Proposal Response to:

Massachusetts Broadband Institute

Applications

Dated: November 2008

Nortel

CONFIDENTIALITY NOTICE – Customer acknowledges by its receipt and use of this proposal that it is confidential and proprietary information of Nortel Networks. Customer may use this document for the purpose of evaluating Nortel Networks' proposal and for no other purpose. Please ensure that this proposal is not disclosed to any persons other than your employees with a bona fide need to know.

© 2008 Nortel Networks. All Rights Reserved.

Table of Contents

Introduction 1

Subscriber Management 2

Pronto Networks 2
Additional partners 6

Advertising 7

121Media, Inc. 8

VoIP & Multimedia 9

Nortel's MCS platform 10
Enhanced communications management 10
Unified collaborative communications tools 10
Telecommuting 11
Converged Mobility – Dual Mode handset **Error! Bookmark not defined.**
MCS Converged Mobility Functionality **Error! Bookmark not defined.**

First Responder 12

Application overview 12
Mobile VPN through NetMotion 12
Mobility Benefits 13
Performance 14
Management/IT Benefits 15
Control 16

Mobile Applications 18

Workforce Automation through Accela 18
Digital Video Surveillance 19
Automated Meter Reading through Miltel 20
Location, RFID and Sensor Services through Blue Vector 21
Fleet Tracking and Monitoring through Blue Vector 26
Inventory, Asset Management, and Site Access Services through Blue Vector 33

Copyright©2008 Nortel Networks. All Rights Reserved.

NORTEL, NORTEL NETWORKS, the NORTEL NETWORKS corporate logo, and the Globemark are trademarks of Nortel Networks. All other brand and product names are trademarks or registered trademarks of their respective holders. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document.

Introduction

Nortel's Wireless Broadband solution is based on a core broadband wireless access infrastructure and layers on top a combination of applications that address consumer, municipal government and Enterprise users.

Nortel's experience in deploying leading edge technologies gives us a distinct advantage in the marketplace, speed to market due to our skilled resources to plan and build, and in some cases, maintain the network, as well as coordination and rigorous interoperability testing of our various partners to offer users a distinctly higher quality experience than our competitors are able to provide.

Building a network is one thing. Finding a way to profit from that network can be a bit more challenging. Building a wireless infrastructure to provide data and voice services is an impressive start, but serious consideration should be given to adding additional revenue generating applications that can increase overall take rates and customer satisfaction levels. Experience has shown us that an additional 25% to 35% of top line revenue can be captured with the right balance of applications.

Nortel's Broadband Wireless solution is based on a core broadband wireless access infrastructure and layers on top a combination of applications that address consumer, municipal government and enterprise users. A given Broadband Wireless deployment will likely have at least one application deployed on the infrastructure and will typically have more than one, therefore it is critical to have a solution which has been fully tested to ensure a seamless level of interoperability is available.

This section identifies application partners whom we support to deliver enhanced services for the network. We are continually working on developing new global partners to deliver even more functionality for our customers, and are pleased to work with any application vendor a service provider may choose to engage, to deliver a seamlessly integrated solution. Please note that the following examples of partner applications are provided to illustrate benefits to communities and to service providers. Nortel will be pleased to locate and find other best in class application vendors to address any specific Massachusetts Broadband Institute requirements.

Our ecosystem of partners and our world class services and integration teams enable key applications such as centralized Subscriber Management, Advertising, Mobile Virtual Private Network (VPN) capabilities critical to securing sensitive information (police, emergency personnel, etc.), Workflow Automation, Centralized Sensor Management and RFID reading and Secure Digital Video Surveillance services.

Subscriber Management

This section identifies application partners who deliver Subscriber Management Services. Such services are most useful when a customer is deploying Hot-Spot or Wi-Fi coverage, but also have some interesting applications for fixed WiMAX networks as well.

Pronto Networks

Pronto Networks OSS™ is an end-to-end wireless software management solution that streamlines and automates the operations and business systems management of wireless networks.

Nortel will partner with Pronto Networks to offer an end-to-end, integrated wireless infrastructure solution tailored for the municipal market. It will enable cities to deliver both public and private services on a single network to improve service efficiency, enhance employee productivity, expand economic development and reduce operations costs.

Pronto provides a Service Gateway platform that is a software based application running on a Linux PC. This device provides the policy enforcement and tracking point for Operation Support System (OSS) services.

Pronto also provides a full back office system to allow the delivery of the OSS functions. These are available from Pronto as either a full deployment by the Wireless Internet Service Provider (WISP) or as a managed service from Pronto. The managed service allows for WISPs to make initial deployments quickly and then to take on the back office responsibility once they have scaled sufficiently.

Virtual partitioning of wireless network for different types of users

Through Nortel's partnership with Pronto we support partitioning of the wireless network enabling the service providers to segregate certain classes of customers or critical devices so they have their own separate partition.

Pronto's solution is multi-tiered, enabling municipalities to sublet its network, if desired, to other network operators. A large carrier, for example, may want to offer its own branded wireless service within the municipality's hot zone. Pronto's support for Virtual Network Operators (VNOs) as well as multiple VLANs enable third party operators to offer their own branded service leveraging the existing wireless infrastructure of the city.

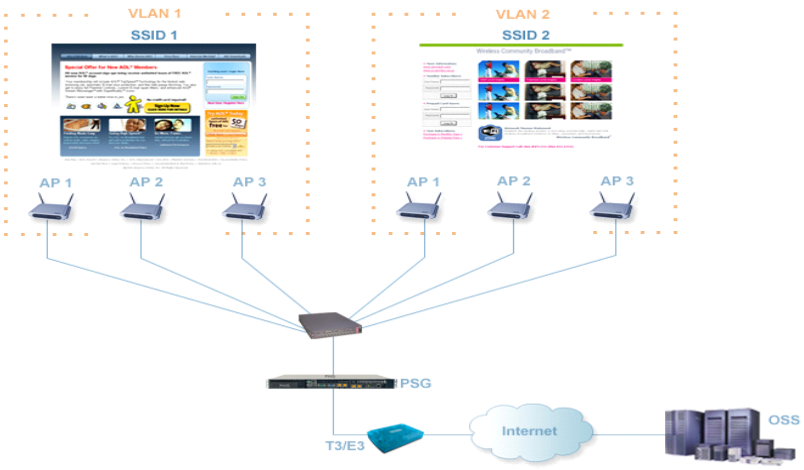

Figure 1: Deployment with VLANs

Pronto's broadband wireless platform supports VLANs and specific Quality of Service (QoS) assignments per user, which enable the network to be separated for both public and private use keeping in mind their specific needs. Multiple Service Set Identifiers (SSIDs) and thus multiple VLANs can be assigned to the same gateway in various situations. Some of these SSIDs could be hidden, e.g. for auto authentication for the public safety and fire department, etc.

Pronto's UniFi OSS™ Solution supports multiple service plans/offerings on the same VLAN (i.e. Captive Portal Page). The Pronto Service Gateway (PSG) can support multiple VLANs with a customized Login Page per VLAN. Even within a single login page, i.e. the same VLAN, the system can simultaneously support different types of users. As an example, the first type of user can have subscription-based login. The second can be for prepaid users. A third option can be to have authentication from an external repository, such as an external RADIUS, or part of a Roaming Network, etc. Each service option, i.e. service plan can have its own Quality of Service (Qos)/Service Level Agreement (SLA).

Multi-tiered rating and service plans enable both retail and wholesale offerings with support for a variety of authentication and payment mechanisms. Credit cards, pre-paid cards, monthly subscription plans and bandwidth usage plans are also supported, as well as roaming settlements with aggregators such as Boingo, iPass, and GRIC. The authentication options can vary from prepaid authentication to USB key based authentication. Pronto's UniFi OSS™ offers Radius AAA and 802.1x support as well as multiple authentication options through external sources, including Radius, MAC based authentication, LDAP-authentication, Short Messenger Server, USB key based authentication, MSN Passport, etc.

Nortel Networks Confidential

This is very useful if one wants to have different IP address ranges for different VLAN subscribers. Using VLANs, the network can be logically segmented to support different domains of users; secure access by government agencies, secure/open access for public users, residential, business users, etc.

All the target users can have a separate logical access to the network, and bandwidth rates that provides quality of service allocation guarantees. In addition to supporting VLANs, which secure city networks by keeping them separate from general-purpose use, Pronto's solution provides a Secure Sockets Layer (SSL)-encrypted registration and authentication process and supports corporate Virtual Private Network (VPN) clients to allow secure, encrypted access to one's corporate LAN.

The Pronto Service Gateway (PSG) can also be configured to support multiple VLANs on its LAN interface. This allows the service provider to offer different captive portals, splash pages, and associated service authentication options on each VLAN.

The customer portal represents the brand image of the service provider to the end users. Keeping this in view, the application provides sophisticated customization capabilities that customize the look and feel at the WISP, Franchisee and Location levels for different VLANs.

When the PSG initializes, it contacts the UniFi OSS™ to find out what configuration files, template files, location specific graphics, etc. it needs. One can add, delete and modify this file listing in the UniFi OSS™. Knowing the WISP/Franchise/Location level and filename, one can create login pages.

For example, WISP/Franchise/Location levels refer to scope of file and its relationship to each PSG under a Wireless Internet Service Provider. A WISP level file can be loaded once and it will be downloaded to each PSG, whereas a location level file must be loaded for each location.

Pronto provides the WISP or municipalities the capability to have their own logos/branding on the login page (i.e. the Captive Portal/Splash Page). The WISP can provide these options to their various franchises that can further let their various locations add advertisements on the login page for additional revenue opportunities.

Nortel Networks Confidential

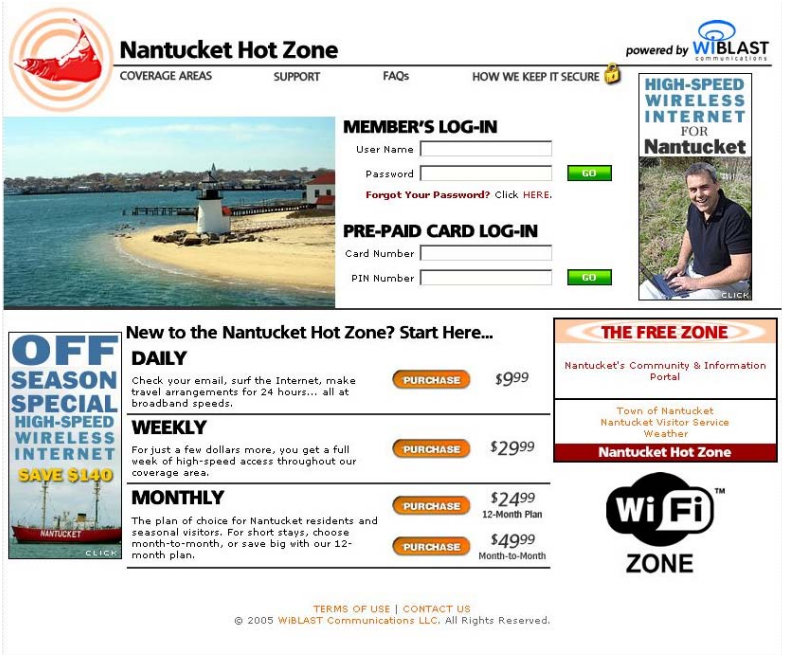

Figure 2: Example of a Pronto Webtool web page

Additionally, Pronto provides the option of adding Walled Garden links on the login page; these can be the links for partners or your own websites for which no subscriber authentication would be required. Any subscriber without valid login credentials can still browse through these pages.

When a user powers up the laptop or Personal Digital Assistant (PDA) and enters the SSID corresponding to the one configured on the Pronto's PSG, as defined by the Wireless ISP (WISP), he/she gets connected. When the subscriber attempts to access the Internet prior to authentication, the PSG redirects the request to its own internal web server located on the PSG, from where it picks up the initialization templates for loading the Splash page on to the subscriber's device

Now the subscriber can enter his username and password to get authenticated for wireless Internet access in that particular hotspot. The initialization template stored in the PSG is a standard template, which gets loaded with the WISP specific files also stored in the Pronto UniFi OSS™.

The Splash page is an HTML page comprising of multiple "cgi-bin" programs for providing different types of authentication options to the subscribers. The initial authentication screen can vary from WISP to WISP and within a WISP it can vary from location to location. A window with a Logout button is provided that can be used by the user to terminate the session.

Additional partners

Additional partners are available for Subscriber Management applications upon request.

These partners develop management solutions used for AAA (authentication, authorization, accounting system), provisioning, security, monitoring, roaming, pre- and post paid billing, etc.

Nortel will work with the customer to choose the best Subscriber Management partner to meet their needs.

In addition to Pronto Networks detailed above, these additional partners will provide:

- Complete Solution for customers to access a service and solution that takes care of all the important aspects when providing public Hotspot services
- Multi Service Provider & Wholesale capabilities allowing users belonging to many different service providers to log on to the same Hotspot through roaming agreements or to pay on the spot and get charged through trusted billing relationships
- Various Authentication and Payment methods including credit card options, User-id & Password, pre-paid vouchers, cash cards and others
- Service Provider and Hotspot owner Branding enabling fully customized login and payment pages
- Integration with existing platform interfacing with existing business processes including billing systems, mediation gateway and others
- A graphical user interface for configuration management of the wireless network and subscriber base

Nortel Networks Confidential

Advertising

Nortel is partnering with industry leading advertising application providers who have developed a network-centric targeting solution for online advertising on wireless networks, which provides incremental revenues to the service provider based on the usage of the network.

These vendors will work with our Service Provider partners across an open architecture interface with a combination of the major advertising portals and online advertising networks to personalize contextual advertising throughout the Internet experience on the wireless network.

- Consumers in the US are spending more time on the Internet than any other media networks, and carriers collect a flat fee to provide users access to the Internet.
- Destination sites (i.e. portals, search engines, websites) on the Internet generate significant revenues which utilize increasing bandwidth, but the network operators do not see these gains
- Advertisers are looking for more "intelligence" about users viewing their content and advertisements, and to economically reach the right audience with the right message: "delivering the right impression"
- Revolutionary approaches are being taken by new advertising partners to deliver relevant ads without compromising the privacy of the user. Device information in the network is "anonymized", and provided to the advertiser's destinations to enable them to deliver customized, personal information to devices on the wireless network.

This technology provides an unprecedented level of accountability for the advertising media planners and buyers.

The technology will enhance any advertising product e.g., search results, classifieds, local, contextual ads, banner ads, etc. These advertisers do not require a user to log in (unlike subscription-based portals), so the user experience to access the network is simple and attractive.

121Media, Inc.

One of our partners, 121Media, Inc. is a leading provider of online marketing services for Advertisers, Networks, Publishers, and ISPs. 121Media works with hundreds of web sites in virtually every industry. This great wealth of content allows them to match the perfect advertiser with the perfect consumer in almost any corner of the web (including blogs, forums, and shopping pages). Unlike other contextual advertising options, 121Media's PageSense does not require any download to a user's computer, and all contextual matching is based on content relevancy, with no personally identifiable information ever needed or used. 121Media is serious about preserving the privacy and anonymity of its users. Secure (HTTPS) pages are ignored and pages where personal data seems to be asked for or provided are ignored. No names, addresses, credit/account numbers, purchases, passwords – anything identity-related are captured.

As a result, 121Media maintains a positive user experience – to retain ISP subscribers and protect advertiser brand reputation.

121Media targeting enables highest value per ad, therefore fewer ads are necessary: adds just 1-3 ads per day, less than 1% of the average of 300-400 online ads per day users normally see. There are no persistent software downloads, and no pop-ups!

With 121 Media's PageSense technology, users are identified only by randomly-selected number. Ads are inserted in a variety of methods, banners, interstitial between domains, or as promotions on the WISP portal site.

121 Media's targeted advertising approach is preferred by user and it fits better with their current interests, therefore making it more attractive to advertisers to provide detailed customer driven promotions.

For more information about other advertising methods and partners, please contact your Nortel sales representative.

Nortel Networks Confidential

VoIP & Multimedia

Our Broadband Wireless solution allows the opportunity for Municipalities and Enterprise customers within the Wireless Coverage area to transform their voice communications with the power of Voice over Internet Protocol (VoIP) and Multimedia Communications Services. These new services, enabled by Nortel Multimedia Communication Servers, allow people to communicate as never before, enhancing productivity, mobility and personalization.

Imagine the power of a handset that leverages the use of WLAN/WiMAX coverage when available, allowing users to save pay for use cellular minutes, as a small example of the power of this technology. Or provide city workers with wireless handsets to take advantage of the Wireless Broadband network instead of a cell phone for daily communications. Other examples include productivity improvements for telecommuters and mobile workers to access the same information remotely as if they were sitting in their office, and allowing government departments the ability to securely transfer files from site to site with the touch of a button.

These products are the leading example of the power of IP Telephony to date because they utilize commercially available hardware and open-standards software to unite voice communications with next-generation applications such as Instant Messaging, video conferencing and file sharing. By funneling all incoming and outgoing messages through one network and one interface, users get more control over communications — essential to managing time more efficiently.

Our Call Server and Multimedia Application Server build on Nortel's extensive expertise in developing mission-critical VoIP systems that deliver true carrier-grade reliability, scalability and manageability. One of the key capabilities of Nortel's platform is that the services are independent of the access technology, so they can be delivered across multiple carrier and enterprise networks, allowing WISP partners to deliver hosted services to a multitude of customers from one central application server location.

Additionally, VoIP and Multimedia services are available through Nortel as a hosted offer, capable of being resold by our WISP partners on a price per seat basis, limiting the capital outlay required to deliver these services.

Nortel's MCS platform

The Nortel Multimedia Communication Server (MCS) platform enables a vast array of new Multimedia Communications Services that enhance productivity and mobility, independent of location. Each feature is independent, allowing users the power to choose individual features they find most valuable.

Enhanced communications management

Personal Agent

The MCS Personal Agent provides users greater control of everyday communications. The Personal Agent functionality allows users to define rules for redirecting incoming calls (based on call attributes such as caller ID, time of day, etc.) from a single directory number (or SIP address) to their most convenient communications devices. The Personal Agent includes features that make communications easier for remote/traveling users. These features include call screening, find me/follow me and simultaneous/sequential ringing features.

Call management

The MCS platform simplifies communications by enabling click-to-call, Microsoft® Outlook® integration (ability to call with one click from Microsoft Outlook), personal and group directories, dynamic call, dynamic availability (presence) control and call logging features. It also enhances the user experience with a voicemail indicator and a picture ID display, as well as ad-hoc and meet-me conferencing capabilities.

Voice

The MCS platform enables workers to stay in contact while on the road by offering traditional voice services over the Wireless Broadband network. Using Session Initiation Protocol (SIP) capabilities, this platform delivers key telephony features including call forwarding, call hold, call transfer, call waiting, call mute, as well as calling line ID (with name, number and subject).

Unified collaborative communications tools

Collaboration

The MCS platform closes the gap for geographically dispersed workers by facilitating sharing of files, images, text and other content easily and efficiently. Enables all workers to communicate more effectively with applications such as secure Instant Messaging, presence notification, white boarding, Web push, co-browsing and instant file transfer features.

Nortel Networks Confidential

Video

The MCS platform enables point-to-point video calling from a user's desktop, without the need for special rooms or complicated dialing procedures. This allows service providers to offer their customers an optional video calling feature that is as simple to use as clicking on a name in a personal or group directory. Video calling is user-controlled and can be activated per call or mid-call.

Telecommuting

With Nortel VoIP and Multimedia platform enabled with our flexible **find me/follow me** feature, telecommuters and home office business owners can have all of their calls routed to one designated phone, so customers and co-workers can always stay in touch.

One mailbox ensures that they can easily access all of their messages from a single voicemail box, regardless of whether the call was placed to a home, work or mobile phone.

Call screening enables telecommuters and home office business owners to immediately identify callers. With this feature, they can avoid unwanted calls (and the wireless charges of answering the phone). They can also take a few seconds to gather themselves when the call is from someone important (prospect, customer or boss). And the audio conferencing feature enables these home-based workers to participate in crucial group meetings.

Automatic presence indication allows users to display their availability online and determine when others are available. Telecommuters and home-based business owners can also take advantage of other powerful features, such as **secure Instant Messaging**, with which they can send and receive encrypted messages.

With **instant file transfer** they can share important files with business partners or fellow employees, even if they are on the phone. Best of all, **desktop video calling** enables home-based workers to enjoy all of the benefits of attending a meeting in person, from giving a powerful presentation that can be seen, as well as heard, to picking up on visual cues from other attendees. With Multimedia Communications Services from Nortel, home-based workers never have to worry about being out of sight or out of mind.

Nortel Networks Confidential

First Responder

Application overview

Broadband Wireless networks introduce another communication network in the municipality that can be used for communications by first responders in addition to cellular network and various licensed spectrum technologies (police bands). One of the key challenges with this diversity of communication technologies is the interoperation between the technologies as it is critical for first responders to be able to communicate with each other regardless of the access technology each is using.

This application provides a number of functions:

- Mobile Virtual Private Network (VPN) services – allowing a VPN to be maintained from a device like a PC in a police cruiser over multiple networks (allowing various network to fail) ensuring reliability of the connection and mobility of the user.
- Application persistence – allowing user applications to be kept alive, even if all network connections have been lost. An example would be a police cruiser entering a parking lot and losing all networks. When exiting the parking lot, the laptop will reconnect and all applications will continue running without effect.
- Encryption – some public safety agencies (federal) require higher levels of encryption on public safety traffic.
- Multinetwork interoperability – allowing the diverse networks; legacy and emerging used by public safety agencies to interoperate. Enabling communication between users on the various networks

Mobile VPN through NetMotion

Nortel partners with NetMotion to provide a Mobile VPN Application.

NetMotion Wireless's flagship product, Mobility XE™, is the acknowledged leader among mobile VPNs. Mobility XE™ provides best-in-class security, mobility and management. Mobility XE™'s strengths have been recognized in the marketplace. Network Computing, in the first Mobile VPN category review, gave Mobility XE™ top marks, recognizing it with an "Editor's Choice" award.

In addition, leading technology analyst firm, the 451 Group, recognized NetMotion Wireless as "the clear leader in the Mobile VPN space."

Most important, approximately 1,000 customers have licensed Mobility XE™ software for hundreds of thousands of mobile workers.

A Standards-based Secure, Virtual Private Network Built for Mobile Users

Data traversing a wireless environment is vulnerable to corruption, eavesdropping, and unauthorized access. Traditional VPNs such as Internet Protocol Security (IPSec) and Secure Sockets Layer (SSL) may seem to solve the security problems, but they are not designed to work over wireless networks.

To address these concerns, Mobility XE™ incorporates a standards-based, secure, virtual private network designed for wireless networking. It offers single-sign-on authentication through Microsoft Active Directory, RADIUS, Kerberos, RSA SecurID, PEAP, and other prevailing standards. Mobility XE™ also uses standard Microsoft Windows login credentials so there are no additional steps to learn or passwords to remember.

The Mobile VPN encrypts all data transmitted between the Mobility client and server using AES in 128-bit, 192-bit, and 256-bit strengths. The algorithm can be configured globally or on a per-user basis, or it can be disabled for mobile workers who do not require such high security. Mobility XE™ uses FIPS 140-2 compliant encryption modules to meet North American security requirements.

This security is tightly integrated with Mobility XE™'s InterNetwork Roaming capabilities. No matter where client devices move, mobile workers are automatically authenticated and the encrypted tunnels are automatically established.

Mobility XE™'s mobile VPN is a solid end-to-end security solution for customer's requiring access into their network from the internet or private carrier connection from any type of wired or wireless access.

Mobility Benefits

What differentiates Mobility XE™ from IPsec VPNs and SSL VPNs is its robust set of mobility-specific benefits: application session persistence, network roaming and performance enhancements. These benefits are key for first responder applications.

Roaming: Access across Multiple Networks

Today's Public Safety agencies use multiple public and private networks. They include conventional wired LANs, high-speed wireless networks on City campuses, private hotspots in community Police and Fire stations, home connections, wireless WANs such as 1xRTT, EVDO, EDGE, HSDPA, etc. and even satellite connections for extremely remote operations. All of these networks have different security and performance characteristics.

Mobility XE™'s InterNetwork Roaming™ turns this multi-network environment into an easily managed system.

Nortel Networks Confidential

It lets mobile workers transition between networks seamlessly, transparently, and securely — and without having to think about their network connections.

The Mobility XE™ server accomplishes this by establishing a virtual IP address for each user, for all communication with the enterprise applications. Even as clients move and are assigned new IP addresses by various networks, the enterprise application servers always see the same, unchanging virtual IP address. There is no need to re-segment networks, implement VLANs, or deploy additional hardware to enable mobile workers to roam freely.

Protection against Lost Connections and Application Crashes

Solutions that merely enable cross-network roaming only solve part of the mobility puzzle. Many agencies have installed these solutions only to find that their applications crash. That is because typical enterprise applications are written to assume a continuous wired connection.

Throughout the working day, mobile users often move into areas where there is no coverage such as parking garages, stairwells, elevators, and even airplanes. They also suspend their devices, change locations, and re-start them. The severed connections trigger application crashes, leading to lost or corrupted data, re-authentication, repeated data entry, and frustrated, less-productive workers.

Mobility XE™ provides Application Session Persistance. The Mobility server acts as a proxy that keeps the connections to the application server alive — as the user crosses networks, or even shuts the device off. To the enterprise application server, mobile users appear as if they are continuously logged on via a wired network. When the client reconnects, the Mobility server automatically resumes sending and receiving data. Depending on the administrator's setting, a user can even start a multi-megabyte file transfer, power down, go on a week's vacation — and boot up the device and resume the transfer exactly where it left off.

Performance

Mobility XE™ is designed to improve performance over wireless networks, especially across slower Wireless WAN links.

Faster Transmission across Lower-Bandwidth Networks

Most applications and the TCP/IP protocol itself were designed to operate over wire at gigabit speeds. Wireless transmissions are far less predictable, and the packet sizes and timing parameters used for wired transmissions are far less efficient when applied to a wireless environment. Through its link optimizations, Mobility XE™ sets the transmission parameters that are most efficient for each type of wireless link. This reduces the number of retransmitted packets, excess control information and other network "chatter."

Nortel Networks Confidential

Mobility XE™ applies data compression to traffic sent over lower-speed links. The threshold is adjustable, allowing the most efficient tradeoff between the CPU overhead introduced by compression, and the speed gained by transmitting less data.

In addition, Mobility XE™ allows the compression of large web images (JPEG or GIF), particularly useful over slower wireless WAN networks. In tests, Mobility XE™ has been shown to more than double the data throughput of wide-area network links.

Management/IT Benefits

Straightforward Installation

NetMotion Mobility XE™ offers a true plug-and-play solution, with no need for custom software development or application rewrites.

Installation can be accomplished in hours — not days or weeks. There are two components: a Mobility server, and a lightweight client that is installed on every wireless laptop or handheld device. The Mobility server runs on a Windows 2002 or 2003 server, and acts as a proxy to enterprise application servers. The client software runs in the background and automatically handles the transitions as users roam across networks. Even as users change locations or cross gaps in coverage, the only hint that Mobility XE™ is at work is a small icon in the system tray. Clients are available for every kind of portable device, using operating systems that include Pocket PC, Windows CE, Windows Mobile (including Windows Mobile 5), and versions of Windows from Windows 2000 to Windows XP. Virtually any application that currently runs in a wired environment and communicates over TCP/IP protocol can be wirelessly enabled with Mobility XE™.

Streamlined, Web-Based Management

Mobility XE™ includes a web-based administration and monitoring console to which secure access is available from anywhere. The Mobility XE™ console offers intuitive access to server and client status, settings, license control, and (if it is installed) the administration of the optional Policy Management module.

The Mobility console presents a graphical and statistical summary of each server's health and current activity, as well as overall system usage on a per-server and pool-wide basis. Administrators may also take servers offline through the console for performing maintenance tasks. In addition, the console reveals the activity for each mobile device including authentication, roaming history, and data transmitted for each location. It also reports more than 100 metrics and statistics including operating system and battery life.

System administrators can grant access to operator users who can view the system and client configurations and status, but not make changes. This is useful for first-line troubleshooting by help desk personnel.

Nortel Networks Confidential

Capacity to Reliably Handle Thousands of Users

A Mobility XE™ deployment can support up to 35,000 mobile users. Each Mobility XE™ server can handle large numbers of users for extended periods because it actively controls data flow by active methods rather than merely caching data.

Mobility XE™ has multiple server capabilities for supporting the largest enterprises:

- **Server Pools**. Multiple Mobility servers can be configured and managed as a single, logical pool. The servers work together automatically to service the combined client load. Large enterprises are able to add new servers to the pool without disrupting current users.
- **Load Balancing**. New client connections are automatically distributed across the Mobility servers in the pool based on the server's capacity, memory use, network traffic volume, and CPU utilization. If servers in the same pool have different capacities and power, load balancing automatically distributes the load accordingly so users experience consistent network performance.
- **Failover**. If one server fails, the users do not lose their connections. The other servers automatically re-distribute the clients among themselves, in accordance with the load balancing rules.
- **"Server Throttling"**. Server throttling prevents sudden spikes in usage that users perceive as slowdowns in system performance. When use of system resources reaches a predefined threshold, each Mobility XE™ server automatically prevents additional clients from establishing connections. Instead, the load balancing redirects new connections to other servers. This ensures that enough resources continue to be available to service the active load, and also helps to combat denial-of-service attacks.
- **Mobility Warehouse**. Mobility XE™ stores system information, user data, and device settings in a Mobility Warehouse that can be located on a server in the pool, or on a separate server. A backup copy can be stored on another machine so, if the warehouse fails or becomes unavailable, the servers in the pool automatically switch to the backup warehouse.

Control

Mobility XE™ includes a Policy Management module that provides centralized, flexible tools for managing applications, devices, and users in a wireless network environment. Mobility Policy Management enables IT managers to control network costs, improve productivity, and ensure data security over any wireless network. Ultimately, Policy Management allows IT managers to ensure that wireless network usage and performance are aligned with corporate IT policies and ROI goals.

For example, an administrator can restrict access to specific network resources either by network, host (IP) address, or application name.

Nortel Networks Confidential

In addition, these access privileges can be dynamically enforced depending on the network type, location, and/or time of day that the mobile worker is connecting.

Policies are established centrally on the Mobility server and then distributed to individual clients. Companies can enforce IT and corporate security policies by assigning rules globally, to workgroups, by class of device, or to individual users and devices.

For applications requiring a hardened router component for mobile VPN solutions, Nortel has several partners we work with to deliver these solutions.

Nortel Networks Confidential

Mobile Applications

This section identifies available applications and providers for mobile applications using the Wireless Broadband network.

Workforce Automation through Accela

Like many businesses, government agencies are employing a significant number of field personnel. Typically, agencies maintain a staff of field inspectors who spend most of their time out of the office, where they gather information, complete work orders, and process daily inspections using paper-based systems. This approach is inefficient and contributes to increased travel time, paperwork backlogs, revenue loss, and citizen dissatisfaction.

Accela's mobile government solution, Accela Wireless™, empowers an agency's mobile workforce to operate more efficiently by extending inspection management capabilities to the field for inspections, code enforcement, work orders, service requests, and more. Inspectors can run Accela Wireless on a variety of portable platforms including tablet PCs, laptops, and handheld pocket PC devices. The application is customized to match the agency's current business processes, allowing users to leverage current knowledge as they transition to an automated solution.

Anytime, Anywhere Access

Accela's mobile government solution can be deployed over Nortel's wireless broadband network to allow inspectors to process inspections, research application data, and retrieve information in real-time. Accela Wireless operates in on-line or off-line (store and forward) mode without interruptions in data collection or transfer. As inspectors move away from hot spots, the application works in off-line mode and data is stored locally on their portable device. As inspectors approach a wireless hotspot and re-establish connectivity or when they return to the office at the end of the day, the application runs in on-line mode and data is transferred seamlessly and securely.

By moving inspectors from the office to the field and giving them the proper tools to complete their daily work, government agencies minimize travel time for inspectors, eliminate processing delays, accelerate revenue collection, and improve citizen satisfaction.

Digital Video Surveillance

Digital Video Surveillance and physical site security are today required in many metro areas. Traffic monitoring systems for both traffic control and law enforcement purposes are being installed. Taking this concept further for law enforcement purposes, many cities are installing multi-angle street corner cameras that are directly monitored by the local police precinct. This is particularly attractive in high crime areas or areas that have relatively lucrative retail establishments. The recent events within our schools have highlighted the need for these types of capabilities in the districts.

The Digital Video Surveillance (DVS) application is Nortel's solution to the requirements to protect and enhance public safety for employees and citizens on our highways, schools, public parks, government buildings and all public spaces from the current anti-terrorist fears, road rage and crime to name a few.

Nortel is in the unique position to provide both the infrastructure and applications. Nortel brings industry leading expertise in the design, integration and deployment of seamless large and complex end to end IP based quality solutions, has a large customer installed base of existing security related components (e911, call center, VoIP), is supported by a world class services organization, can draw on an extensive best in breed partner eco system and provides customers with a single point of project contact, coordination and delivery via their world class Program Office (PMO).

Digital Video Surveillance is a flexible and scalable solution that can be applied to a single building, a campus, multiple locations, or across a city wide deployment with the assistance of our professional services group to design, install, and optimize the multiple components required to deliver an end to end DVS solution that meets a wide range of customer needs.

Nortel has an extensive portfolio of companies we partner with to provide customers with an end-to-end DVS solution. Through our partnerships Nortel provides an integrated solution with the latest technology innovations in cameras, video management, storage and analytical software as well as expertise in design, deployment and support.

A Nortel dedicated Program Office (PMO) provides the oversight and coordination to deliver projects on time and on budget by managing and reporting on your total schedule, risk, cost, quality, scope and resources across all projects. The Nortel PMO provides expertise tailored to your business requirements while taking responsibility for all projects included in your company, enterprise or program.

The PMO administers, coordinates and brings together all aspects of your implementation including partners under one project and provides the extra focus and resources for project management excellence for companies of all sizes. A truly effective PMO not only delivers projects

on time and on budget, but also ensures that projects are aligned with overall business goals to set business strategy in motion and propel your business forward.

Automated Meter Reading through Miltel

With Wireless Broadband coverage blanketing MBI's coverage area and its member jurisdictions, we believe that automated meter reading, location, sensor and RFID services will provide significant benefit to residents, businesses and to municipal government.

Nortel can provide a fixed AMR solution that will provide automated reading from every meter in the city, every day.

Meters can be read at rates from 1 reading per day to as frequent as 288 readings per day (or every 5 minutes). All readings are automatically transmitted from the meter to a centralized management and control infrastructure and will eliminate the need to physically visit the meter to conduct data logging activities for business and residential meters. The costs and time for performing this function (i.e. truck rolls) will be eliminated as well.

A fixed AMR solution removes the human or manual element from meter reading and is ideally suited for hard-to-access and hard-to-read meters. In fact, the City will have no reason at all to gain physical access to the meter to collect a reading. This key benefit not only provides for safe, secure, and reliable meter reading but also reduces insurance claims and other cost associated with collecting reads while also ensuring more accurate billing of services. Over time, the city should see a reduction in operating costs from having fewer truck rolls to physically read meters as well as an increase in revenues from the deployment of sensor-based meters.

For Automated Meter Reading applications (utility, parking), Nortel has partnered with Miltel to provide this functionality. We have an additional partner, Blue Vector, described in the following section who will work in concert with Miltel to deliver a centrally managed solution for both AMR and RFID, sensor, and tracking solutions for municipalities, when these multiple application solutions are being deployed.

For those instances when a specific utility Meter reading application is preferred, Miltel's Automated Meter Reading devices and network management system will be used.

Miltel is a provider of Automated Meter Reading technology, specifically a fixed network system architecture. Miltel technology is multi-utility capable – meaning it supports water/gas/electric meters reads.

Miltel has demonstrated that AMR systems are not systems designed merely for meter reading. Based on periodic stream of consumption data, the management system is able to provide extensive information that not only details updated billing data but also contributes to

significant savings on the operational side, and extensive information that can make the customer support functions more efficient.

Miltel's solution employs State-of-the-Art Wireless Technology with 450-470 MHz range transmitters passing data to wireless receiver modules, either at another metered site, in a central location in the Wireless Broadband network or to a repeater unit available to collect data outside wireless zone (<5 miles).

The Miltel central management platform is a standard Windows Based OS Server in the customer Data Center which provides a direct link to existing billing systems, with automatic conversion for ease of deployment. The system is a full scale database management system (SQL) with a GUI Based application interface.

The Miltel solution provides a revenue share opportunity for WISP providers to partner with Utility/Municipalities providing not only standard metering services, but also Sub Metering to large complex, shopping center & condo environments.

The Miltel solution is a low cost, flexible deployment utilizing Nortel's Plan and Build Services to design and deploy the solution.

Location, RFID and Sensor Services through Blue Vector

Further utilization of the Wireless Broadband infrastructure can be realized through deployment of location, sensor and RFID services to provide new services for tracking and monitoring of equipment, assets, vehicles, and even people. This will increase productivity and satisfaction of the city's residents, businesses as well as municipal government.

Through our partnership with Blue Vector, we offer a single unified solution for managing any asset tracking, sensor, or RFID service on the network. This includes fleet tracking, yard management, secure site access, automated checkout, people tracking, as well as management of sensors, video and light boards for parking meters and traffic controls.

The Nortel unified solution for management of location, RFID and sensor services using the Blue Vector X-3000 system together with the Nortel Wireless Broadband network. This will allow us to offer the town and its businesses a powerful means to innovate, automate and dynamically control complete business processes that utilize real-time information from RFID, sensor, and location devices.

In addition to RFID, GPS, and mobile tracking systems, this also includes management of any remote sensor device, including automated parking meters, light boards for traffic signs, traffic sensors, and monitoring equipment can be incorporated into our services using this unified architecture. The Nortel – Blue Vector system scales to handle any business task and across any geography:

Nortel Networks Confidential

- Tracking and optimizing mobile asset utilization in a yard and across a city
- Enhancing facility and public campus security with RFID and sensory capabilities
- Automated meter reading for water, utility or other metered services
- Tracking item level inventory in a warehouse or across an entire national supply chain
- Managing city-wide traffic control and emergency messages in response to an event

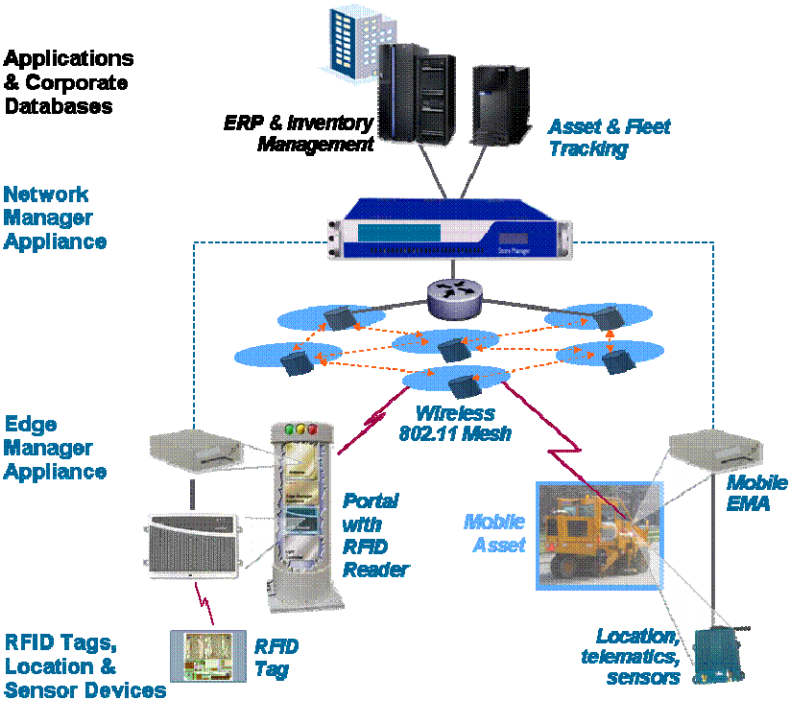

Figure 4: One architecture for providing mobile asset tracking and managed RFID & sensor services utilizing the Broadband Wireless network (WiFi or WiMAX)

The Blue Vector Edge Manager Appliance (EMA), coupled with a Wireless Broadband CPE, acts as a client on the Wireless Broadband network. EMAs can be stationary or mobile. The mobile EMA includes a GPS receiver. The EMA communicates with any type of device such as RFID readers and other sensor devices over TCP/IP or serial line connectivity. The EMA controls the devices and associated data-flows. EMA's are located on the customer premises or on customers' mobile assets.

The Blue Vector Network Manager Appliance (NMA) communicates with assigned EMAs. The NMA distributes the required business rules to EMAs that govern device data collection, how device data should be combined and distributed, and what constitutes a business event that

must be acted on. In this way, thousands of intelligent devices can be managed and easily integrated with back end systems.

A Global Manager Appliance (not shown in the figure above) can be encompassed into the architecture to accommodate multiple enterprise sites and to enable scalable collection of information from many NMAs (thousands) and their assigned RFID/sensor devices (tens of thousands). NMAs are distributed around the provider network are connected back to a central GMA. Each NMA talks to the GMA, for purposes of exchanging configurations, heartbeats and data. Data transmitted to the GMA from a local NMA is sent using a store-and-forward mechanism for fault tolerance.

With this approach, we can enable a variety of completely managed RFID, location & sensor services to customers.

Blue Vector's X-3000 system creates a scalable, automated infrastructure that spans the entire network and can be used to manage multiple customers across their entire business if desired. It greatly simplifies the processes associated with integrating multiple RFID, location-based systems and sensor deployments with multiple backend business systems, and, subsequently, lowers costs related to the rollout and on-going management of larger scale RFID, location and sensor installations. This will allow the town's wireless network to support cost-effective RFID, location and sensor services for the town and local businesses.

The Blue Vector X-3000 system is designed to manage thousands of independent intelligent devices − including RFID readers, GPS receivers, sensors, lights, displays, scales and gates. The X-3000 system is vendor agnostic, so, for instance, it can work with all vendors' RFID readers and tags.

A key feature of the X-3000 system is distribution of processing logic to the physical edge of the network. GMAs and NMAs distribute business logic to EMAs to control all of the intelligent edge devices connected to the EMAs. Business logic is all centrally configured and is automatically distributed to the applicable EMA. In this way, these devices can respond to changing situations at the edge in real time, such as an RFID-tagged asset entering a non-restricted zone.

Finally, the X-3000 system integrates with back-office systems. Therefore, its data can be used in any existing operations reporting applications. If desired, the X-3000 can also offer its own reports for real-time data monitoring. These reports are available in the Infrastructure Status module of the CMS.

With the X-3000 system, large-scale, centrally-managed RFID network operators can control real-time information about physical assets and processes, changing the system's behaviors quickly and easily from a central location to respond to changing business needs. All this is done without expensive refactoring, without time consuming hardware upgrades, and without requiring technicians to make changes in the field. The town wireless network service can offer a customer a standard set of business logic to govern customer device data flows, or

Nortel Networks Confidential

provide services to customize logic to meet a customer's unique needs. Secure device data flows are directed to customer applications or to a customer portal managed as part of the town's wireless network.

The Blue Vector appliances have pre-configured functionality and are Linux based. This means that all functionality is built into the appliances; therefore there is no need to load and install any software. Blue Vector's NMA and GMA were designed to integrate smoothly with enterprise applications (e.g., Oracle database application, SAP ERP application, Microsoft application).

Nortel Networks Confidential

The web-based Configuration Management System (CMS) software layer of the X-3000 resides on the Network Manager and Global Manager appliances. The CMS enables not only remote configuration and setup of the RFID infrastructure, but also remote monitoring for ongoing operations and changing business needs.

CMS tools, the Configuration Module and the Deployment Module, allow a user to set up, configure, deploy, and manage the software that controls physical devices, such as the RFID readers, indicator lights, photo eye sensors, etc.

The X-3000 distributes business logic through use of BLOX. BLOX are applets of programmatic functionality that encapsulate tactical business processes that must be executed at the edge. Lightweight and customizable, BLOX allow the RFID, sensor, and location network to be customized to any unique business processes and environment. The Blue Vector Configuration Management System (CMS) tools allow BLOX to be easily distributed to EMAs and, consequently, applied to respective physical edge devices.

An intelligent system: Sample configurable process rules let the system understand *the context of information* so that it can react accordingly

Distribution Centers	• Shipping Ops • Receiving Ops • Authentication
Warehouse Receiving Ops	• Pallet Validation • ASN Reconciliation • Put Away Verification • Pallet Location
Warehouse Shipping Ops	• ASN Generation • Tag Validation • Notify IT Systems
Consumable Assets	• Item Location • Inventory Control • Vendor Managed Inventory
Reusable Assets	• Item Tracking Location • “Library” Functionality: • Security Alarms

Nortel Networks Confidential

Analytics/Applications	• KPIs – data analytics • Counterfeit Detection • Fault Detection
Pharmacies	• Receiving Ops • Dispensing Equipment
Retail Store Ops	• Smart Shelf • Promotional Display Tracking • Anti Theft • Item Location

By using a single unified architecture for management of a variety of location, sensor, and RFID service on top of the town's wireless network, we believe that we can combine these capabilities almost endlessly to provide services that are visible to the town's citizens. For instance, by tracking public transit and school buses, we can assist the town in making bus stop arrival times visible to parents and riders using their cell phones or PCs to access an Internet portal or even sending customized messages to citizens that subscribe to a service to warn them when the bus is getting close to their stop or if a particular bus is running early or late.

We can assist MBI to make information on town services much more visible to citizens through automation, giving them a better sense of how their town is performing. Additionally, through similar services to businesses, we can help town businesses to enhance their service to customers as well as their own asset utilization and efficiency. We believe that having a network and flexible service capability can allow us to work with MBI to prove out new innovate services that can provide a model for other towns to follow.

Fleet Tracking and Monitoring through Blue Vector

Nortel partners with Blue Vector to provide Fleet Tracking and Monitoring. One of the key location applications for Broadband Wireless networks is fleet tracking and monitoring. Nortel's fleet tracking and monitoring solution allows government and businesses to collect detailed information from their fleet, perform time-motion analytics on the data and begin to optimize fleet operations. Now local fleet owners can realize the benefits of fleet management services, such as: reduced fuel costs, reduced driving time between appointments through route optimization, reduced time spent on fleet administrative paperwork, and ability to provide enhanced customer services like automated messages.

For a completely managed service offered by a Broadband Wireless provider, much smaller fleets can take advantage of these savings usually only available to larger fleets.

We can enable a complete solution for managed services to local businesses, providing location and telemetric devices for the fleet, device management, customized data delivery and automated alarms and updates using intelligent business rules. Fleet information can be delivered via a secure Internet portal or direct to customer applications.

Also, using a mobile EMA, we can connect a number of peripheral electronic devices that might be located inside the vehicle that we would also like to manage information flow from, such as onboard medical equipment inside an ambulance.

Sample target businesses for fleet tracking and monitoring services

Local in-house fleets	Delivery companies like groceries, furniture, and home heating fuel
	Services companies like landscaping and moving services
	Any distribution centers within the municipality
City service vehicles	Fire trucks and ambulance
	Street cleaning, snow removal, sanitation services
	Postal service
	Dept of Transportation
Public transit & buses on routes	Public transit buses
	School districts
	Intercity bus or train companies
	Outsourced & charter busing services

Fleet management services can provide the following benefits and more:

- Reduce fuel costs: monitoring driver habits encourages less aggressive driving and more direct route-finding; eliminate fuel theft; reduce idling times; monitor personal use; monitor engine performance to ensure vehicles are performing in the most fuel-efficient manner.
- Reduce unplanned maintenance overtime and engine wear: timely warning of maintenance issues ensures that vehicles are properly maintained and allows better maintenance planning and scheduling.
- Reduce administration: automated odometer readings, diagnostics and proof of service completion (for instance, that a road had been plowed) reduce error and allow staff to focus on other things.

Nortel Networks Confidential

- Increase safety and public perception: aggressive driving is reduced or eliminated.
- Increase customer satisfaction and service: ability to provide new automated alarms and messages allows accurate and automated status updates, customer visibility of delivery times.
- Automated generation of alarms selected by the fleet owner to improve business flow or improve responsiveness.
- Know and be able to measure the real status and performance of your fleet and set measurable objectives for increased performance.

Location Solutions for Fleet Tracking & Monitoring Services

Using the Blue Vector X-3000 system with mobile EMAs, we can offer completely managed asset tracking and monitoring services via a secure customer portal or send location or status data directly to mapping, asset management, or fleet tracking applications owned by the customer. Mobile EMAs include a GPS device and a choice of 802.11b or CDMA-1XRTT radio. EMAs are securely connected to NMAs via the Nortel Wireless Broadband network or a cellular provider network as a backup connectivity option. NMAs feed the required location, telematics and sensor dataflows to fleet tracking applications managed by the municipal service provider or the end customer.

For location services that must incorporate spatial capabilities such as ESRI or MapPoint to provide maps, geocoding, content and routing, we are bringing together application and integration partners, one is AppLocation Systems Inc. AppLocation System Inc offer its Pathfinder platform as an application for asset and fleet tracking. Pathfinder has been deployed in many telecom environments for managed location-based services. It provides carrier-level security and auditing capabilities, and is designed for carrier grade reliability and availability. The Pathfinder platform interfaces with most major spatial mapping tools and databases and is specifically designed to allow rapid integration with enterprise applications such as maintenance, inventory and billing systems.

Nortel Networks Confidential

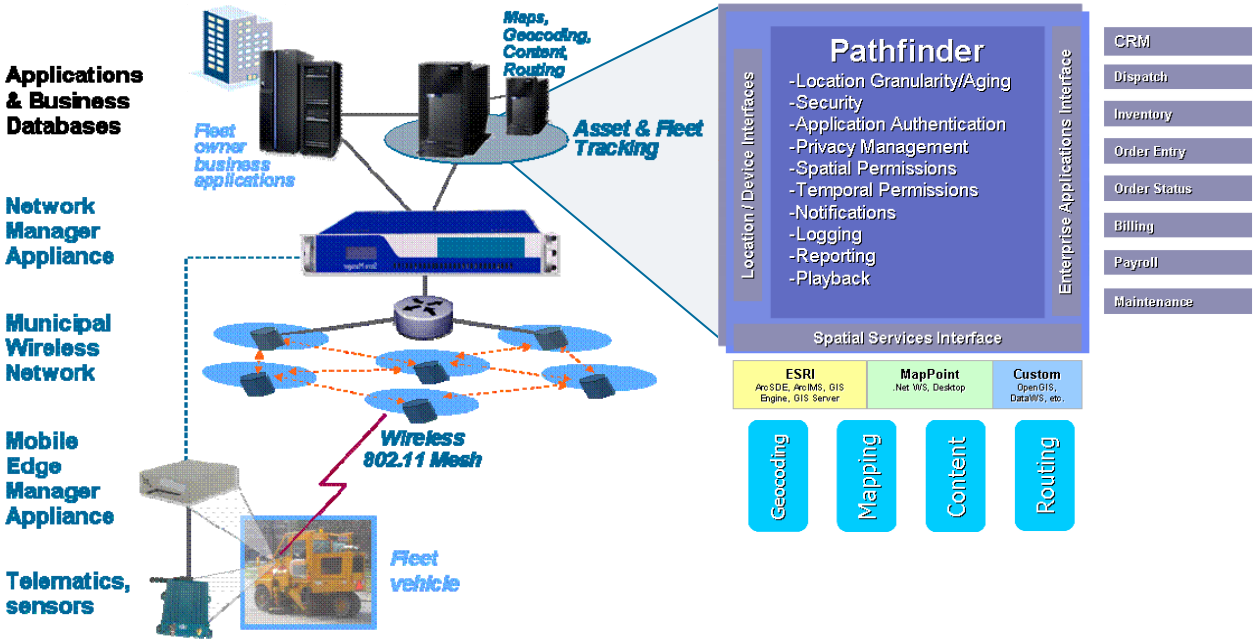

Figure 5: Enhanced location-based services utilizing the unified architecture

Pathfinder is a Java-based multi-purpose wireless and location enabling platform that is deployed, managed and controlled by the enterprise or an ASP operator to manage location-based services on behalf of their clients. Pathfinder is designed to meet the information needs of a business that utilizes a mobile workforce and/or fleet. The platform is flexible and can be configured to utilize and extend existing applications and infrastructure to minimize deployment costs and timeframes.

Pathfinder provides access to this wireless and location information to authorized users and/or "line of business" applications throughout the enterprise.

Pathfinder includes component solutions for:

- email, SMS and WAP notification service delivery,
- spatial service integration from one of a variety of sources,
- a flexible enterprise application interface that allow rapid wireless and location enabling of enterprise applications such as CRM, order entry & fulfillment, maintenance, billings, and payroll.

The robust authentication and security components allow selective and secure customer access to location information and other status, scheduling information which can provide a powerful opportunity to differentiate services in a competitive market.

Key features of the Pathfinder platform include:

- Notification Gateways
  - Device and user notifications can be created and sent through Pathfinder based on temporal and spatial event triggers. Email, SMS and WAP interfaces and gateways are supported.
  - In addition, instant messaging and integrated messaging services embedded within applications are also supported via Web Services APIs.
- Spatial Services
  - The AppLocation Pathfinder platform includes mapping functionality that allows viewing of unit locations on a dynamic map display that allows traditional computer mapping features such as zooming, panning and changing displayed map layer data. Additional unit information is displayed including unit status, latitude, longitude, last report time, speed, and heading.
  - The proposed map display component could use ESRI, AutoDesk, or other existing GIS packages to generate web enabled map images. Or it can also be configured to utilize external sources such as Microsoft's MapPoint web service. Either implementation will include street and road networks, major facilities and landmarks, and geocode and routing services. The platform mapping features also provide custom and dynamic layer generation to support AVL enabled units overlaid with differentiation of vehicle types by using different icons.
- Security
  - All applications written on the Pathfinder platform use authentication, authorization, and auditing mechanisms built into Pathfinder. Users must log in using a username and password. Additionally, the application will revoke user access after a configurable inactivity time to prevent unauthorized access.
  - Pathfinder stores its location and telemetric data in a protected database that requires a minimum of username, password authentication. In addition access to the database is restricted to the servers that host Pathfinder.
- Reporting and Playback/History
  - Pathfinder supports a wide range of reporting requirements including detailed, transaction and access based reports, trip and stop reporting or exception, fuel tax, status or event reports.
  - Pathfinder integrates historical and real-time location information to efficiently enable enterprises to review their operations at regular intervals. Historical location records can be accessed through spatial services or reports to support general time/space analysis, trip reporting, and customer billing validation or regulatory agency compliance.

Nortel Networks Confidential

- Pathfinder can easily be integrated into existing LOB applications to improve or extend their current reporting capabilities. Pathfinder supports Oracle, MS SQL Server, and PostgreSQL databases or can be configured to also provide reporting independently of existing applications.

Sample Location/RFID/Sensor services: Yard Management, Inventory, Asset management, & Site Access Services

Government or business entities that have large outdoor spaces may also benefit from being able to track people and assets within their campus or compound, called yard management services. The Broadband Wireless network can provide secure wireless coverage for these outdoor spaces to provide comprehensive yard management services or just basic connectivity for any 802.11-enabled device within the space. Trucks or any other mobile asset or person can also be tracked and monitored inside a yard or when entering or exiting, for improved yard utilization, asset visibility, locating people, and for theft deterrence.

Sample target businesses for yard management services

Locating trucks, containers	Distribution centers, logistics companies
	Bus companies
	DOT depots
Tracking large mobile assets	Airports, seaports
Locating people	Events
	Theme parks, attractions, city-wide tourist location services

Benefits of yard management services to end customers:

- Improved asset utilization: Where is the nearest available baggage cart? How long are assets idle?
- Improved yard utilization: Which parking spots are available? Who parked in the wrong spot?
- Enhanced customer and local tourist service: Which restaurants are close to my current location and what kind of food do they serve?
- Improved efficiency: Where is truck xyz? Where is container 123? Which truck is in the wrong lane?
- Real-time time-and-motion studies for fuel and time savings or visibility of customer behavior: How much are paths overlapping? Where do people congregate?

With the same unified architecture, we can also offer a variety of inventory, asset management, and site access services using RFID and sensors for businesses and for the town. We provide an integrated portal solution that can be placed at any chokepoint, such as gate entry/exit points, cargo docking bays, room entryways.

Wireless network coverage is utilized to provide connectivity or fully managed services for chokepoint portals that are within the Broadband Wireless service area. In addition, by using stacked chokepoints, assets can be located or managed by zone. Using portals at chokepoints, any information associated with an asset can be collected when the asset goes through the chokepoint. This could be information on its identity and current status, using RFID and sensors or telemetric data, or could also include any information collected since the asset last went through the chokepoint.

Customers subscribing to services enabled by this RFID and sensor solution can save significant operations and capital costs through improved utilization of shared assets, improved visibility of inventory, ability to monitor the environment of sensitive assets and inventory, ability to quickly locate people and assets quickly when needed, automation of administrative processes, and theft deterrence.

Sample target businesses for asset management, inventory & site access services

Secure access: Truck gate in/out	Distribution centers, logistics companies
	Airports, seaports
	Public utility, oil & gas facilities
	Oil & gas facilities
Secure access: Truck id, contents, weight	Customs & border protection
	Weigh stations
Asset management: Shared or high-value assets in/out	City government depot, Dept of Transportation depot
	Retail stores (shopping carts), Hospitals (wheelchairs, etc)
	Businesses with laptops
Asset management: People tracking	Prisons
	Patients and staff in hospitals, mines, teachers in schools
	Museums
Inventory management: Pallet in/out	Retail distribution centers, grocery stores, pharmacies
	CPG, Pharmaceuticals, and electronics manufacturing
	Hospitals
Inventory management: Container in/out	Reusable containers for chemicals
	Beer distribution (kegs)
Inventory mgmt: Auto-checkout	Libraries

Nortel Networks Confidential

Sample benefits to end customers include the automation of security and business processes:

- Enhanced efficiency of security processes: Is driver tag xyz allowed access? Is driver xyz expected to be bringing container with tag abc today? Which lane should driver xyz with container abc be directed to?
- Improved efficiency of business processes: How many containers have been returned and must be cleaned in order to meet customer requirements today?
- Reduced theft: A chainsaw or laptop is leaving the yard—is it with an employee —who? How many wheelchairs left the building and need to be retrieved?
- Improved inventory visibility: What are the contents of pallet 123? Was pallet 123 expected today? When do the contents of pallet 123 expire? Which order should these pallets be opened? What departments do the contents of these pallets go to?
- Improved asset utilization: Which bus is still in the yard? Did the bus have any fuel when it last entered the yard?
- Improved safety and security: Which room did the teacher that called 911 using her SIP wireless phone enter? Is that person allowed access to area z?
- Post time-and-motion studies for fuel and time savings: Which route did the delivery truck take today and how much fuel did that use, how does that compare to other routes?
- Post proof of performance: Which streets were cleaned? How many buses were on time?
- For customers that are already subscribing to fleet management and/or yard management services, addition of a chokepoint solution at the entrance/exit of a yard or depot is highly complementary and can provide additional control of assets.
- These asset tracking, RFID and sensor services are just some examples of the many services that we can develop in partnership with MBI.

Inventory, Asset Management, and Site Access Services through Blue Vector

Nortel partners with Blue Vector to provide Inventory, Asset Management, and Site Access Services.

Our chokepoint architecture can be customized to provide a variety of inventory, asset management, and site access services. We provide an integrated portal solution that can be placed at any chokepoint, such as gate entry/exit points, cargo docking bays, room entryways.

Nortel Networks Confidential

Broadband Wireless service providers can leverage their wireless network coverage to provide connectivity or fully managed services for chokepoint portals that are within their service area. In addition, by using stacked chokepoints, assets can be located or managed by zone.

Each portal includes a Blue Vector Edge Manager Appliance and RFID reader, and is prepped with power and a wired or wireless 802.11 Ethernet network connection. Each fixed portal is bolted into the floor as close to a wall as possible, and is typically protected by a bollard. Mobile readers can be placed in hardened enclosures and subsequently mounted on forklifts or other cargo transport vehicles.

RFID readers and tags come from various vendors: Symbol, Alien Technologies, Intelleflex, Identec, ThingMagic. RFID tags come in various types (passive, semi-passive, active) and form factors (badge, square, rectangle, low profile label). It is not uncommon for a business to deploy different types of RFID tags for different purposes.

This will become a normal operations practice as RFID processes enjoy greater adoption. Even in the near term, businesses will need a system that helps to manage growing heterogeneous RFID and sensory device deployments. This solution will support any reader and tag vendor or type, and still allow us to provide comprehensive managed services to businesses and the town.

RFID tags are placed on containers, pallets, vehicles, or people that will be going through the chokepoints. The strategic portal point placements are referred hereto as 'points of automation' (POAs). Note that POAs are points where RFID reads will take place. However, POAs are also points where specific business processes can be applied; thus automating each point and not just simply reading an RFID tag.

Nortel Networks Confidential

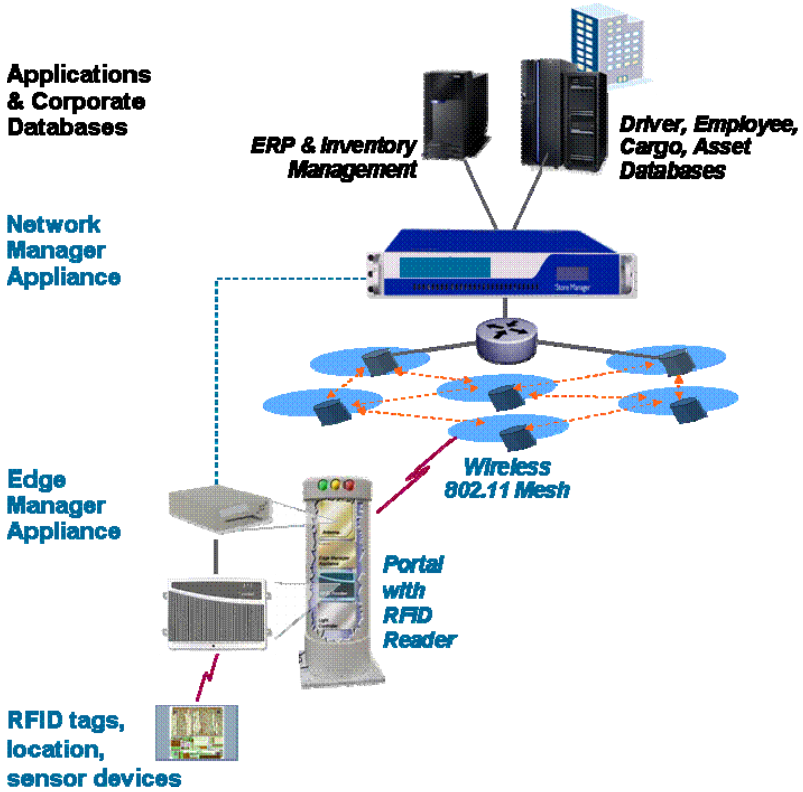

Figure 6: Chokepoint solutions for managed RFID, sensor, and zone location services utilizing the unified architecture