Position Paper

Where’s the fire?

The impending emergency in enterprise E911 services—for converged IP and traditional voice network environments

In North America, we expect that whenever we dial 911, emergency response personnel will be able to find us and send help quickly. But what if you’re calling from inside a private phone network—where many extensions share a few outside lines? What if you are calling from your laptop-based IP telephony client, and you are not in your office? Under those conditions, will your emergency call go to the right Public Safety Answering Point? Can emergency teams find you? Will someone on site be automatically notified? Read on to find out how technology is enabling emergency response teams to find emergency callers in the increasingly mobile world enabled by IP enterprise networks.

NORTEL NETWORKS

Executive summary

It is an expectation as well as legislation in North America that when you dial 911, you will be directed to an appropriate operator who can identify your location, access any special considerations about you, dispatch the right type of assistance to the right location, and to be able to re-establish contact with you.

For any enterprise, effective and timely emergency response by calling 911 is critical on several fronts, being simultaneously a:

- **Business imperative—**protection for valued company assets and people
- **Homeland security issue—**preventing incidents from becoming catastrophes
- **Moral imperative—**an ethical responsibility to your people
- **Legal imperative—**protecting the organization from liability caused by poor response
- **Regulatory requirement—**dictated by state and federal legislation

For residential and small business users, the North American 911 system works as advertised. It reaches 70 to 100 percent of the population, depending on where you live. With the advent of E911, PSAP operators automatically receive further information about the caller's location—generally the street address associated with the seven-digit calling number.

The story has been different if you're calling from private phone systems, such as a PBX (private branch exchange) system in an office building, conference center, hospital, or campus—where many phone stations share a few outside lines and are not necessarily uniquely identified with seven-digit numbers recognized by the phone company.

The issue is further complicated in enterprises that have adopted a converged voice/data network over Internet Protocol (IP). IP reduces the cost of enterprise networking and enables users to move around at will, to work at home or on the road, and have their enterprise-based services follow them. But what about 911 service?

Location is the biggest issue. The IP network lets you unplug from one location and plug in somewhere else, while the enterprise network finds you and follows you. But where does a 911 call placed from your mobile workplace go? Does it go to the emergency response center in your hometown? The one serving your residence? The one serving your current, temporary location? Is location information detailed enough to enable response teams to find the emergency? Who within the enterprise organization should be notified when a 911 call is made?

Nortel Networks has technology solutions today to enable enterprises to answer these questions and provide effective 911 emergency service to their users. This position paper describes how Nortel Networks addresses these issues in a converged environment.

Where's the fire?

The impending emergency in Enterprise E911 services—for converged IP and traditional PBX network environments

Help! Somebody call 911!

In 1967, the President's Commission on Law Enforcement and Administration of Justice stated, "Wherever practical, a single (police emergency) number should be established at least within a metropolitan area and preferably over the entire United States." The pre-deregulation "Ma Bell" responded, and by January 1968, American Telephone and Telegraph announced that within its serving areas the digits 9-1-1 were available for use on a national scale as the single emergency telephone number.

With basic 911 service, an emergency dispatcher automatically receives the calling number (automatic number identification, or ANI) and the billing address associated with that number.

In an emergency situation, response time depends on the accuracy and completeness of the information available to the Emergency Response Center, known in North America as the PSAP. However, in some situations, ANI is unavailable or inadequate for pinpointing the location of the caller—and the emergency.

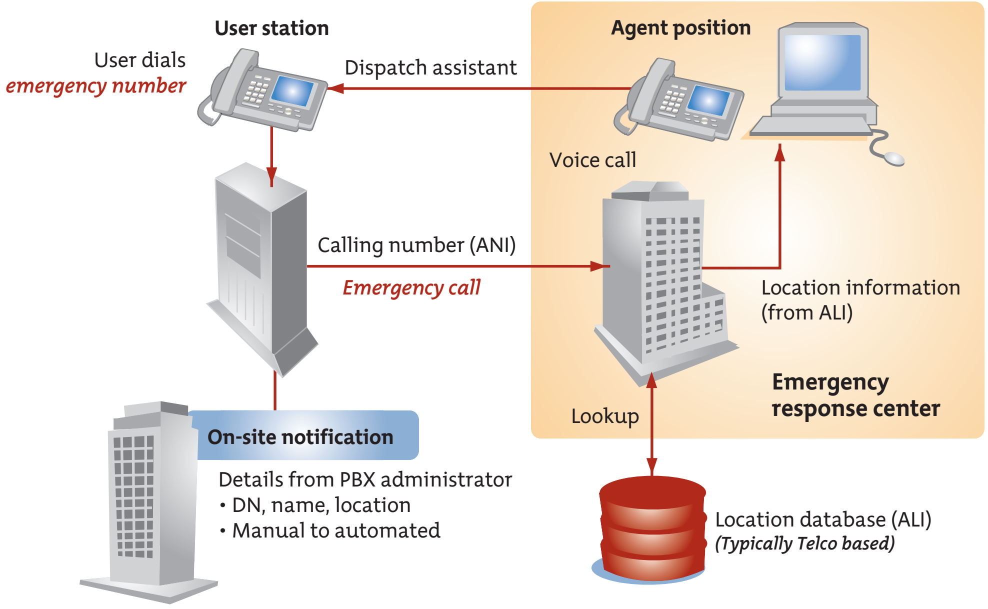

Figure 1. *PBX systems can be equipped to give the PSAP "visibility" to detailed location information about private phone stations, to provide emergency response equivalent to residential E911 service.*

Location, location, location.

Finding 911 callers within traditional TDM-based private networks

Enter "enhanced 911," or "E911." With E911, the system automatically sends the PSAP operator information about the caller's number. The telephone company's E911 system routes that number to a database of location information, to retrieve not just billing address, but also the physical location associated with the caller's telephone number. This automatic location information (ALI) is kept current in telephone company databases. So, even if you can't speak, or don't know the address, emergency operators know the location of the phone you're using, and can relay that information immediately to emergency response personnel.

However, a street address isn't much help if the 911 call comes from within an enterprise PBX (private branch exchange) network. The PSAP operator might only see the location of the main PBX equipment, not the caller's station.

PBX systems can be equipped to automatically relay not only the organization's street address, but the caller's specific location, such as "East wing, fourth floor, aisle 5, row Z." The solution is provided by a private E911 service which sends out a unique number (ANI) with every call, which identifies the calling station by means of an ALI lookup.

Automatic location identification is only one challenge to E911 services within private enterprise phone systems. What about automatic notification to on-site emergency personnel and systems? Do you provide Enterprise 911 coverage to telecommuters and home office workers? How do you ensure that whether employees dial an access code or not ("9-911" or "911"), they still get an outside connection to the PSAP? How do you synchronize your constantly changing database of employee locations with the ALI database at the telephone company?

Fortunately, technology solutions are available now to empower PBX systems to provide these capabilities.

Good corporate citizenship becomes law

Implementing full E911 capability in enterprise PBX systems is good business, good corporate citizenship, and in some states, it's the law. Illinois and Vermont, for example, already require owners of private phone switches to provide E911 service for all stations in business buildings, schools, hospitals, and hotels/motels. At the time of writing, seven states require PBX E911 capability in multi-tenant residential units. Other states and provinces are in various stages of consideration. An employer who knowingly fails to meet the requirements of the law could possibly be found negligent in a civil suit, without insurance coverage for the case.

The thrust of the legislation is to ensure that sufficiently detailed location information is available, the PSAP can call back if a call is disconnected, any station on the PBX can dial 911 without a prefix or special action, appropriate on-site personnel will be notified, and designated trunks will always be available for 911 calls.

The technology has been available for years to meet those requirements on traditional TDM-based PBX systems. But enterprise networks are evolving, and private 911 services must evolve with it.

The gulf created by convergence

Addressing E911 considerations in IP PBX environments

While convergence of voice and data services onto an Internet Protocol (IP) network has a number of significant advantages, it presents new challenges to the Enterprise 911 solution.

These challenges cover technical implementation as well as re-visiting 911 policies in a converged network.

In a converged voice and data communications environment, privately managed IP networks and the global Internet extend services to local, remote, and mobile users.

Even though state and federal legislation is being formulated for enterprise E911 services, E911 calling standards for IP telephony are still in the early stages of being defined. Pending and recent legislation in North America does not yet address the nuances of convergence, but it is happening.

The Federal Communications Commission (FCC) has demonstrated growing interest in establishing 911 requirements for IP telephony. At minimum, converged IP and wireless networks will be expected to match the required E911 functionality of wired private phone networks, such as unrestricted access to 911 from any phone, routing to designated trunks, sending the calling station's ANI with the call, and on-site notification.

In short, although the underlying network that supports communication may be fundamentally changing, users' requirements for prompt emergency response have not. Network administrators must consider several factors when extending E911 services into an evolving, converged network environment.

The way users use the network has irrevocably changed. Convergence makes it possible to present users with a personalized telephony experience. As a result, the emergency response system must handle a dramatically increased variety of call scenarios. Those calls could come from traditional phones, IP desktop phones, PCs equipped with "softphones," wireless devices, or other IP-enabled devices. Callers could be using their IP client from their regular office, conference room, home office, high-speed train, or anywhere a jack is available to connect to the Internet—or a signal is available for wireless connectivity.

These factors will stretch the boundaries of what emergency response capabilities will be required, and how they can be offered.

Enterprise networks will be heterogeneous for the foreseeable future. TDM and IP telephony infrastructures will likely coexist for some time, while migration to an all-IP environment takes place in phases. That means the enterprise must provide consistent emergency response service regardless of the underlying infrastructure carrying the 911 call.

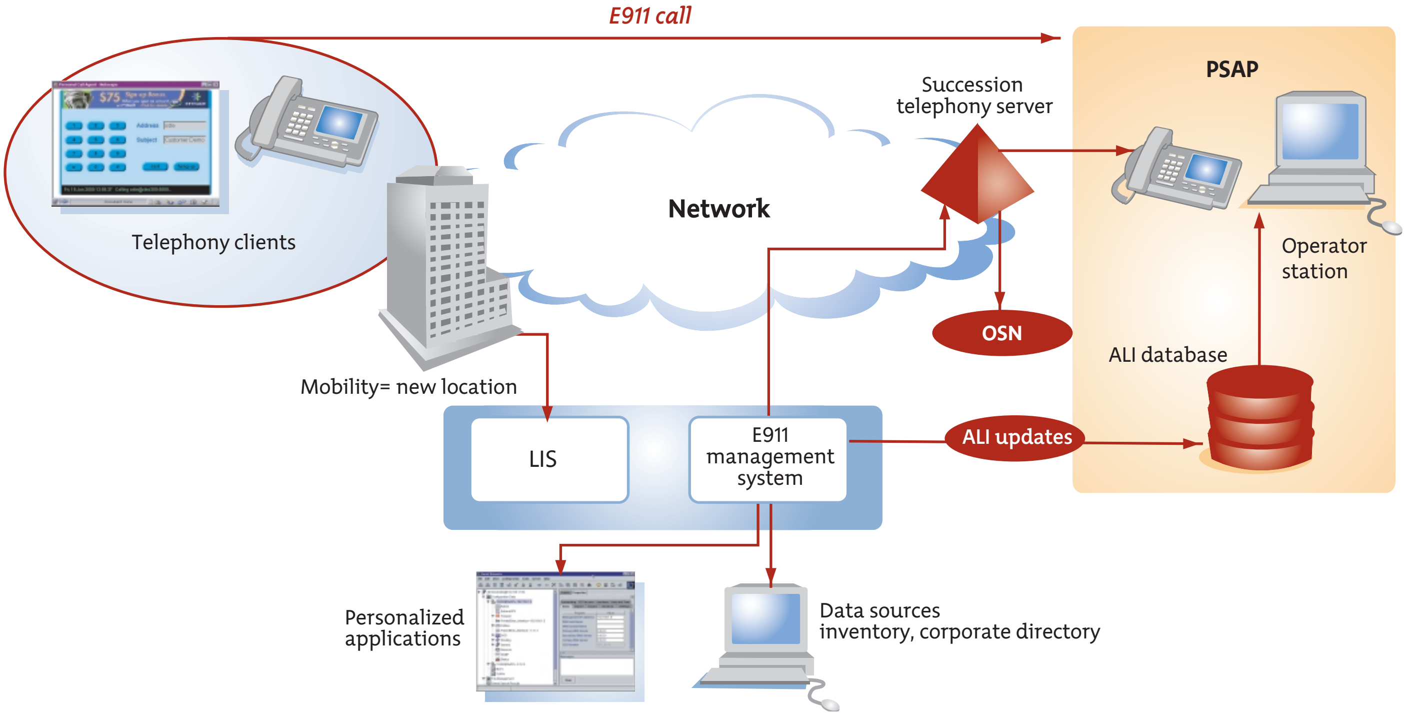

Figure 2. *With regular discovery of adds/moves/changes, and auto-discovery of mobile users' current locations, enterprises can provide effective E911 service in hybrid or pure-IP network environments.*

Furthermore, while new converged private networks use IP, North American E911 networks have been built on the public switched telephone network (PSTN), which uses completely different schemes for identifying communication ports and stations, and for transmitting call information such as ANI and ALI. The PSAP can only accept and work with information that conforms to PSTN standards. That means whether the enterprise uses a traditional PBX, IP-enabled PBX, or pure IP voice-and-data network, it still must comply to PSTN signaling standards to support 911 services.

The National Emergency Number Association (NENA) has recently submitted proposals for IP-based PSAP infrastructure, but the prevailing PSAP architecture will likely remain PSTN-based for some time.

Policy and engineering issues must be addressed in tandem.

The private E911 solution must provide functionality equivalent to its TDM predecessor and be compliant with state and federal legislation. However, the user scenarios in a converged network significantly increase, and it is necessary to revisit the Enterprise 911 policy. Should the policy include support for enterprise road warriors in a hotel conference room? It may not be in the user's or the enterprise's best interest to attempt to do so given the difficulty in locating a user outside the enterprise perimeter and routing the emergency call. Educating users on the right action to take in such a scenario (such as using a wall phone) and educating enterprise personnel on how to respond to a call becomes important.

The following is an overview of the components to enable emergency services in a converged environment.

Location, new location, new location.

Tracking the elusive user in highly dynamic, mobile IP environments.

A key benefit of IP is its flexibility and mobility. An IP network lets you unplug from one location and plug in somewhere else, while the enterprise network finds you and follows you to maintain your identity. It supports telecommuters and road warriors, as well as offices that move from month to month. But where does a 911 call placed from your mobile workplace go? How does the system recognize where a user is in real time and respond appropriately?

The flexibility of a converged network is one of its biggest advantages, but it makes it difficult to keep up with users' constantly changing locations, and to keep public ALI databases current to reflect all those adds, moves, and changes. Enterprises need a way to streamline the process of gathering, updating, and disseminating location information so accurate E911 location services can be delivered to users in fixed locations, remote offices, at home, or from transient locations.

Specifically, the Enterprise 911 system must be able to handle several types of mobility:

- **Keep track of your location as you move from building to building,** anywhere in the enterprise, taking your IP "softphone" (typically a laptop computer equipped with IP telephony software) and all its features, with you.
- **Keep track of adds/moves/changes** when a user's fixed desktop phone or desktop PC with "softphone" are moved to a new office location.
- **Keep track of your location in a "virtual office,"** when you log in from anywhere and any compatible device, and access your personal network features as though you were at your home location.

In short, to keep up with user-initiated changes—unplug from here, plug in somewhere else, switch on demand from one device to another, work at home or on the road—the Enterprise 911 system must dynamically locate that user across a broad range of possible locations, access devices, and network infrastructures. Let's take a look at how E911 service is achieved for these three mobility scenarios.

Keeping track of mobile users in the multi-location enterprise

One day you and your IP softphone might be in the San Francisco office, the next day in the building across the street, and in two different New York offices on the third day.

The user's location might be determined by a number of different techniques, each of which have their advantages in particular call scenarios, client types, and enterprise policy—and one technique is not likely to cover all. As a result, the emergency response solution must be able to support different mechanisms.

Some examples of these techniques are:

- Administrative configuration, such as assigning direct inward dial (DID) numbers at a very granular level
- Dividing up enterprise locations into physical zones known as "emergency response locations" (ERLs), and auto-discovering the ERL or asking the user to select a location profile when logging in
- Location Information Service (LIS)—Network discovery technology which itself has several techniques:
  - Capturing SNMP traps when the client is first plugged into the new location
  - Using Smart Panels, which are inline patch panels that maintain an up-to-date inventory of what is plugged into them
  - Using Global Positioning System (GPS) to identify the current location of the IP device
  - Discovering via DHCP and utilizing subnet for emergency zone

The E911 system can then correlate that trap or notification to a pre-established database of wiring plans or physical addresses, such as building floor, floor partition, or room number.

For example, let's say you left your San Francisco home and arrived in the New York office. When you plug your soft-phone-enabled laptop into an outlet in the New York office, an LIS recognizes a change of state in the outlet, identifies the IP device that's just been plugged in, and relays this information to the E911 system. If you called 911 from this location, the call server would handle the call (trunk selection, ANI, and on-site notification) as appropriate for your current physical location (the New York office), not the San Francisco location associated with the IP device.

Another key consideration is determining what the Enterprise 911 policy must encompass to balance servicing the user with feasibility of providing that service.

Keeping track of adds/moves/changes

While real time mobility/portability is most often thought of when the issue of location updating and E911 is discussed, adds/moves/changes are a significant administrative cost to the enterprise.

A key advantage of IP is that it is so easy to set up and take down semi-permanent connections to meet changing requirements of project teams and departments. The greater number of adds/moves/changes requires that enterprises adopt more efficient ways to capture new location information and relay it to the PSTN provider to update ALI databases.

Fortunately, the same location discovery techniques previously discussed for tracking mobile users can be leveraged administrative adds/moves/changes. This means that while addressing the evolving 911 requirements as a result of convergence, administrative costs from adds/moves/changes can also be reduced.

However, because we're changing the long-term location of the user, rather than marking just a transient location, the 911 system would also supply this new location information to the PSTN provider to update the ALI database. Since this is typically a component of a planned administrative process, real time updates of the ALI database are not necessary.

Keeping track of mobile users in the "virtual office"

Succession 1000 Virtual Office capabilities empower users to enjoy a personalized network experience from access devices that are not their own. You could walk into someone else's office anywhere in the enterprise and log onto their IP-telephony-equipped computer or IP phone as yourself. Their IP device now performs just as though it's yours, and provides your usual portfolio of calling features and customizations.

Since Virtual Office enables you to use a foreign access device just as if it were your home access device, you can call someone in your home territory as a local call, even though you might physically be across the country. In this scenario, the 911 system needs a way to differentiate your identity (needed for purposes of providing consistent calling features regardless of physical location) versus your real, physical location, required for purposes of dispatching emergency assistance.

Nortel Networks addresses this issue by using intelligence in emergency system software to re-route emergency calls to the local call server, rather than the home call server that supplies the user's "virtual office" capabilities. ALI updates are not necessary for tracking these transient, mobile locations.

Suppose you're physically in the New York office yet logged into your San Francisco-based "virtual office." The call server in San Francisco is handling your voice and data calls, but when you dial 911, that call server passes the call to the New York call server for trunk selection, routing, and on-site notification appropriate to your real location.

Keeping current: Interacting with the PSAP

Sending E911 calls. In a converged environment, the primary routing for 911 calls continues to be via CAMA (Centralized Automatic Message Accounting) analog or ISDN digital trunks, in order to deliver ANI information to the emergency services dispatcher.

The Enterprise 911 system determines the user's current location and assigns an Emergency Location Identification Number (ELIN) corresponding to the number representing that location. This is provided to the PSAP and the dispatcher is presented with the current location (determined from ALI reference) as well as the call back number (ANI). NENA has issued proposals for IP-based PSAPs, but this is not reality yet.

Updating the PSAP ALI database. As we discussed in the generic 911 description earlier, ALI describes the physical location associated with the caller's telephone number—which must be kept current in telephone company databases. In today's enterprise environment where adds/moves/changes are frequent and made easier by IP, ALI is constantly changing, which greatly increases the challenge of keeping the PSAP ALI database up-to-date. This interface between the enterprise and PSAP ALI database is defined by published standards, but the reality is that implementations differ quite substantially—from PC utilities and e-mail, to fax and automated systems. The choice of method depends on the local service provider and the complexity of managing updates within the enterprise.

The Nortel Networks Succession* development group continues to work with technology associates to provide the necessary interfaces and information for automating ALI database management. Innovators such as RedSky, Teltronics, and Xtend provide value-added E911 management applications that help the enterprise manage administrative activities pertaining to location discovery and ALI database maintenance.

Letting your own people know: On-site notification (OSN)

On-site personnel require immediate notification of an emergency situation. The receptionist, front-gate guard, security office, and facilities personnel, among others, could very well be instrumental in responding to and/or containing the emergency. On-site personnel can meet the response team to assist with location-specific information, as well as take appropriate action (such as evacuation of a building) to lessen the impact of the emergency. On-site notification (OSN) can be even more critical in IP environments, because users are more mobile.

With the Nortel Networks Emergency Services Access (ESA) feature today, an on-site alert is delivered to a designated OSN set or terminal, which buzzes and flashes a key lamp when a 911 call is detected. When the OSN key is pressed, caller information, such as caller and calling number information, is displayed on the set and printed on a designated display terminal as soon as the 911 call goes to an outgoing trunk.

On-site notification with caller information can also be sent via alternate means such as Instant Messaging (IM). Nortel Networks provides this functionality for converged environments today, and is adding more capability through integration with technology associates such as Teltronics OSN solutions.

Take advantage of third-party solutions: open interfaces

In any enterprise, the emergency response system is tightly coupled into the operational environment, and can benefit from a variety of third-party solutions that offer value—added functionality. Therefore, the E911 system in a converged network must provide open interfaces to support use of:

- A choice of LIS (Location Information Services), such as Smart Panels or GPS
- Import and export of information to third-party systems, for such capabilities as ALI database management systems and on-site notification

Nortel Networks private E911 solution for Meridian* PBX environments has always provided open interfaces for integration with third-party databases and solutions.We continued that tradition in our enterprise portfolio for converged networks.

Protecting the protector: E911 system security

The core of an enterprise emergency response system is a database with sensitive information about your users, their locations, access privileges, and more. Furthermore, its functions must always be available when needed in an emergency. Yet network convergence—which typically includes opening the private network to connections from the public Internet—presents some new concerns for protecting the security and integrity of all enterprise network systems, E911 included.

Enterprises have a serious responsibility to prevent unauthorized access to information, Denial-of-Service (DoS) attacks, and corruption of E911 service. That means all interfaces into the system as well as the information itself must be secured. It is also important to generate an audit trail or history of emergency calls. This is not only useful in post-event analysis of an emergency situation, but may be crucial in legal situations.

Nortel Networks Enterprise Succession networks can be protected by our Unified Security Architecture, which delivers comprehensive security capabilities covering all aspects of enterprise networks and services:

- **Protection for confidential data in transit—**Virtual private networks and virtual local area networks protect data through encryption, tunneling, segmentation, dynamic routing, and more.
- **Perimeter defense—**ICSA-certified stateful firewalls protect a network or its nodes against unauthorized users.
- **High availability and redundancy —**Load-balancing, hardware/software redundancy, and failover mechanisms provide premium uptime and recovery time.
- **Authentication and intrusion detection—**Integration with third-party systems provides verification of users and acceptable utilization.
- **Audit trails—**Detailed history logging of all caller and administrator activity and system events can identify and deflect potential security issues.

A closer look at Nortel Networks solutions for enterprise E911 service

For the enterprise network, Nortel Networks provides traditional PBX and centrex systems, IP-enabled hybrid systems, pure IP telephony systems, and multimedia communications and collaborative services platforms with support for E911.

- **Our market-leading Meridian telephony/circuit-switching systems** support the industry's richest set of voice/data features and business-building applications, and offer an intelligent evolution path to IP.
- **Our Succession IP networking portfolio** extends the benefits of IP to enterprise applications, such as integrated voice and video calls from your PC, and IP-powered call centers —whether you choose to build a pure IP network or IP-enable your existing communication system.

Nortel Networks Enterprise Portfolio—E911 service

Nortel Networks portfolio of enterprise communication servers, gateways, softswitches, and multimedia application servers combines the best of the Internet with the best of the phone network—creating next-generation packet networks that reliably transport voice, data, and multimedia traffic over a single infrastructure. This portfolio supports a common approach to E911 services in a converged IP network, including:

- **Special treatment of emergency calls** to facilitate effective emergency response
- **Flexibility to implement policies** such as ANI number translation for DID and non-DID numbers, mapping to defined ERL zones, and more, to fit legislative and business requirements
- **Support for IP-enabled low cost mobility** by automatically detecting and responding to location changes to properly route E911 calls.
- **Open architecture** for integration into legacy and hybrid enterprise environments where callers use analog, digital, and IP-enabled phones and sets. This open architecture supports a common emergency management system across the Nortel Networks enterprise portfolio.
- **Premium performance,** leveraging the proven attributes and architecture of Nortel Networks Succession and Unified Security Architecture platforms to provide high availability, reliability, and security
- **Cooperation for added value,** through technology alliances and open interfaces that enable your enterprise to benefit from third-party, value-added E911 solutions for ALI updates, OSN, etc.

Succession 1000 is a server-based, full-featured IP PBX, providing the benefits of a converged network plus advanced applications and more than 450 world-class telephony features. Fully distributed over an IP LAN and WAN infrastructure with built-in reliability and survivability, Succession 1000 supports business-critical applications, including unified messaging, customer contact center, interactive voice response, wireless IP Telephony, and IP phones.

The Succession 1000 Emergency Services Access (ESA) feature is being extended to support the Succession Enterprise E911 architecture for IP-enabled mobility—which includes support of the Succession 1000 Virtual Office as well as client mobility.

Multimedia Communication Server 5100 (MCS 5100) is a new communication server that converges voice, multimedia, and data networks for enterprises of all sizes. Unique to MCS 5100 is the ability for a mobile user—whether accessing the IP private network through a PC client, Web client, or Nortel Networks i200X IP telephone set—to choose the appropriate ERL for their current physical location. The user has the ability to select their location from a drop down menu—this location information can be office, floor, building, campus, etc. It can be customized for the specific customer.

If the user is in a hotel or at home, they will be warned not to use the phone for 911 service. For static assignments, the system can be engineered for auto-discovery of ERL information when a phone registers for the first time, or after a move.

Succession 2000 is a server-based, full-featured IP PBX supporting large enterprises. The Succession 2000 currently allows a person to initiate an emergency call when using static wireline devices or static IP telephony devices (IP soft clients, IP hard clients, etc.). This capability is being extended to support the Succession Enterprise E911 architecture for IP-enabled mobility.

Succession Business Communications Manager (Succession BCM) is a cost-effective, applications-rich platform that delivers to small- and-medium-sized businesses and enterprise branch offices the only converged voice and data solution in the marketplace—giving enterprises the choice of either an IP-enabled or pure-IP strategy.

Location Information Services for automatic location determination

Nortel Networks has collaborated with a number of vendors for this functionality, including RiT Technologies, a market leader in adding intelligence to the physical layer of the network. RiT PatchView Smart Patch panels automatically detect moves, adds, and changes in an IP network. PatchView scanners continuously scan all patch panels in the network and provide the updated location of IP devices in the network to enterprise call servers, administrators, and, in emergency call situations, to the appropriate PSAP.

Emergency services management system

Telident 9-1-1 solutions from Teltronics enable the PSAP to determine the exact location, or zone, of a 911 telephone call placed from the enterprise PBX, to dramatically improve emergency response times.

Cielo telemanagement software from RedSky Technologies, Inc. (*www.redskytech.com*) dramatically increases business agility and performance for E911 service, call accounting, and internal directory management.

XTEND Enterprise Alert allows an organization to interface with the public E911 network. Enterprise Alert integrates with industry-standard CAMA trunks, and addresses both NENA (National Emergency Number Association) and NENA2 formats and will continue to comply with future NENA standards as they are ratified.

Nortel Networks platforms interwork with these third-party solutions to streamline and enhance all administrative activities pertaining to location discovery, ALI database maintenance, and call management.

Summary

Converging voice and data services on an IP infrastructure offers significant advantages to enterprises in terms of flexibility, cost-effectiveness, and new functionality. However, the same characteristics that represent IP's greatest value propositions —easy mobility, client choice, and frequent adds/moves/changes—also present some new challenges for providing emergency services.

The Enterprise 911 policy must be revisited to determine the appropriate response to the variety of call scenarios that convergence makes possible. This goes beyond technical implementation and includes education and notification of users and the enterprise support staff.

An effective private E911 enterprise solution for a converged network environment must meet the following requirements:

- Provide comprehensive E911 functionality, meeting legislated and baseline 911 requirements while achieving reliability and availability targets
- Support mobility, with dynamic location determination and call treatment
- Support IP client access devices, such as IP phones and IP-enabled PC "softphones"
- Provide the right balance of granularity versus complexity to implement corporate policy on E911 services, administration, and security
- Provide open interfaces that enable value-add solutions from third-party vendors to complement the base solution
- Provide interoperability across platforms, to support a consistent user experience in heterogeneous networks
- Reduce the complexity of system administration in an environment where user-driven adds, moves, and changes will be commonplace

Whether your enterprise uses a traditional TDM network, converged IP network, or a hybrid of the two, Nortel Networks has a solution to support full-featured E911 services to all users and stations. To find out more about Nortel Networks E911 solutions for enterprises, visit us on the Web at: ***www.nortelnetworks.com.***

In the United States:
Nortel Networks
35 Davis Drive
Research Triangle Park, NC 27709
USA

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

In Caribbean and Latin America:
Nortel Networks
1500 Concorde Terrace
Sunrise, FL 33323
USA

In Europe:
Nortel Networks
Maidenhead Office Park
Westacott Way
Maidenhead Berkshire SL6 3QH
UK

In Asia:
Nortel Networks
6/F Cityplaza 4,
Taikooshing,
12 Taikoo Wan Road,
Hong Kong

Nortel Networks is an industry leader and innovator focused on transforming how the world communicates and exchanges information. The company is supplying its service provider and enterprise customers with communications technology and infrastructure to enable value-added IP data, voice and multimedia services spanning Wireless Networks, Wireline Networks, Enterprise Networks, and Optical Networks. As a global company, Nortel Networks does business in more than 150 countries. More information about Nortel Networks can be found on the Web at:

www.nortelnetworks.com

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

*Nortel Networks, the Nortel Networks logo, and the globemark design, and Succession are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document.

GSA Schedule GS-35F-0140L
1-888-GSA-NTEL