



## Frequently Asked Questions

### Secure Multimedia

#### Introduction, scope and objectives

The intent of this Frequently Asked Questions (FAQ) is to provide an overview of some of the answers to some of the common security questions surrounding the Nortel Secure Multimedia Solution. This document will highlight some of the Secure Multimedia capabilities of Nortel's Multimedia and IP Telephony systems.

#### Secure Multimedia — market landscape and Nortel position

For several years now, CxO, IT and Telecommunication Managers have reported security as a key barrier to wide-scale deployment of multimedia and IP Telephony solutions in the enterprise. Nortel continues to respond to this need by continually incorporating security capabilities into each release of our convergence products.

#### Market baseline of security capabilities

The key dimensions of emerging security baseline are:

- › A trusted, hardened computing platform
- › Responsive and resourceful vulnerability management systems
- › Confidentiality and privacy of voice conversations
- › Protection from man-in-the-middle, spoofing and Denial of Service (DoS) attacks
- › Strong password management capabilities
- › Toll fraud protection
- › Secure remote management access

#### Questions covered in this document include:

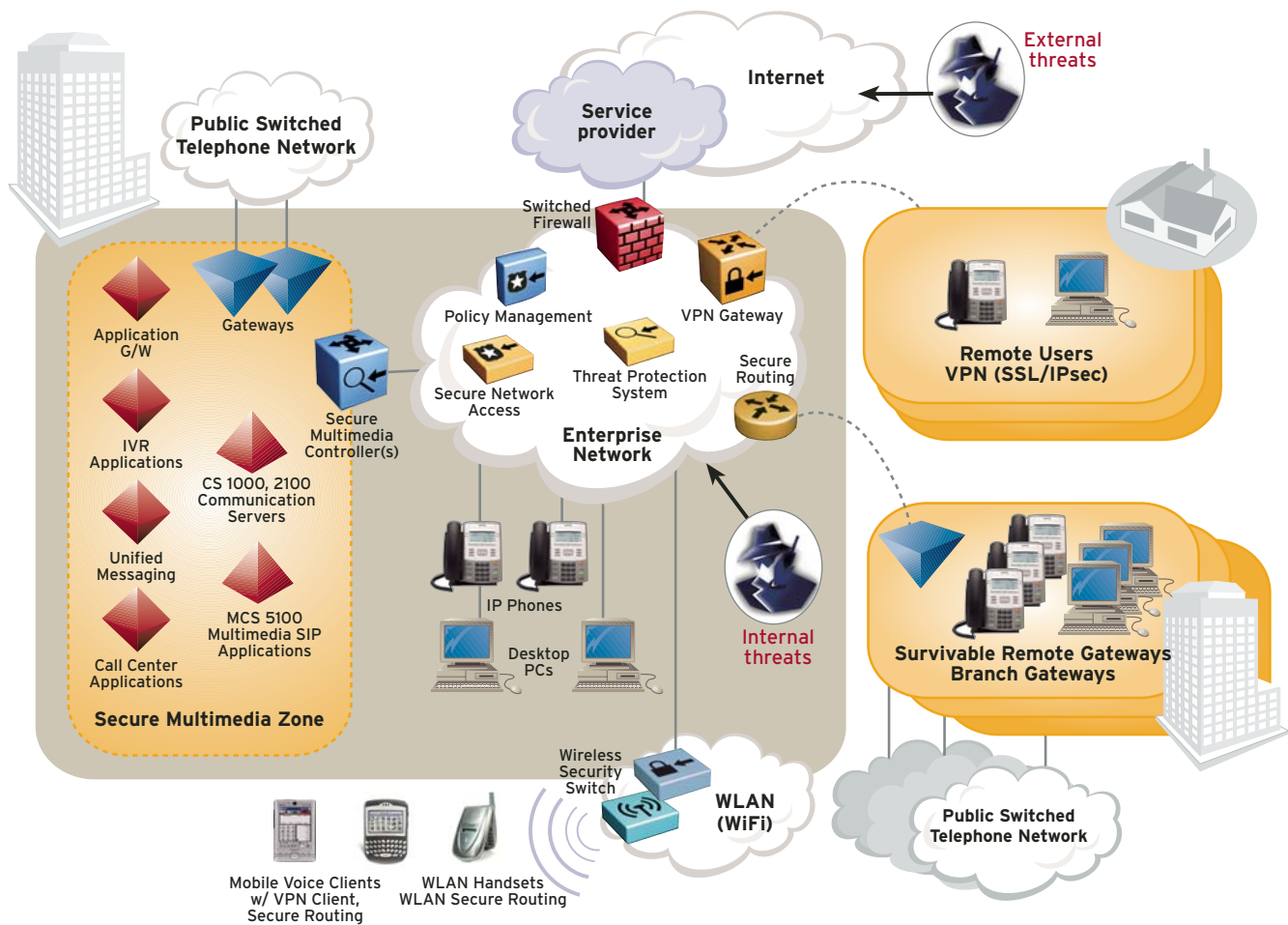
<b>Q1.</b> What solution does Nortel offer to secure IP Telephony and multimedia communications? ( <i>Secure Multimedia</i> )	2
<b>Q2.</b> What is Nortel's overall strategy for providing comprehensive network and communications security? ( <i>Layered Defense</i> )	3
<b>Q3.</b> Does Nortel offer an overall security framework (including not only technology, but also people and processes) to help me formulate a security plan for my organization? ( <i>Unified Security Framework</i> )	4
<b>Q4.</b> How can I protect my multimedia and IP Telephony servers from attacks? ( <i>Secure Multimedia Zone</i> )	5
<b>Q5.</b> How can I prevent attacks from occurring on the user LAN and affecting my Voice over IP (VoIP) and multimedia communications? ( <i>Threat Protection System</i> )	5
<b>Q6.</b> How do I prevent unauthorized clients and endpoints from accessing my IP network, and possibly gaining access to my IP Telephony and multimedia communication services? ( <i>Secure Network Access Solution</i> )	6
<b>Q7.</b> How can I prevent man-in-the-middle attacks and impostor servers or clients? ( <i>Authentication, Encryption</i> )	6
<b>Q8.</b> How do I prevent manipulation of IP Phones? ( <i>Hardening, Authentication, SMC, Tamper-Proofing/Passwords</i> )	7
<b>Q9.</b> How do I prevent DoS attacks from affecting my communications? ( <i>SNAS, SMC, TPS</i> )	7
<b>Q10.</b> How can I secure multimedia and IP Telephony on my Wireless LAN? ( <i>WLAN Security Switch, NSNA</i> )	8
<b>Q11.</b> How can I secure communications to my remote teleworkers or road warriors? ( <i>IPsec, SSL, VPN</i> )	8
<b>Q12.</b> How can I secure communications to my branch offices? ( <i>Secure Router, VPN Router, BCM</i> )	9
<b>Q13.</b> How do I prevent eavesdropping and protect privacy of communications? ( <i>VPN, Encryption, SMC, VLAN, Ethernet Switching</i> )	9
<b>Q14.</b> How does Nortel ensure their communications platforms are secure? ( <i>SATE, Hardening</i> )	10
<b>Q15.</b> How do I secure access to system management capabilities? ( <i>Out-of-band management, password policies, VPN</i> )	10
<b>Q16.</b> What measures are available to protect me from toll fraud, both via traditional means and via IP and wireless networks?	11
<b>Q17.</b> How do I guard the privacy of usage and billing data?	12
<b>Q18.</b> How do I ensure the privacy of my voice mail and unified messaging systems?	12
<b>Q19.</b> How can I prevent unauthorized moves/adds/changes to my IP Phones, and how can I ensure that my users have the correct access to emergency dial codes, such as E-911?	13
<b>Q20.</b> What other resources are available to learn more about the Nortel Secure Multimedia Solution?	14

**Q1. What solution does Nortel offer to secure IP Telephony, VoIP and multimedia communications?**

*(Secure Multimedia Solution)*

**A1.** Nortel's Secure Multimedia Solutions allow organizations to deploy IP-based voice and multimedia applications, while still meeting or exceeding their need to secure critical information, communication and services. Secure Multimedia uses a layered defense approach designed to ensure communication privacy and protection from the theft of intellectual property as well as maintaining reliability by protecting critical communication resources from service disruption via attack protection, secured management and geographic redundancy technologies. Nortel Secure Multimedia Solutions address these customer challenges by using hardened application/call servers, VPN technology (IPsec and SSL), secure routing, high performance firewalls, Secure Multimedia Zone, Nortel *Secure Network Access* endpoint security and the Nortel *Threat Protection System*, as well as device management and professional services — including security network design, installation and maintenance.

**Figure 1. Secure IP Telephony, VoIP and multimedia communications**



## Q2. What is Nortel's overall strategy for providing comprehensive network and communications security?

(Layered Defense)

**A2.** Nortel focuses on network and communications security for mobile and converged applications. We do this through a Layered Defense approach to network security that is designed to ensure there are no single points of security failure in a network. This means leveraging multiple approaches to security enforcement at multiple areas within a network.

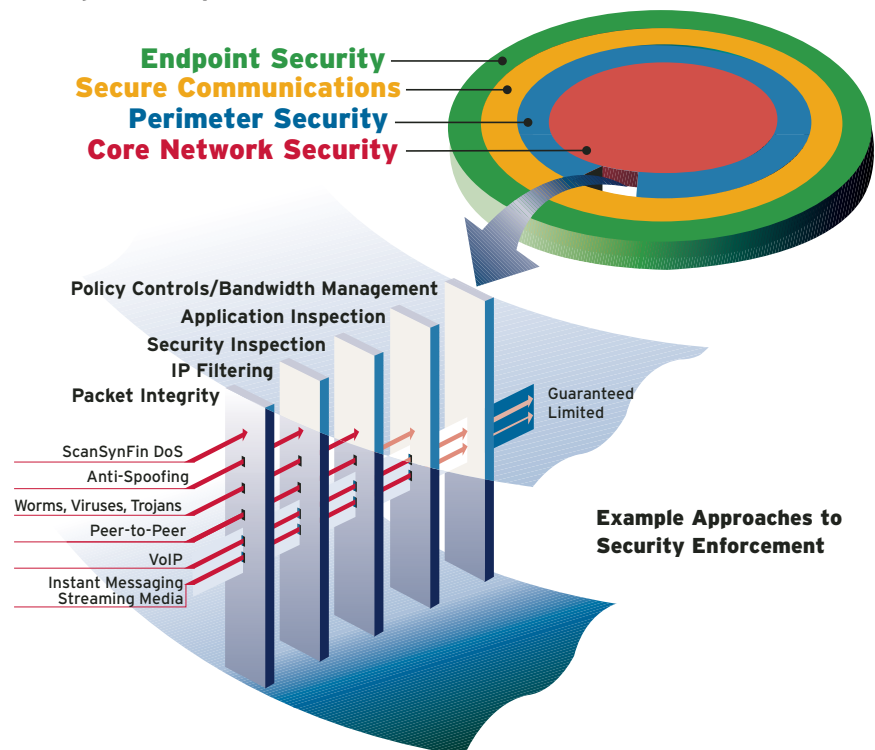
Nortel has long built highly reliable networks by removing single points of security failure. This philosophy of implementing security in a layered fashion ensures network and security resiliency. If a primary layer of security is breached, the secondary layer (or tertiary, etc.) is in place to thwart an attack. While these layers can represent specific areas within a network such as Endpoint Security, Perimeter Security, Core Network Security and Communications Security, they can also represent multiple approaches to security enforcement such as filtering and signature-based inspection.

On the chart we have a cross section of the perimeter security layer with several example approaches to security enforcement. As you can see, the diagram illustrates how different types of traffic — attack and non-attack based — are interrogated by different approaches to security enforcement as they pass into the network. While the first approach layer, packet integrity, may stop the ScanSynFin DoS attack, viruses evade the first two approach layers and are stopped by the security inspection layer. Further layers of security enforcement can allow traffic to pass, but restrict its bandwidth, so as not to exceed a specified amount.

Some of the features that set Nortel apart in this space include:

- > *Open architecture* solutions that rely on strategic partnerships and standards compliance to minimize integration costs, enable state-of-the-art security capabilities and address future security needs.
- > *Minimizing TCO* by focusing on improving operational efficiency, integration simplicity and actively responding to unforeseen security threats. We work to provide fully-integrated security products/solutions that are agnostic to the primary network architecture.
- > Maintaining *Quality of Experience* for end user communication quality while still simultaneously providing high levels of security.

Figure 2. Layered Defense



### Components of a Layered Defense:

- **Core Network Security** — Keeping watch for malicious software and traffic anomalies, enforcing network policy and enabling survivability.
- **Perimeter Security** — Keeping the “good stuff” in and the “bad stuff” out by securing the boundaries between zones of different levels of trust.
- ◆ **Communications Security** — Ensuring information protection from unauthorized discovery over the network.
- ▲ **Endpoint Security** — Ensuring valid identity and connected device security policy compliance.

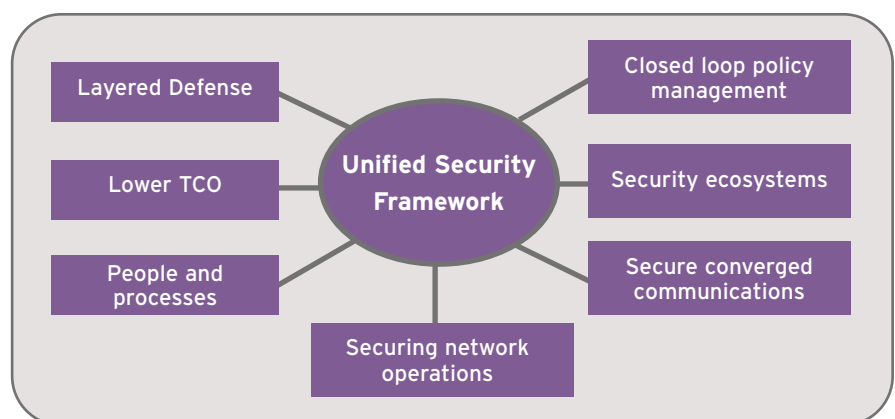
**Q3. Does Nortel offer an overall security framework (including not only technology, but also people and processes) to help me formulate a security plan for my organization? (*Unified Security Framework*)**

**A3.** Nortel does offer a customer blueprint for deploying world-class security architectures. Nortel's *Unified Security Framework* provides customers with a blueprint for forming their own comprehensive security plans considering all aspects of network security — the people, processes and technologies.

To help our customers, Nortel has developed a framework which assists in understanding that network security involves not only technology, but the people — and their behaviors on the network — and the processes the organization puts in place. This framework considers all aspects of network security required to build a strong security solution or architecture. The attributes behind the Unified Security Framework provide organizations a security blueprint that they can use as they move towards increasingly open network environments.

There are seven attributes behind the Unified Security Framework:

- › Implementing a *Layered Defense* approach to network security by using multiple approaches to security at multiple locations in a network.
- › Driving for *lower TCO* with regards to security infrastructure by focusing on operational efficiency and application prioritization.
- › *People and processes* refers to developing and enforcing security policies that address not only technical considerations, but also the business and human aspects of security. A properly designed and implemented security policy must clearly identify the resources in the enterprise that are at risk and resulting threat mitigation methodologies, whether these are procedural or electronic.
- › *Securing network operations* — Given the greater access authority and functional privileges granted to network management personnel, their access and activities must be carefully secured to protect network configuration, performance and survivability.
- › *Secure converged communications* — Given that unified networks can carry voice, data and video — each with their unique performance requirements and security considerations — when and where to protect this traffic is a major consideration and is a key element of any enterprise security policy.
- › *Security ecosystems* — The term 'ecosystem' is a common industry term. Here this term applies to a process whereby the business value of solutions can be expanded through partnerships leveraging open solutions and standards, and thus unleashing more innovation.
- › *Closed loop policy management* includes configuration management of network devices, enforcement of policies in the network and verification of network functionality via audit trails. All are implemented in a feedback loop to ensure that policies are continually refined for maximum security.



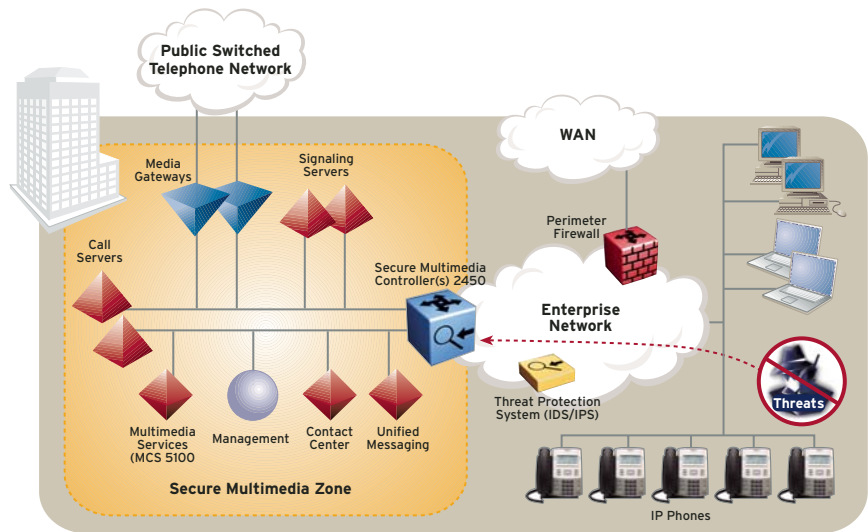
#### Q4. How can I protect my multimedia and IP Telephony servers from attacks? (*Secure Multimedia Zone*)

**A4.** Multimedia servers face threats not only from outside the corporate network, but also face a far greater threat from internal users whose PCs and workstations have greater access and bandwidth to provide bots, worms, viruses and other ‘malware’.

Size and complexity make large headquarters one of the most challenging environments to secure. Since more than half of all security threats come from inside the corporate network, the Secure Multimedia Solution uses a Secure Multimedia Zone to protect IP Telephony and multimedia application servers. This Secure Multimedia Zone shields the organization from internal security threats and any external threats that penetrate the network perimeter firewall.

The Nortel *Secure Multimedia Controller* is the most convenient way to establish a Secure Multimedia Zone. A security appliance with built-in VoIP application firewall, the Secure Multimedia Controller protects Nortel’s IP Telephony and multimedia servers by creating a near-instant Secure Multimedia Zone. By automatically establishing a Secure Multimedia Zone, the Secure Multimedia Controller saves time, reduces effort and eliminates the risk of configuration errors.

The Secure Multimedia Controller not only protects multimedia servers against attacks, but also provides an architecture that powers current and future encryption technologies. Encrypted signaling prevents the monitoring of call signaling, while authentication keys allow IP phones to authenticate servers, preventing man-in-the-middle attacks from any impostor servers that send false signals to the phones.



The Secure Multimedia Controller can not only be deployed in a redundant configuration, but can also be deployed in conjunction with a Nortel *Application Switch*, which adds the capability of SIP load balancing, failover re-direction and geographic redundancy to form a high availability secure multimedia solution.

#### Q5. How can I prevent attacks from occurring on the user LAN and affecting my VoIP and multimedia communications? (*Threat Protection System*)

**A5.** Nortel’s *Threat Protection System* provides “Day Zero” protection against network worm and distributed Denial of Service (DoS) attacks.

For an added layer of protection, the Nortel Threat Protection System can be added to the headquarters user network or core network that surrounds it. The Threat Protection System provides early detection and protection against not only known threats, but also “Day Zero” attacks. The system recognizes attack behavior and applies policies to stop DoS and other attacks from occurring on the user LAN.

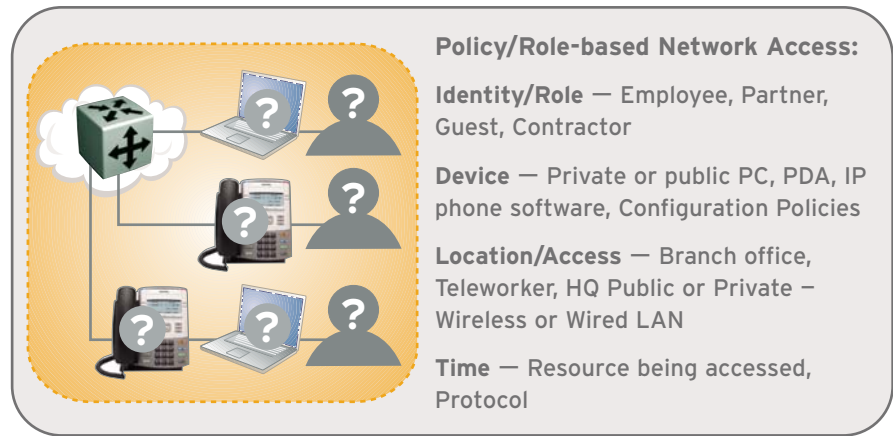
The Threat Protection System patrols and monitors user LANs for suspicious activities, blocks new attacks and provides full active threat protection for the multimedia services. Since the Threat Protection System is out of path, it is able to provide security without introducing any delay that would lower service quality.

In addition to the Threat Protection System, the Nortel *Secure Network Access* solution can continuously scan all network endpoints, ensuring that only those devices with the latest security patches and approved configurations are allowed to have network connectivity. Any non-compliant endpoint is connected to a “remediation LAN”, where users can be instructed to download appropriate software patches and make necessary configuration changes to remain compliant with corporate security policies and be allowed back onto the user LAN.

**Q6. How do I prevent unauthorized clients and endpoints from accessing my IP network and possibly gaining access to my IP Telephony and multimedia communication services? (Secure Network Access Solution)**

**A6.** An important aspect of secure multimedia communications is securing communication endpoints. This requirement is critically important for a wide range of users such as mobile workers, road warriors, home-based office workers, branch offices and headquarters.

The Nortel *Secure Network Access Solution (NSNA)* secures multimedia endpoints such as IP Phones, PCs and PDAs in two ways. It uses standards-based IEEE 802.1x Extensible Authentication Protocol (EAP) and Nortel's *Tunnel Guard* technology to connect devices from remote locations as well as local wired and wireless networks. Once authenticated, endpoints can be assigned automatically to a virtual local area network (VLAN) and controlled by user-oriented policies.



NSNA also interrogates devices to verify compliance with organizational security policies, such as the latest firewall and virus software definitions. If a device does not meet security policy, it can be placed in a remediation VLAN until the device becomes policy-compliant.

Nortel is working with Microsoft and Trusted Computing Group to ensure comprehensive, policy-based security that will provide consistent endpoint security coverage across not only PCs, but also IP Telephony hardware, accessing the network via wireless LAN, VPN and multi-vendor standards-based wired and wireless IP networks.

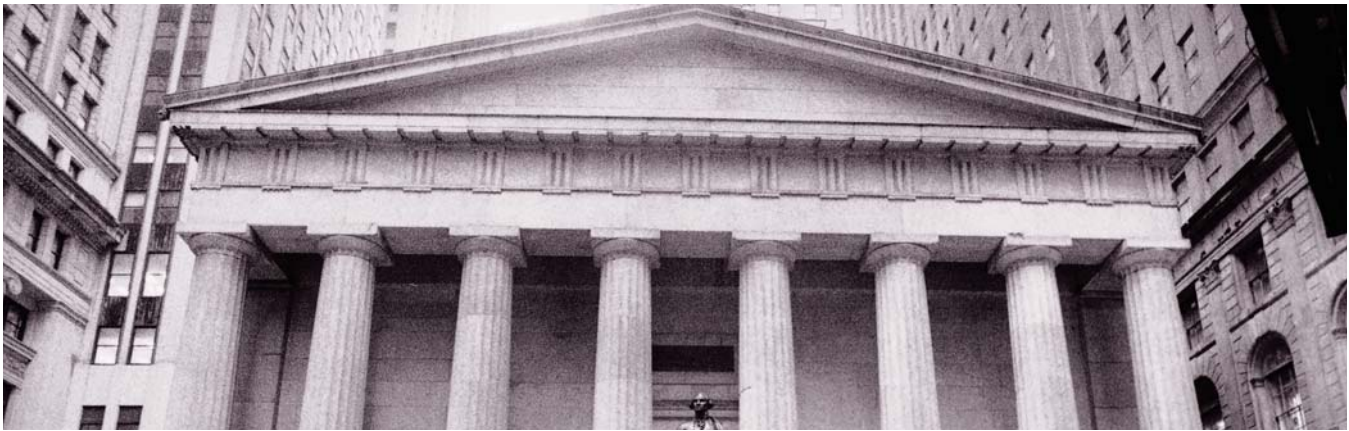
**Q7. How can I prevent man-in-the-middle attacks and impostor servers or clients? (Authentication, Encryption)**

**A7.** *Nortel Secure Network Access* prevents unauthorized endpoints from joining the network, limiting the ability of untrusted or non-compliant PCs and devices from joining the network.

*Secure Multimedia Controller* has the capability of providing encrypted signaling between servers and IP phones. This helps to prevent tampering or manipulation of the signaling by any endpoint that somehow gains access to network infrastructure between the server and an endpoint. While most other vendors concentrate on stopping impostor IP Phones, there is an even bigger risk of a PC attempting to impersonate the IP PBX server, controlling not just one phone, but an entire system of phones. The Secure Multimedia Controller is able to address this risk by enabling IP Phones to use digital certificates to authenticate where VoIP signaling is coming from, allowing IP Phones to distinguish between valid and impostor signaling.

Multimedia servers face threats not only from outside the corporate network, but also face a far greater threat from internal users whose PCs and workstations have greater access and bandwidth to provide bots, worms, viruses and other 'malware'.





**Q8. How do I prevent manipulation of IP Phones?** (*Hardening, Authentication, SMC, Tamper-Proofing/Passwords*)

**A8. Physical attacks of the phone:** IP Phones need to be protected from manipulation from a variety of sources — from the physical phone itself to the network interface that connects that phone to the network. At the physical phone, Nortel's *IP Phone 1100 series* can prevent casual end-users from accessing or changing the configuration of an IP Phone by password-protecting the phone's configuration, requiring an installer to enter a passcode before changing any local settings on the phone.

*O/S and USB expansion attacks:* The phone itself runs a hardened operating system. Firmware checks and secured firmware downloads prevent outdated or non-compliant phones from attaching to the VoIP network. The USB expansion port does not have "plug-and-play" capability, so only authorized USB devices can be attached to the phone.

*Server and signaling attacks:* The *Secure Multimedia Controller 2450* uses 128-bit AES encryption to encrypt signaling to and from the phone. This prevents modification of any signaling coming to or from the phone. The IP Phone can use strong authentication to verify where signaling is coming from (using a 1024 bit RSA private key), so that it does not accept false signaling coming from an impostor server.

*Network-based attacks:* Nortel's Threat Protection System's Intrusion Detection functions can detect IP network-based attacks, and prevent them from affecting VoIP services. Nortel *Secure Network Access* endpoint security prevents unauthorized devices from impersonating an IP Phone.

**Q9. How do I prevent Denial-of-Service attacks from affecting my communications?** (*SNAS, SMC, TPS*)

**A9.** At the IP-PBX server, the *Secure Multimedia Controller* shields the servers from the effects of denial-of-service traffic, helping ensure that services are still available and being provided to end-users.

At borders between different zones of trust (such as connections between organizations, departments, business partners and Internet-based users), Nortel's *Switched Firewall* and integrated firewall products keep bad traffic from flowing from one part of the network to another, limiting the scope of an attack to a specific network area. These advanced firewall products understand multimedia protocols such as Session Initiation Protocol (SIP), H.323 and Real Time Protocol (RTP) at the level necessary to secure VoIP and multimedia services, and provide security and Quality of Service (QoS) at the performance levels necessary for high-quality voice and video communications.

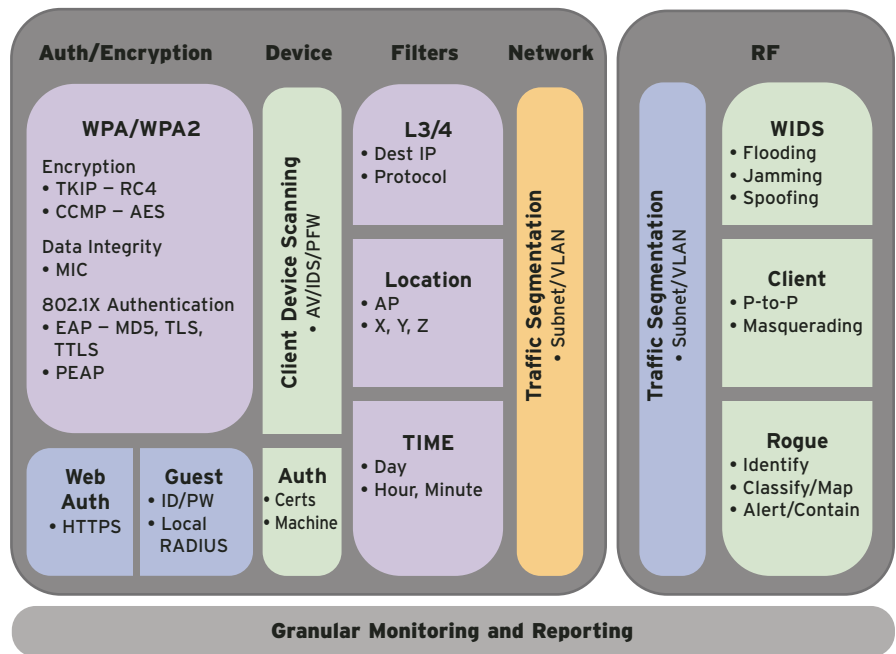
Within the user networks, the Intrusion Detection Sensors of Nortel's *Threat Protection System* identify attacks based on signatures, as well as behavior, providing "Day Zero" protection against attacks. Attack traffic can be blocked at the source, and infected machines can automatically be removed from network access.

**Q10. How can I secure multimedia and IP Telephony on my Wireless LAN?** (*WLAN Security Switch, NSNA*)

**A10.** Nortel's *WLAN Security Switch* provides centralized security for WLAN networks. Centralization of security is important in order to provide consistent security policies uniformly applied across all access points. Centralization also speeds the roaming process for IP Handsets, since the network can understand that someone simply moved, rather than independent APs that start security and authentication processes from scratch every time someone moves within coverage. This centralized architecture will also play an important role in identifying the physical location of attacks (for example, an intruder attempting to access the WLAN from a particular parking space), as well as potentially in the future locating WLAN Handsets that may be placing emergency calls (for example: E911 services in North America, 112 in Europe).

For basic and intermediate levels of wireless security, Nortel's WLAN portfolio offers a wide range of standards-based wireless security features (see diagram).

For those customers wishing the highest levels of security, the *WLAN 2212 IP Handset* features a built-in Nortel *IPsec VPN client*. This allows all wireless communication to and from the handset (voice, as well as data/application access) to be sent through a secure, authenticated, encrypted tunnel. With the *WLAN 2212 IP Handset*, the *Wireless LAN Security Switch* can be set to only allow authenticated IPsec traffic to reach the corporate network through wireless LAN access — this is the same type of rule commonly applied to remote users for remote access from the Internet, meaning that the Wireless LAN can be set to the same trust-level as the outside Internet. In addition to the Wireless LAN handsets, Nortel also offers a variety of multimedia software clients for PCs, PDAs and smartphones that can be deployed with VPN encryption technology.



**Q11. How can I secure communications to my remote teleworkers or road warriors?** (*IPsec, SSL, VPN*)

**A11.** Nortel's award-winning VPN technology is optimized to provide access for remote Internet users not only to data applications, but also to voice and multimedia communications. IPsec VPN clients provide access to corporate client devices, while SSL-VPN access can provide access for employees using their own devices or public kiosks. Nortel *VPN Gateways* provide access to both types of technology in a single easy-to-manage device. Regardless of which type of connection (IPsec or SSL), Nortel's *Tunnel Guard* technology provides the ability to ensure that all endpoints are compliant with corporate security policies (operating system updates, application and software patches, allowed/disallowed software, virus/firewall condition and configuration policies). Nortel's remote worker solutions are also compatible with centralized two-factor authentication systems, helping to ensure that only authorized users are at the other end of these remote devices.



## **Q12. How can I secure communications to my branch offices?** (*Secure Router, VPN Router, BCM*)

**A12.** Nortel provides a number of ways to secure communications with branch offices. For an integrated solution available even to small businesses, Nortel's *Business Communications Manager (BCM)* has integrated IPsec VPN technology, providing a single-box solution that not only supplies voice and multimedia communications, but also secures both voice and data communications between branch offices and headquarters. This VPN technology can also provide a secure channel for securely managing branch office equipment from a remote location.

For sites larger than those served by BCM, Nortel has a number of branch office solutions, depending on needs. The VPN Router supports a large number of encrypted tunnels between locations, while the Nortel *Secure Router Series* provides secure branch communications with a number of features that optimize performance for multimedia communications.

An additional option is the High Availability Secure Multimedia Solution, featuring the Nortel *Application Switch* and *Secure Multimedia Controller* working together with features such as geographic redundancy to ensure that branch offices remain secure and in service during a disaster recovery/failover scenario.

## **Q13. How do I prevent eavesdropping and protect privacy of communications?** (*VPN, Encryption, SMC, VLAN, Ethernet Switching*)

**A13.** Protecting against eavesdropping is more than simply encrypting voice communications. In order to fully protect communication privacy, there are several areas that need to be protected.

*Infrastructure* — Infrastructure should be fully switched where possible, preventing end users from seeing traffic not addressed to them. LAN switches such as Nortel's *Ethernet Routing Switches* ignore gratuitous ARP signals and other tricks that end-devices can use to confuse a LAN switch into "leaking" packets onto other ports. Management and troubleshooting functions such as traffic steering or port mirroring need to be secured from general access, and physical access to wiring closets needs to be restricted to prevent end-user manipulation.

*Authentication* — Endpoints need to be authenticated. Nortel *Secure Network Access* keeps invalid, corrupted or unauthorized endpoints from joining the network and potentially compromising security. IP Phones need to authenticate servers so that they do not accept any false signals sent from impostor servers that may be attempting to trick them into breaching privacy. Proper authentication is an important pre-requisite to encryption, since encrypting to an unknown, untrusted and unverified endpoint does not improve security.

*Signaling encryption* — Secure Multimedia Controller allows VoIP signaling to be encrypted, to prevent manipulation or interception of signaling by system administrators or anyone with physical network access between the endpoints and servers. Encrypting the signaling is generally more important than securing the media path, since signaling is control-oriented, and generally all flows towards a single server with a more predictable path. Without signaling encryption, unauthorized endpoints intercepting signals could capture passwords to applications (including unified messaging/voice mail and SIP collaboration). Endpoints without signaling encryption can also be vulnerable to man-in-the-middle attacks and social engineering attacks, where an unauthorized endpoint takes control of a user's phone by manipulating the control signaling that tells the phone what to display or what audio to play.

*Media path encryption* — Nortel plans to implement standards-based SRTP (Secure Real Time Protocol) in upcoming versions of our communication systems, gateways and applications. Media path encryption will be supported in a firmware update to Phase 2 IP Phone 2000 Series, as well as the IP Phone 1100 series. Phones with updated firmware will feature an indicator on the display screen of the phone informing users when their call is being encrypted.

We are also driving the standards committees that are creating a standards-based way to securely distribute and exchange per-session encryption keys. This will allow large-scale encrypted systems without the need to manually enter long encryption keys when installing endpoints. This will also promote better industry interoperability with future third-party applications and service providers.

*Secure applications and core features* — Both gateways and multimedia applications themselves need to be secure. When encrypted and unencrypted endpoints communicate, some indication needs to be given to the secure user that they are

having an unencrypted conversation. Multimedia communication applications need to support different levels of user restrictions and control access to recording/monitoring/troubleshooting features. Traditional anti-toll fraud capability needs to be extended and enhanced to cover IP communications (for wired, wireless and remote IP users). The applications and operating system of the application servers need to be hardened and secured. Non-voice information traveling between VoIP endpoints (i.e. data applications on IP Phones) may also need to be authenticated, encrypted and secured.

*Secure collaboration and conferencing* – Sitting squarely between low-risk internal IP calls and high-risk Internet and wireless calls is an environment especially prone to snooping: meet-me collaboration and conferencing. Access to conference calls is traditionally controlled by an operator or passwords sent to participants; anyone who learns the password through social engineering (impersonating someone claiming to have misplaced their password) or by picking up a wayward invitation printout can dial in. While some systems have limited chairperson controls via phone keypads, these controls are hard to remember and seldom used. Nortel's *Multimedia Communication Server (MCS) 5100* meet-me collaboration provides easy-to-use conferencing security features through a chairperson visual control panel, allowing the chairperson to track who has joined or dropped off the call, and can even require people to revalidate through a secondary password. These features make conferencing and collaboration significantly more secure than older audio-conference environments.

#### **Q14. How does Nortel ensure their communications platforms are secure? (SATF)**

**A14.** Nortel secures communication platforms at several levels. Most systems run on hardened operating systems, such as VxWorks (a realtime operating system), Nortel carrier-grade Linux or embedded versions of MS Windows (customized hardened builds with all unused parts removed). Within these systems, audit trails report operating system and administrator activities, and watchdog timers that automatically reset portions of systems minimize the effects of attacks affecting system components.

*Proactive vulnerability management:* The main goal of proactive vulnerability management is to stay ahead of the emerging threats that might pose a risk to Nortel's customer networks, and ensure that customers are not overwhelmed by the flood of irrelevant information. Each component and software release undergoes thorough security testing with a library of security assessment and exploit tools. Security vulnerability testing utilizing industry-accepted best practices is performed on each software and hardware build.

*Reactive vulnerability management:* A multi-functional vulnerability management team (Security Advisory Task Force) is in place to assess each incoming vulnerability in terms of impact to customers. The team assesses the vulnerabilities, tracks them and engages resolution process to drive them to closure as required. This includes validation of security updates and patches from operating system suppliers and a wide variety of industry groups focused on security. Nortel issues timely bulletins to notify channel partners and customers of any critical security patches if they prove necessary. For example, enterprise multimedia applications compatibility with Microsoft critical patches are validated, with advisories provided within 48 hours from the time they are publicly announced.

#### **Q15. How do I secure access to system management capabilities? (Out-of-band management, password policies, VPN)**

**A15.** System management capabilities can be secured at several layers.

On the people-level, organizations need to know which administrators should be trusted with which levels of access. Applications need to provide multiple levels of access, rather than trusting all administrators with access to all parts of the system. For example, a technician may only be allowed to move or modify a phone, but it may take a higher-level administrator to authorize a phone for unlimited access to international calling.

Most systems have out-of-band management capabilities, where management data and access can be physically restricted to a separate network. These features are even available on very small systems, such as the BCM 50. Access to this separate management network can be completely physically isolated, or can be accessed via secure VPN technologies, depending on organizational policies. Requiring VPN authentication can also secure remote management access of branch equipment from offsite.

In addition to multiple access levels and out-of-band management access, audit trails can be used to record administrator activities, including software modules accessed, etc. Alarm reports also can notify administrators of attempts to access management interfaces.

**Q16. What measures are available to protect me from toll fraud, both via traditional means and via IP and wireless networks?**

**A16.** Toll fraud has always been a concern of telephony systems, and this “theft of service” is still a concern with VoIP systems.

**Application-level protection:**

Various features in the telephony applications can be used to restrict users or devices to levels of service for which they should be authorized to access. These features can restrict calling to inside-only, emergency calling only, no long distance or other levels. These restrictions can also be set on a time basis (different rules for business hours, weekends, etc.). Authorization codes can be required to access different levels of services by different users.

The Call Detail Recording feature can be used to track usage, including calling and called parties, time and duration of a call. Tracking authorization codes allows toll fraud detection from both inside and outside sources.

Call re-direct and routing features such as DISA and Call Forward can be restricted (inside-only, no long distance, etc.).

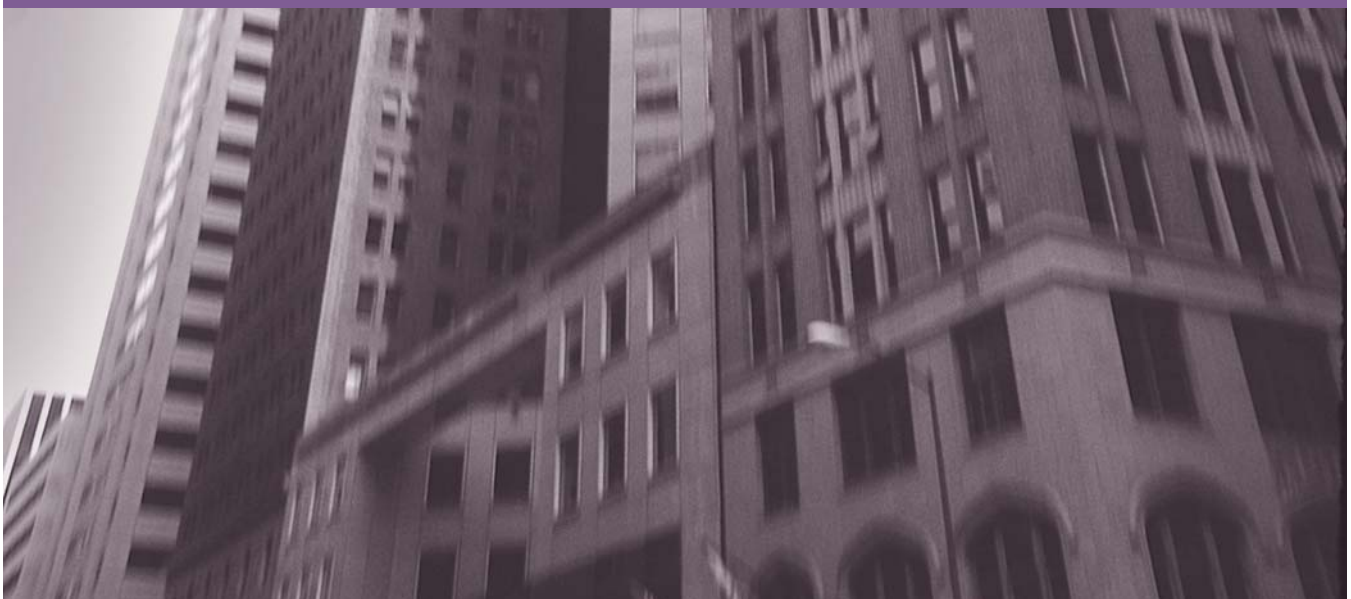
Applications can be set to secure accounts via strong passwords, password aging and similar access policies.

**Infrastructure-level protection:**

At the IP infrastructure level, Intrusion Detection systems such as those found in the *Threat Protection System*, wireless security such as that found in the WLAN Security Switch, and endpoint security such as that found in the Nortel *Secure Network Access* can help to keep IP-level attacks from stealing service and committing toll fraud. Encrypted and authenticated signaling, as found in the *Secure Multimedia Controller*, also prevents monitoring of call activities by unauthorized parties. Secure Routing and Ethernet switching, VLAN and VPN technologies can partition network devices and users from monitoring usage activities on the network.

Features such as *Communication Server 1000 Telephony Manager* Call Tracking provides activity monitoring capability. This application module tracks activity in real time, and can generate alarms and notify administrators of unusual calling patterns that may indicate toll fraud. Call Tracking provides a graphical dashboard display giving a quick view of calls by origin, duration and percentage of calls meeting certain criteria.

For an added layer of protection, the Nortel Threat Protection System can be added to the headquarters user network or core network that surrounds it.



## **Q17. How do I guard the privacy of usage and billing data?**

**A17.** It can be important to guard and protect usage and billing data, as this information can contain proprietary information (such as who is talking to whom), as well as information that can be used to discover security issues such as toll fraud.

*Server access:* At the server side where billing records are created, an audit trail is configurable to record the date, login-in/out time, user-id and software modules accessed. Failed login attempts are monitored, logged and checked against an acceptable threshold. If that threshold is exceeded, an alarm is generated and that login port is disabled for a configurable amount of time. Also, the system will notify the next administrator logging in of these failed attempts.

*O/S hardening techniques:* For the PC systems that collect, process and distribute billing reports via Telephony Manager's billing module, a variety of measures can be taken in order to secure billing records. O/S hardening techniques can be followed, as well as patch management practices, anti-virus and anti-spyware measures.

### **Billing application access:**

Within the billing application, whoever has access to usage records detail is controlled by assigning access privileges. Telephony Manager allows read/write, read only and no access choices to the Billing application at a management access level. For example, if the Telephony Manager user profile is "no access", the Telecom personnel assigned this access profile will not even see that there are Billing Application reporting tool features.

Another useful feature in Telephony Manager is the ability to schedule tasks and log out. So if your workspace is in a public area and you need to start processing a special billing or usage report that is not one of the regularly scheduled reports, you can begin your reporting tasks or even schedule the tasks for a specified hour and log out of Telephony Manager before leaving your work area.

### **Physical security and policies:**

One would also typically install the Telephony Manager PC Server behind locked doors in the switch room or data center as one would not wish a PC server containing potentially sensitive data such as the collected CDR to fall victim to theft. Of course "policy" also plays a factor in guarding privacy of usage and billing data. If reports or data are archived to CD or DVD, one should be sure to keep the archived media properly locked away in a cabinet or locked drawer. Printed reports should also be shredded or archived media properly destroyed when disposed of. It may be a company's legally permitted policy for managers to review communications systems usage. In fact, letting employees know that their calling activity can be monitored with reports is often enough of a deterrent to prevent "time abuse" and keep employees productive — employees who might otherwise spend too much time on the phone on non-business related matters. In fact, where most companies once had Call Accounting application software to bill back toll calls to departments, with today's very low toll costs or network bandwidth cost, most companies are now instead purchasing Call Accounting application software such as the Telephony Manager Telecom Billing System as a deterrent to "time abuse", which can be far more expensive than the actual cost of a call.

## **Q18. How do I ensure the privacy of my voice mail and unified messaging systems?**

**A18.** Nortel's *CallPilot Unified Messaging* systems are secured at many levels.

*Hardened operating system:* Regular security updates are distributed periodically by Nortel ([www.nortel.com/support](http://www.nortel.com/support)). These updates include any security updates to the operating system, as well as the application, and are tested and bundled by Nortel for easy installation. Unused operating system modules and user accounts have been removed in order to maximize reliability and security. Strong password enforcement is also available and recommended.

*Anti-virus:* CallPilot is protected against viruses and network worms by supporting standard anti-virus software, including Computer Associates eTrust InoculateIT, McAfee NetShield, Symantec Norton Anti-Virus and Trend Micro Server Protect.



Nortel's *Threat Protection System* also helps to keep viruses and worms from spreading through the corporate network, and Secure Multimedia Controller helps to protect servers from DoS and other server-targeted attacks.

#### **Secure clients/communication:**

MS Exchange/Outlook, Lotus Notes and Groupwise CallPilot clients support CRAM MD5 challenge response authentication to minimize the risk an unauthorized agent could “spoof” being the user. SSL encryption can optionally be used to prevent unauthorized access to messages through “sniffing” on the network.

Internet Mail Clients such as Outlook Express and Netscape Messenger support SSL for message send/receive and address book lookup. When IMAP clients are configured for SSL, certificates are used to allow the client to authenticate the server (preventing impostor servers), and for the server to authenticate the client (preventing user-spoofing) before encrypted communications (preventing eavesdropping) are held. (Eudora Pro doesn't support SSL.)

Web Messaging users can access the MyCallPilot web user interface via Nortel's *VPN Gateway*, which allows granular access to various applications.

**Secure storage:** Messages are stored in a specially encoded Nortel format, allowing not only for maximum compression, but also preventing the easy decoding of the message database by anyone who gains physical access and removes the server disk drive.

#### **Q19. How can I prevent unauthorized moves/adds/changes to my IP Phones, and how can I ensure that my users have the correct access to emergency dial codes, such as E-911?**

**A19.** As one of the few vendors supplying telecommunications equipment to carriers, enterprises and public safety agencies, Nortel has been a leader in 911 technology development. For a detailed discussion on E-911, see the Nortel Position Paper, “Where's the fire?” (document #NN104540-082103). Nortel also supplies solutions for public safety systems in other regions of the world, such as the European Union's 112 service.

The mobile nature of IP endpoints, combined with unauthorized end-user moves, may result in the failure to locate a user dialing an emergency assistance number. Fortunately, Nortel has a number of technologies that can be used to minimize unauthorized endpoint moves (between buildings/floors, for instance).

Nortel's *Secure Network Access* technology provides comprehensive endpoint security for converged multimedia as well as data-only networks. Nortel's Secure Network Access, in conjunction with EAP (Extensible Authentication Protocol) and IEEE 802.1x standards, allows a LAN switch to dynamically check a centralized server (such as RADIUS) to see if an endpoint or user is authorized to use a specific LAN port, in a specific area.

Another solution that some organizations use to control unauthorized endpoint moves involves MAC address-based security, available on Nortel's *Ethernet Routing Switches*. Nortel's BaySecure™ LAN Access provides real-time security, safeguarding Ethernet networks from unauthorized endpoints. MAC address security blocks devices from connecting to an unauthorized Ethernet port without prior administrator approval. Nortel's Ethernet Routing Switch 5510 currently supports up to 448 allowed source addresses per port, and the Ethernet Routing Switch 5520 and 5530 support lists of up to 32 allowed devices per port.

For organizations with high levels of changes and moves, Nortel's open, standards-based systems integrate with leading-edge software from Nortel Developer Partners ([www.nortel.com/dpp](http://www.nortel.com/dpp)). Solutions such as Quovia's Location Gateway Server enables E-911 data to be gathered and forwarded to the appropriate PSAP (Public Safety Answering Point), keeping accurate location information for the dispatch of emergency personnel to an end-users' location.

Future technologies being implemented, such as IEEE 802.1ab topology protocol and new wireless standards, may allow management systems to better physically locate phones and other IP devices, and potentially some day completely automate the location tables for each phone on the network.

**Q20. What other resources are available to learn more about the Nortel Secure Multimedia Solution?**

**A20.** Check Nortel's Secure Multimedia website — <http://www.nortel.com/enterprisesecurity> (Secure Multimedia Solution is listed under Featured Products & Solutions at the bottom of the page).

Nortel also offers a variety of security services, ranging from security audits and vulnerability assessments to security architecture, planning, and implementation. (See more at [www.nortel.com](http://www.nortel.com), click on Services > Security).

**In the United States:**

Nortel  
35 Davis Drive  
Research Triangle Park, NC 27709 USA

**In Canada:**

Nortel  
8200 Dixie Road, Suite 100  
Brampton, Ontario L6T 5P6 Canada

**In Caribbean and Latin America:**

Nortel  
1500 Concorde Terrace  
Sunrise, FL 33323 USA

**In Europe:**

Nortel  
Maidenhead Office Park, Westacott Way  
Maidenhead Berkshire SL6 3QH UK  
Phone: 00800 8008 9009 or  
+44 (0) 870-907-9009

**In Asia Pacific:**

Nortel  
Nortel Networks Centre  
1 Innovation Drive  
Macquarie University Research Park  
Macquarie Park, NSW 2109  
Australia  
Tel +61 2 8870 5000

**In Greater China:**

Nortel  
Sun Dong An Plaza  
138 Wang Fu Jing Street  
Beijing 10000  
China  
Phone: (86) 10 6510 8000

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at [www.nortel.com](http://www.nortel.com).

For more information, contact your Nortel representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

Nortel, the Nortel logo, the Globemark and CallPilot are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2006 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel assumes no responsibility for any errors that may appear in this document.

