AVAYA

IP Telephony
Contact Centers
Mobility
Services

WHITE PAPER

Exploring Alternative Convergence-Ready Solutions from Avaya and Extreme Network

An Executive Brief Linking Business and Operational Objectives to Achieve Trusted Communications

May 2005

Table of Contents

Trusted Communications

Trusted Communications occur when an organization creates and develops a convergence-ready architecture that is both secure and reliable. The main goal of this architecture should be to link a company's business and operational objectives with both the IT infrastructure and the services the infrastructure supports. This paper defines the key characteristics of Trusted Communications and details the importance for IT professionals to create a convergence-ready architecture.

Section 1. Executive Summary — Linking Business and Operational Objectives for Communications at the Heart of Business

Avaya, a worldwide leader in IP communications convergence, and Extreme Networks, a worldwide leader in enterprise infrastructure, have created a focused technology alliance to bring the richness of traditional telephony, enterprise class PBX features, and advanced IP data networking into the emerging Session Initiation Protocol (SIP) and VoIP-based world. This paper will recommend IT architecture considerations and highlight the solution that Avaya and Extreme are jointly developing to deliver a convergence-ready architecture for trusted communications.

In order to align IT with business initiatives, it is necessary to deploy business and communications systems that improve the delivery of customer service, increase the productivity of workers, and support efficient communication and information exchange between customers, suppliers and business partners. The deployment of converged communications, the seamless integration between the IT infrastructure and communication and business applications, enables significant business transformation. To reap the full benefits of converged communications, a company must link its business and operational objectives with both the IT infrastructure and the services that the infrastructure supports. Embedding communications into the heart of business helps deliver business applications to achieve a more productive and effective linking of business and operational objectives.

The migration to converged systems must be accomplished while balancing the demands of: changing regulatory requirements, increased operational control, and minimizing associated risks. To respond successfully to this changing network environment, IT organizations must implement communication and information systems that are both secure and reliable (i.e. Trusted Communications) as well as create a convergence-ready architecture that makes Trusted Communication possible. By creating this linkage, the architecture ensures that an IT organization can respond to evolving business requirements without a significant increase in cost, complexity, or risk.

Trusted Communications occur when an organization creates and develops a convergence-ready architecture that is both secure and reliable. The main goal of this architecture should be to link a company's business and operational objectives with both the IT infrastructure and the services the infrastructure supports. This paper defines the key characteristics of Trusted Communications and details the importance for IT professionals to create a convergence-ready architecture.

Section 2. Business Drivers in IT Transformation

Research recently conducted by Avaya indicates that the top two challenges that companies are facing on a worldwide basis are: the drive to increase profitability, and to reduce operating expenses. However, there are a number of other key challenges facing companies today that include:

- Improve the quality of customer service
- Increase their flexibility and speed of execution
- Increase the productivity of their workers
- Improve their relationship with customers and suppliers
- Increase control and minimize risk
- Adhere to government or industry regulatory guidelines such as the Sarbanes-Oxley Act[1], HIPPA[2], and the Gramm-Leach-Bliley Act[3]

The rapid change in how work is performed in a company is also quite challenging to the IT organization. As recently as a decade ago, the vast majority of work was done on-site and by a company's employees. That style of work allowed IT planners to assume that if a person was doing company work, he/she could be trusted. But today, a large and growing percentage of employees work remotely, either from their homes, hotel rooms, branch offices or client sites. In addition, most firms outsource at least part of the development and operations of their IT function. These two trends have led to a fundamental shift in the trust relationship. In particular, IT planners now need to accommodate multiple layers of trust. For example, a third party applications developer must be granted total access to the application under development, and at the same time be precluded from accessing anything else. This change in trust relationship leads to the concept of Trusted Communications. Trusted Communications refers to communication and information systems that are both secure and reliable. The primary goal of Trusted Communications is to reduce business risk while leveraging communication capabilities.

At the same time that companies are migrating towards Trusted Communications in order to reduce business risk, they are also implementing converged communications as a way to realize their goals of lower cost, increased flexibility, better service to their constituents, improved speed of execution, and increased employee productivity. Converged Communications refers to the seamless integration between the IT infrastructure and communication and business applications.

The phrase "business applications" refers to a wide range of enterprise business applications such as Enterprise Resources Planning, Supply Chain Management, and Customer Relationship Management.

Today's environment is clearly characterized by rapid change in multiple dimensions, including the rapid change in how work is performed, the growing emphasis on ensuring Trusted Communications, and the movement to deploy converged communications. Ensuring that the IT infrastructure responds to a broad range of challenges is always difficult. However, that difficulty is significantly increased when there are rapid changes taking place in the environment. In order to respond to these challenges, IT organizations must develop a convergence-ready architecture that enables trusted communications. The key to developing this architecture is to plan for the evolution of the IT infrastructure in a holistic fashion. A primary goal of Trusted Communications is to reduce business risk while leveraging communication capabilities. Trusted Communications accomplishes this goal by ensuring that communications are both secure and reliable while supporting comprehensive functionality.

[1]This act requires management to make a written assertion stating their responsibility for establishing and maintaining an adequate control structure and procedures for financial reporting.
[2]HIPAA (the Health Insurance Portability and Accountability Act) requires companies in the health care industry to provide administrative simplification, security, and privacy.
[3]This act requires companies to give consumers privacy notices that explain the institution's information-sharing practices and to give consumers the right to limit some of the sharing of its information.

Converged communications is characterized by the seamless integration of the IT infrastructure with communication and business applications. The goal of converged communications is to allow companies to realize their goals; i.e., to lower costs, increase flexibility and speed of execution, to provide better service to their constituents, and to increase the productivity of the company's workers.

Section 3. Trust Model in Communications

As in any form of communication, establishing trust is a basic prelude to engaging in information exchange. The need to mutually verify identities among communicants is basic to engaging in communications of any kind. The solution is straightforward in a brick-and-mortar paradigm—visual, auditory (voice) or other certified validations of identities. The trust model in cyberspace is no different in analogy, but vastly different in technology. Businesses are increasingly shifting to the Internet model of e-commerce externally, and layered trust internally, in the enterprise—extending the 'need-to-know' policy to their data, meta-data and network infrastructure. This means that the network has to be highly resilient so that business processes can continue uninterrupted.

Figure 1 Trusted Communications Model

Trusted Communications occur when an organization creates and develops a convergence-ready architecture that is both secure and reliable. The main goal of this architecture should be to link a company's business and operational objectives with both the IT infrastructure and the services the infrastructure supports. This paper defines the key characteristics of Trusted Communications and details the importance for IT professionals to create a convergence-ready architecture.

The requirement for establishing trust and the resiliency demands on the network establishes the three key principles that form the basis for implementing Trusted Communications — **Security, High Availability,** and **Business Continuity**. Due to the inherently interrelated nature of these elements, it is critical that they be designed in a holistic fashion. For example, assume that a company is in the process of creating a business continuity plan. Further assume that as part of creating this plan, the company has identified a number of business processes that are essential to the operation of the company. In order to ensure the continuity of these processes, it is necessary that the systems that support these processes be designed to have a level of availability and security that is appropriate given the design of the business continuity plan.

To be effective, a company's approach to implementing Trusted Communications must be both **pervasive** and **comprehensive**. In addition, the company needs a migration plan that guides the evolution of its network toward the goal of providing Trusted Communications.

To be **pervasive**, the approach that the company uses must extend to:

- The form of access used (i.e. remote approach or internal approach)
- The type of applications used (e.g. home grown apps, third party apps, data center apps, PC apps)
- The infrastructure used (i.e. Ethernet in the LAN, WAN services such as DSL, T1, or Frame Relay)
- The tools and processes used (i.e. switches, routers, and servers)

To be **comprehensive**, the approach that the company uses must include:

- Tools to support identity and access management (i.e. Radius, Access Control Lists (ACLs), and enterprise directories)
- Ability to support privacy and presence, where presence refers to the user's status (e.g. online or offline)
- Availability (i.e. instant messaging, cell phone, office phone)
- Secure data exchange
- Tools to implement security (i.e. beyond the perimeter to customers and partners and within the perimeter to individual resources such as a server)

a. Security

Of the three pillars bearing the framework of Trusted Communications, security has the role of establishing trust between communicating entities (points), securing the communication path and enforcing access control inside and at the network boundaries, and enabling authorizations to resources inside (trusted clients) and through the perimeter (e.g., extranets). Thus, IT administrators are finding themselves dealing with the virtual bounds of the wire-line and wireless access challenges of the extended enterprise.

Changing business and technical requirements are driving the need for IT organizations to look at security as more than implementing firewalls to secure the perimeter of the enterprise. As can be seen in Figure 1, security must also be looked at inside the core of the network. This section of the document will highlight some of the key changes to perimeter and core security that need to be included to deliver Trusted Communications in a convergence ready architecture.

A number of security mechanisms have developed in response to the obvious security vulnerabilities associated with Wireless Local Area Networks (WLANs). One such mechanism is the emerging IEEE standard[4] 802.1X. This standard is focused on port-based network access control and provides an authentication architecture that is applicable in both wired and wireless environments. The 802.1X standard is intended to secure the network access control inside the enterprise.

A key concept within the 802.1X standard is identity. In this context, identity refers to the accurate and positive identification of network users, hosts, applications, services, and resources. As part of the 802.1X standard, a server will verify a client's identity in order to ensure that authorized users gain access to the appropriate enterprise computing resources, while unauthorized users are denied access.

[4]More information on the IEEE 802.1X standard can be found at www.standards.ieee.org/getieee802/download/802.1X-2001.pdf

The use of 802.1X is an example of the closer integration of the application layer and the network layer. In particular, as part of this standard, the network asks an application server to identify the access rights of a given user.

The 802.1X standard also reinforces the need for the holistic planning of the evolution of the IT infrastructure. In particular, it is a key component to implementing effective security across a wired and a wireless environment, reinforcing the need to plan for the coexistence of the wired and wireless environment. In addition, the 802.1X authentication process identifies detailed information on users and devices. Since this information can be used as part of implementing Quality of Service (QoS), that reinforces the need to plan for authentication and QoS in a holistic fashion.

In order to protect the core of the IT infrastructure, it is necessary to continually measure the behavior of users and applications. One goal of performing these measurements is to identify anomalies that have a high likelihood of representing a security breach. Once an anomaly has been identified, it is important to be able to respond to it in a variety of ways, including further analysis, manual intervention, or automated intervention.

A convergence-ready architecture needs to recognize that there is a significant difference between data and voice. In particular, data consists of two distinct traffic flows, corresponding to network management and the actual information being transferred. Voice adds a third traffic flow, corresponding to voice signaling. A convergence-ready architecture should consider whether or not it will segregate these traffic flows, and if it does, will the segregation be physical (i.e., separate links) or logical; i.e., using Virtual Local Area Networks (VLANs). The architecture also needs to consider which, if any, of the traffic flows should be encrypted.

i. Perimeter & System Integrity
The amplified threat of viruses and Trojans from outside the perimeter has signaled a need to address the problem domain-wide in addition to individual host protection.

This has served to underscore the need to partition and layer security within the perimeter as well. Segmented accesses (perimeters inside) to critical network servers and services include hardening of servers, systems and access paths; systems in-lining firewall access controls; and intrusion prevention mechanisms.

Zero-day attacks have been on the increase. This refers to the same-day time-to-exploit when a detected vulnerability in a system is published. Time-to-exploit has always managed to stay ahead of time-to-resolve and time-to-patch a vulnerable system. The interim window between exploit availability and patch/remediation requires fast-path reactive mechanisms to protect vulnerable systems and services while keeping them up to ensure business continuity.

Bridging and forwarding devices at network boundaries may integrate generic network protection schemes to enforce firewall-like access control and possible intrusion detection and prevention.

Thus, several methods of middle-box functions such as firewalls, IDS, and IPS, offer detection and protection for access control and authorization.

ii. Identity & Access Framework
Unambiguous and rigorous (mutual) validation of communicating entities needed to establish trusted communication sessions. This is true of communication systems, devices and users. This also derives directly as a proactive measure to secure systems as discussed above from unauthorized access and use of resources.

Perhaps the hardest part of creating a secure ecosystem is crafting policies and validating consistency checks across the different policy enforcement points in all layers of a network.

A fail-safe access management & provisioning framework, discussed later, is key to a fully secure management that is self-validating and self-protecting (disallowing invalid configurations). These fail-safes serve to enforce a holistic policy view across all network layers through an administrative domain.

iii. Secure Data Exchange

Having established identities, secure communication sessions are required when traversing paths that are not fully monitored for unauthorized access or disclosure. Conversely, cryptographically secure communications enhance the reach of access across the insecure world of external networks such as the Internet.

Secure data exchange is also required to offset insider attacks to snoop or modify sensitive communications inside a secure perimeter, in addition to communicating through external and public networks of unknown integrity.

Wireless LAN access standards provide 802.11i (impending standard) protocol for securing communications over the air from clients to peers or access points. IPsec VPNs provide encryption and security controls for IP transmission across networks. TLS offers transport-layer security for connection-oriented protocol sessions. The latter two are popular remote access methods for the extended enterprise and nomadic access. Wireline standards are set to extend 802.1X switch/bridge access control framework to establish secure communications.

Application layer security provides session level security of end-to-end, peer-peer or client-server networks. Examples are signaling channel and bearer channel security of VoIP flows. Where policies and sensitivity of applications (such as VoIP) and their related security requirements are distinct enough, application layer security will need to be enforced without assumptions on transport and IP layer security policies.

Content security profiles, deployed for securing self-contained messages such as IM and email (using S/MIME or XML-encryption), are also involved in IP communications.

iv. Security Practices

Security begins at the source. Security of a whole system is only as good as the strength of its weakest link.

1 Secure by Design

Thus, a solution is secure when each autonomous element (product) in it is secure. However, a flawed design or implementations will nullify the value of the most secure elements.

2 Secure by Default & Configuration

However secure a built product/solution is, two scenarios leave the door open for install-time and runtime problems. They are:

1 Inability to deploy safely out of the box

2 Not configured appropriately to fit the (customer) operating environment

Ease of secure configuration is a benefit to the customer and vendor alike in terms of virtual savings in man-hours and support overhead. It also affects productivity by improving business continuity as a result of minimized system downtimes.

v. Secure Management
Management of systems involves: configuring, policing and regulating shared resources. Previous sections referring to secure practices call for securely configuring to fit an environment. Compromising management subsystem is an easy way to annul all the security built into a secure solution and environment. Management framework is the last of the links in the proverbial chain that can't afford to be weak.

Providing a secure management framework is an integral part of Best Practices in Secure by Design required to facilitate Secure by Default and Configuration.

Secure management practices constitute use of appropriately secure configuration protocols such as SNMPv3 and TLS/SSH transports; and suitable role-based administrative policies based on strongly provisioned authentication mechanisms.

Provisioning, network management, identity, and policy management are the typical elements of a management subsystem. Network management itself typically constitutes monitoring and configuration of network elements, servers, switches, routers and client devices—potentially across multiple connected networks.

Management security is an essential part of the system security. This includes secure methods of access and updates to the management repositories, servers and consoles.

vi. Accreditation: Security Standards & Certifications
Besides internal best practices for security, to ensure multi-vendor interoperability and compliance to rigors of standard security protocol implementations and practices, several independent accredited organizations offer certification programs. They include programs for firewall, IDS, IPS, VPNs, AntiVirus and cryptographic federal standards—FIPS 140-2. Security sensitive vertical markets such as finance and healthcare are sensitive to regulatory requirements on privacy and access to customer data and meta-data. They have additional responsibility in use of security guidelines and accreditation to ensure a vendor solution has the ability to help them meet regulatory requirements.

b. High Availability and Business Continuity

The changing business environment has caused even more emphasis on ensuring availability and business continuity. For example, there is an ever-increasing reliance on the IT infrastructure to support a wide range of business functions—i.e., sales, engineering, and customer service. As a result, if the IT infrastructure is either unavailable or performing badly, there is a significant negative impact on the business.

A conventional IT architecture enables high availability and business continuity for selected components of the IT infrastructure. A convergence-ready architecture needs to ensure high availability and business continuity for a range of new and different types of devices and services such as communications servers and gateways. A convergence-ready architecture also needs to have a greater emphasis on scalability than was previously necessary because of all the additional network elements that the IT infrastructure needs to support. One component of scalability is the ability to support a large number of MAC and IP addresses.

In order to support the business need for high availability and business continuity, the convergence-ready architecture needs to identify what functionality is required in each of the first three layers of the OSI model.

1 At the first layer of the OSI model, the architecture needs to ensure that each piece of equipment (i.e., switches, routers, servers) can be upgraded without taking that piece of equipment out of service. The architecture also needs to ensure that each piece of equipment has the ability to continue to operate in the event of a failure somewhere else in the network.

2 The architecture needs to consider providing for redundancy at the second layer of the OSI model. Possible solutions include load balancing across multiple links as well as implementing one or more hot stand-by routers.

3 At the third layer of the OSI model, the architecture needs to ensure that the network is self-healing. One component of a self-healing network is to ensure that there are multiple paths between devices, and that there are fast fail-over protocols that will switch traffic from one path to an alternative path in a matter of milliseconds.

As will be discussed in the next section of this document, an effective IT architecture needs to plan for high availability and QoS in a holistic fashion.

Section 4. Communications & Convergence

At the same time that IT organizations are migrating towards Trusted Communications in order to reduce business risk, they are also implementing converged communications as a way to better realize their goals — to lower cost, increase flexibility, provide better service to their constituents, improve the speed of execution, and to increase the productivity of the company's workers. As depicted in Figure 2, "Converged Communications" is characterized by the intelligent integration of the IT infrastructure with both communication applications and business applications.

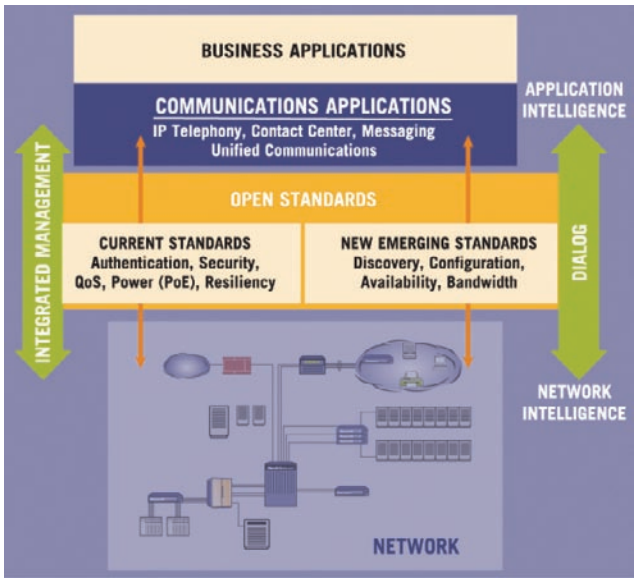

Figure 2 Converged Network for Trusted Communications

A key component of converged communications is the focus that it places on end user capabilities and on end user control. Converged communications enables users to be connected to information resources from anywhere, according to their individual preferences and availability. It also enables users to utilize whatever mode (wired or wireless) and whatever devices are most convenient to them, in order to access any information for which they have authorization.

The movement to deploy converged communications also increases the need to plan for the infrastructure in a holistic fashion. In the "Trust Model in Communications" section of this document outlined one reason why holistic planning is essential. As discussed in that section, the plans that a company makes for business continuity impact how it needs to plan for component availability and security.

However, in addition to planning holistically across functionality such as business continuity, availability and security, it is also necessary to plan a particular function or process across the entire IT infrastructure. For example, employees are using an ever-increasing array of phones, PCs, PDAs and other appliances to access their company's applications. An efficient authentication process that allows for this, and includes both communications and applications, is necessary in to maintain the manageability, security and cost effectiveness of the IT infrastructure.

The movement to deploy converged communications drives some fundamental changes throughout the IT function. Some of the primary changes driven by the movement to converged communications are described below.

a. Access

The movement to converged communications forces IT professionals to re-examine some of their fundamental assumptions relative to access. For example, it is now possible to access voice mail that is stored on a PC, and to access email via speech.

While giving workers more ways to access their company's data can clearly increase the productivity of those workers, it also increases security vulnerabilities. In particular, prior to the deployment of converged communications, the only way that the vast majority of workers accessed their company's data was over the company's data network, typically using a PC. The security for this traditional form of data access is normally provided by a combination of user login and password.

Speech access represents an alternative path to access corporate data that must have appropriate security mechanisms. Given the volume of end users, it is critical that these security mechanisms be easy to administer. It is also a requirement that these security mechanisms allow a given user the same access to company data independent of how the user accesses that data. Finally, it is a requirement that when it is appropriate to change or delete a user's access to company data, that it is easy to do this for all possible paths that the user has to access company data.

i. Wireless

Wireless has rapidly reached near-ubiquity in all walks of life—corporate, residential and public spaces. Not only does wireless access offer an un-tethered convenience to facilitate seamless anywhere-access, but it also enhances productivity.

However, the current 802.11 security model can be proven insecure. When first generation WLANs were implemented in enterprises, their relative lack of security functionality represented a security vulnerability compared to the apparent security of wired LANs. Because of that, as organizations began to deploy second generation WLANs, they typically implemented a variety of security mechanisms, including encryption using Data Encryption Standard (DES) or Triple Data Encryption Standard (3DES) as well as dynamic Wired Equivalent Privacy (WEP). In addition, new encryption techniques such as Advanced Encryption System (AES) are being developed. Because AES allows for a 256-bit key, it is significantly harder to break than DES or 3DES.

ii. Wire-line

An interesting characteristic of wired LANs is that they are insecure, but not as obviously so as WLANs. In particular, now that companies have deployed WLANs with encryption and dynamic WEP, it is the wired LANs that represent relative security vulnerability.

Existing standards in wire-line security within the enterprise have been traditionally limited to port-based access control. Threats to the network infrastructure have brought up the need to protect link and IP layer

communications between forwarding entities (routers, bridges). The 802.1X port-based access control mechanism is used as the authentication framework to establish security associations in WLANs and is being extended to consider similar security to wired LANs.

b. Performance

Traditional network architecture is intended to support a relatively narrow range of traffic types; for instance, email and standard inquiry/response applications. While traditional network architecture primarily focuses on network parameters for availability, delay and packet loss, a convergence-ready architecture needs to support additional traffic types such as voice and video. As such, a convergence-ready architecture needs to ensure a more stringent level of availability, delay and packet loss than would be found in a traditional network architecture. In addition, a communications ready architecture also needs to ensure low, predictable jitter.

QoS refers to the ability of the network to implement policies that ensure that preferential treatment is given to certain classes of traffic. QoS is a necessary component of a convergence-ready architecture because the architecture requires support for a broad range of traffic types.

However, the use of QoS in a convergence-ready architecture must be planned in conjunction with how high availability will be supported. In particular, as part of ensuring high availability, a convergence-ready architecture must provide multiple paths between devices as well as fast fail-over protocols that will switch traffic from one path to an alternative path in a matter of milliseconds. However, once this traffic is switched to an alternate path, it is likely that there will not be sufficient capacity to carry both the traffic that was originally on that alternative path plus the traffic that was just added.

A convergence-ready architecture must ensure that when a fail-over does occur, that QoS mechanisms will maintain the appropriate level of service to a wide range of applications. In a convergence-ready architecture, integration must occur between multiple classes of applications and the network.

c. Network-Application Integration

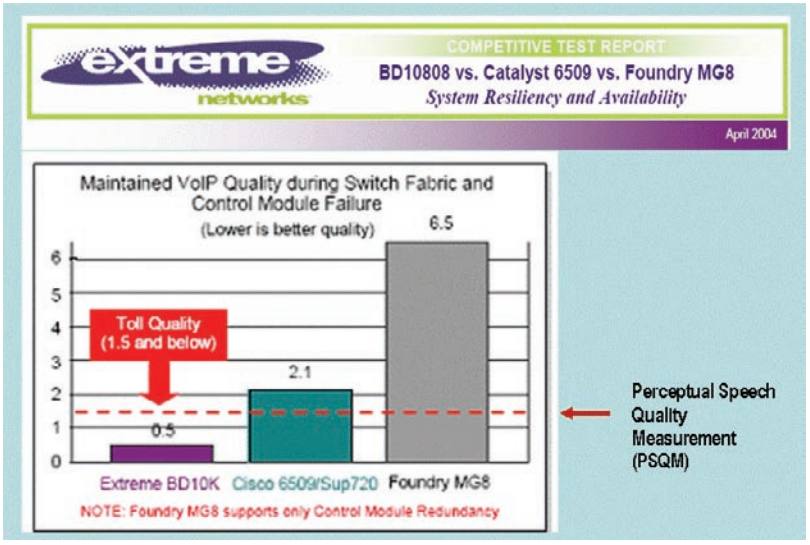

Figure 3 Highly Available and Resilient Infrastructure Supports Trusted Communication Networking

The phrase "communications application" refers to communication solutions such as contact center, unified communications messaging and telephony.

Integration is required between business applications and communications applications. Integration is also required between the network infrastructure and both classes of applications. Note that Figure 3 depicts how much of the infrastructure functionality that has been discussed in this paper (i.e., QoS, 802.1X, security, resiliency) is positioned within a convergence-ready architecture.

Secure management introduced the concept of integrated adaptive management in the context of providing security. Integrated adaptive management is the ability to control and manage the behavior of users and applications running on the network based on an analysis of up-to-the-minute network conditions. Integrated adaptive management requires a closed-loop process whereby changes in the network can be analyzed, and this analysis results in enforcement of policy changes within the network.

d. Personnel Issues

A traditional IT architecture is concerned primarily with the various elements of the IT infrastructure, i.e., switches, routers, servers. In addition to those elements, a convergence-ready architecture is also concerned with the personnel who will be using the system. Topics that impact personnel must be accounted for in a convergence-ready architecture, including E911, emergency power, and regulatory requirements such as the Americans with Disabilities Act.

Access to E911 services is a requirement that introduces some demanding challenges. In particular, in many situations the law requires that when someone calls 911, both the calling number, as well as the location of the caller, must be available to the 911 operators.

In a traditional voice system, it is relatively easy to support E911 access, as there is a long-term relationship between a port on a PBX and a phone. However, one of the advantages of IP telephony is that it lowers the cost associated with moving equipment. IP telephony does this by making it possible to move a phone to a new location without involving the IT organization.

Hence the new challenge is to allow for easy, low-cost movement of phones while adhering to legal requirements. One way this can be accomplished is with an application that maintains a database mapping the IP phone's unique layer 2 address to a physical location being served by a port on a switch.

In a traditional approach to voice communications, the phone is powered by the system over the same wires that carry the voice signals. However, IP telephones are cabled to the Ethernet LAN switch and not to a PBX. As such, a convergence-ready architecture needs to ensure that there is power available to IP phones for normal operation. While IP telephones can typically be powered at the desktop, loss of building power will render the telephone inoperable. The alternative is to power the telephones from the wiring closet using Power over Ethernet where backup power—or un-interruptible power supply—can ensure the telephones continue to operate when electrical power is lost to the building. This helps to ensure that a company's personnel can make calls in spite of an emergency such as a flood or electrical storm.

There are a number of regulations relative to the requirement to support equal access to communications solutions, including:

- Titles II, III and IV of the Americans with Disabilities Act
- Sections 251 and 255 of the Telecommunications Act
- Sections 504 and 508 of the Rehabilitation Act amendments

A convergence-ready architecture needs to ensure compliance with these regulations. For example, a typical business phone presents a broad range of information to a sighted person such as the name and number of the calling party, whether or not a new message is waiting, as well as which lines are available and which are on hold. In order to present this information to users who are visually impaired, a convergence-ready architecture should consider leveraging the user's PC in order to provide the information by voice output from the PC.

In addition, since many persons with hearing disabilities still rely on their TTY telephone to communicate, IT managers must ensure that their networks will support the reliable operation of these devices, which introduces challenges when the TTY signals must traverse an IP network.

Section 5. The Mandate to Create an IT Architecture

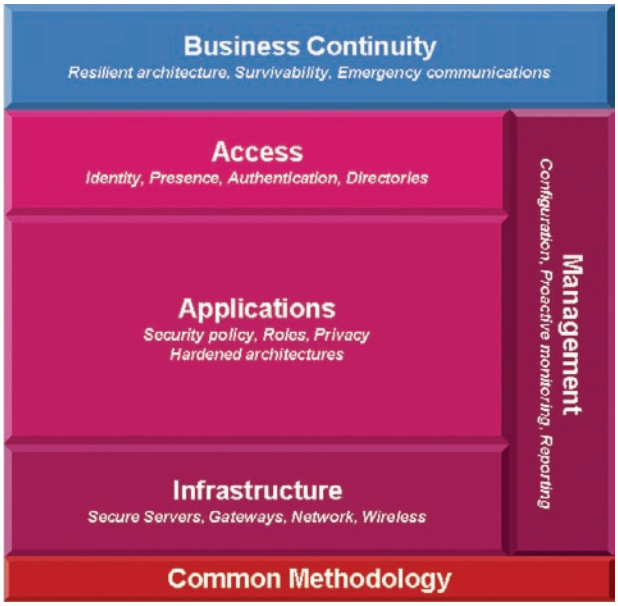

Figure 4 Trusted Communications Architecture Framework

As mentioned in the " Business Drivers in IT Transformation" section, market research that was recently completed by Avaya identified the top challenge for companies is to grow profitability in general, and to reduce operating expenses in particular. Given this, it is not surprising that the most important business issue for IT organizations is the requirement to do more with less.

In order to meet this challenge, an IT organization must first define IT architecture. A key goal of the IT architecture is to link a company's business and operational objectives with both the IT infrastructure and the services that the IT infrastructure supports. By creating this linkage, IT architecture ensures that an IT organization can respond to changing business requirements without a significant increase in cost, complexity, or risk.

Without IT architecture, networks typically evolve in an unplanned fashion. In some instances, this means deploying a new solution for each new business requirement. If a company has grown by mergers and acquisitions, this can also mean creating a network by combining disparate IT infrastructures. Both of these approaches leads to a complex IT infrastructure.

A complex infrastructure introduces significant challenges:

- Increased cost of maintaining and modifying the IT infrastructure
- Increased difficulty and expense of providing for Business Continuity
- Increased difficulty and expense of implementing security in ways that enable multiple layers of trust

A convergence-ready architecture must be constructed to conform to the following principles:

- The ability to scale to meet business needs
- Granular control over the network and its resources
- End-to-end simplicity for design and management
- Standards-based architecture for increased flexibility and investment protection
- Security and reliability to protect corporate assets

In order to be effective, IT architecture must be constructed to conform to certain principles:

- **Appropriately Simple:** This means that an effective IT architecture must carefully choose which functionality should be included as part of the IT infrastructure. This choice needs to be made by balancing the business benefit provided by the functionality against the added complexity associated with the functionality.
- **Scalable:** In this context, scalable certainly refers to the addition of an ever-increasing number of users and devices. However, scalable also refers to the ability to easily add new functionality to the IT infrastructure.
- **Granular:** For example, in order to support effective security, the architecture must specify a sufficient number of Access Control Lists. In order to support effective QoS, the architecture must specify a sufficient number of levels of QoS.
- **End-to-End:** The architecture needs to address communications requirements from origin to destination, independent of whether or not the user is at a company site or in a hotel room.
- **Integrated:** The architecture needs to ensure that technology is included in the network, servers, and applications in ways that allow them to operate seamlessly.
- **Standards-Based:** In order to ensure interoperability, the architecture must focus on standards-based solutions.

Section 6. Ease of Migration

For architecture to be effective, it must be relatively easy to migrate from the current IT infrastructure to the one envisioned in the architecture. Some of the key steps that must be taken to assess whether or not it is relatively easy to migrate to a convergence-ready architecture include:

- Document the current IT infrastructure. This includes identifying the equipment that is in production, the configuration of this equipment, the version of software that is running on this equipment, as well as the overall network topology.
- Identify the company's key applications, whether they are existing applications or are under development.
- Baseline the performance requirements of these key applications.

- Assess the network's ability to support acceptable levels of:
  —Availability
  —Delay
  —Jitter
  —Packet Loss
  —Quantify the network's ability to support the additional loads that result from combining all traffic onto a single infrastructure
  —Assess the ability of the infrastructure to protect and defend against security attacks
  —Determine the company's ability to manage the IT infrastructure in an integrated manner

Section 7. The Avaya and Extreme Solution

Avaya is a worldwide leader in IP communications convergence bringing the richness of traditional telephony features to bear into the emerging SIP and VoIP-based world. Extreme Networks is a worldwide leader in enterprise infrastructure with established excellence in wire-line and fast-evolving wireless LAN technologies.

Convergence and service-oriented architecture paradigms are quickly maturing and have begun to deliver application services unobtrusively to the enterprise business processes and end-user consumers alike. Network resiliency, security and quality of service with integrated secure management are critical to the high availability, continuity and manageability of backend infrastructure services—both the distributed and centralized network. In turn they form the foundation to guarantee the resiliency of communication services architecture. This is achieved by deeply embedding best-in-breed communications into the heart, or fabric, of business, using software, services and systems that layer seamlessly on any network.

Avaya and Extreme are committed to deliver best-in-class network and application platforms with seamless discovery, authentication, authorization, policy management and mobility. Extreme's network and link layer technologies offer solid infrastructural footing that highly available enterprise-class IP communications from Avaya builds upon. The Avaya commitment to application availability, security and QoS, combined with Extreme's standards-based enterprise-class networking resiliency, deliver best-of-breed solutions. This forward-looking alliance is based upon joint strategic initiatives in technology and standards.

Avaya and Extreme are leaders in communications applications and enterprise Infrastructure—mutually complementary strengths in enterprise communications—with a highly synchronized approach to convergence. Together, Avaya and Extreme are poised to deliver seamless solutions committed to meeting customer expectations of best-of-breed convergence and multi-vendor interoperability.

As emphasized and established through this paper availability, business continuity and security are the corner stones of enterprise communications. A synergic confluence of standards-based resilient enterprise switching infrastructure platforms with communication services delivers value-enhanced features for converged communications spanning the seven network layers.

a. The Value Proposition of Avaya and Extreme Alliance

High availability, reliability and quality of service demands required in conventional telephony networks combined with the security and business process continuity of today's data networks in the conventional and extended enterprise and beyond raises the bar on converged networks for the whole to be greater than the sum. End-to-end security, availability and reliability are no longer nice to have, but have become core requirements. Manageability becomes an equally critical entity to bring continuity, consistency among converged element configurations and monitoring.

Together Avaya and Extreme Networks provide a substantial foundation to support security, availability, reliability and manageability across end-to-end networking layers. Avaya has been unique and first in its enforcement of end-end security, building a proactive and reactive security model for converged applications. Combined with Extreme's network-level 802.1X-based AAA framework, the Avaya integrated perimeter security portfolio of VPNs, firewalls, CLEAR-flow based intrusion detection, and action and response capabilities provide a unique and adaptive self-protecting converged network framework.

Extreme's excellence in network layer fault detection, redundancy and high availability switching architecture, combined with the Avaya application layer resiliency of local survivable processors offers a unique and provable end-end business continuity proposition to the extended enterprise. This end-to-end cross-layer resiliency, when configured right, offers an industry-first adaptive self-healing converged network framework.

Avaya and Extreme have taken the initiative to co-develop an integrated management framework resulting in a holistic converged management model. This, combined with the evolution of self-protecting and self-healing converged networks, is the first step towards an adaptive converged management framework—which extends beyond mere network management—to management of identities and policies.

Section 8. References

1. Extreme's CLEAR-Flow Architecture.
2. Avaya IP Telephony Implementation Guide.
3. Avaya Communications Architecture
4. Avaya IP Solutions: Reliability & Availability
5. Avaya IP Voice Quality Networking Requirements
6. VoIP via VPNs
7. Security in Converged Networks
8. Avaya Communications Manager – High Availability Solutions
9. Deploying VoIP in the Federal Government
10. Memory Scanning and Remapping in Extremeware
11. Security on IP Networks

Call to Action

For more information on how Avaya can take your enterprise from where it is to where it needs to be, contact your Avaya Client Executive or Authorized Avaya BusinessPartner, or visit us at www.avaya.com

About Avaya

Avaya enables businesses to achieve superior results by designing, building and managing their communications infrastructure and solutions. For over one million businesses worldwide, including more than 90 percent of the FORTUNE 500®, Avaya's embedded solutions help businesses enhance value, improve productivity and create competitive advantage by allowing people to be more productive and create more intelligent processes that satisfy customers.

For businesses large and small, Avaya is a world leader in secure, reliable IP telephony systems, communications applications and full life-cycle services. Driving the convergence of embedded voice and data communications with business applications, Avaya is distinguished by its combination of comprehensive, world-class products and services. Avaya helps customers across the globe leverage existing and new networks to achieve superior business results.

AVAYA

COMMUNICATIONS
AT THE HEART OF BUSINESS

avaya.com

Printed in the U.S.A.
04/05 • EF-SVC2658