is done once in a central management software interface, and then enforced throughout the network with a single click of the mouse rather than having to make a manual configuration change to each switch in the network.

With the Enterasys solution, establishing the communications policies important for security and QoS of converged application traffic is accomplished with the use of a centralized software interface. Policy rules for voice, video and other communications are configured with the use of an intuitive graphical interface. The policy rules are synchronized with appropriately defined business roles for users and devices – such as surveillance camera *role*, IP phone *role*, enterprise user *role*, etc.), and then fully distributed to the network switches. The network switches are configured globally from the central management interface to enforce the correct policy profile based on the dynamic detection, identification and classification of a connecting device, user and/or application(s). The result is a highly scalable and very easy to administer network policy framework to support all convergence application requirements.

An example of the operational advantage of an Enterasys policy framework versus legacy device specific configuration can be seen below.

Traditional ACL Configuration for Converged Networks	vs. Enterasys Policy Framework
Using ACLs to enforce QoS for a video application's traffic you have to: 1. Telnet to switch 2. Display ACL configuration file 3. Highlight ACL text and copy 4. Paste ACL text into Notepad 5. Evaluate ACL order and insert several QoS rules 6. Re-order remaining rules 7. Copy text in Notepad 8. Paste into switch Telnet session 9. Repeat – for each switch on network *Observed time to deploy one change = 1 hour +*	**Using the Enterasys Policy Framework to enforce QoS for video application's traffic you have to:** 1. Create QoS rule using GUI in Policy Manager 2. Link rule to appropriate device/user role(s) – 1 click 3. Enforce to every switch on the network – 1 click *Observed time to deploy one change = 1 minute*

Summary

In order to keep up with the significant advances in technology-enabled business processes, deploying a converged IP network is inevitable. The benefits of unified communications, completely integrated mobile services, and interactive technologies will drive IT organizations to converge traditionally dispersed business-critical services. Understanding the benefits convergence brings to the business is important, but understanding how to address the additional risks associated with a significantly more important network environment is paramount to an IT organization's ability to build its next-generation business network. Service quality, security, flexibility and integration are the goals, and Enterasys delivers the converged network solution that will help you meet those goals.

A converged network solution from Enterasys offers these key benefits:

- Highest availability of the network and the critical business services that run on it
- Most secure network environment for converged applications and end systems
- Easiest operational model to prioritize critical services and ensure their availability to the business.

With an Enterasys solution, you can select any convergence business application from any vendor and easily implement it with the assurance of total security, availability and quality. If you want to move your network infrastructure to support the next generation of converged business application, look to Enterasys to provide the industry's leading solution.

Contact Us

For more information, call Enterasys Networks toll free at 1-877-801-7082, or +1-978-684-1000 and visit us on the Web at enterasys.com

Thought Leadership
Patented Innovation

enterasys® Secure Networks™

07/08

Delivering on our promises. On-time. On-budget.