



>THIS IS THE WAY

WLAN SOLUTIONS ALLOW OPERATIONAL SAVINGS AND PRODUCTIVITY, WITHOUT COMPROMISING SECURITY AND CONTROL

>THIS IS NORTEL™

Position Paper

WLANs— The power of one network

Securing and scaling the Wireless LAN

First-generation Wireless LAN (WLAN) systems were all about basic standards, connectivity and end-user productivity. They did not address a number of key enterprise requirements. Second-generation WLAN systems are all about enhanced standards addressing security, Quality of Service (QoS), interoperability, enterprise-wide roaming and architected solutions with placement of functionality for optimal price, performance and control. This paper describes Nortel's second-generation secure WLAN architecture, which is centered on the networking element — the WLAN Security Switch. Deployment of second-generation WLAN solutions will lay the groundwork for third-generation WLANs, which will be highly integrated and include support for seamless roaming across public and private networks. This position paper focuses on addressing the

challenges and issues of today's enterprise WLAN environments through second-generation WLAN architecture and solutions. This position paper should be of interest to IT professionals, whether they are aggressively rolling out WLANs or are considering what they should do and how.

The Wireless LANscape

Modern business requires mobility and always-on connectivity to compete. Cell phones and PDAs have become indispensable for business. Laptop computers give us the mobility to allow us to take our work with us — whether to a conference room, home or around the world.



Wireless LANs, now a standard feature of many PDAs and laptops, are being deployed particularly in hospitals, universities, homes and in thousands of hotspots in coffee shops, hotels and airports.

Consider the following:

Challenge: You need to stay connected to information as you roam the building, factory, hospital, store or campus with instant access to corporate information and applications.

Solution: With WLANs as an extension of the IT infrastructure, your information is where you are, with instant access. *Win time. Gain business agility.*

Challenge: You are in an executive meeting and discover you are missing important information on your laptop. It would be awkward to leave the meeting to search for a working Ethernet jack.

Solution: With a WLAN, you can discretely connect and instantly retrieve the information you need without leaving the meeting. *Win time. Make informed decisions.*

Challenge: You are on the way to the airport after a customer meeting in a city, and the phone rings. You have to send some key documentation you have on your laptop to the customer within the hour, or lose the bid to the competition.

Solution: With WLAN access in the airport business lounge, you securely tunnel to the enterprise. *Win time. Win business.*

Infotech estimates that there will be over 25 million WLAN users globally by 2008.[†] WLANs offer a new dimension in productivity for business users. A Gartner study suggested that enterprises could expect a 22 percent productivity improvement by introducing WLANs.^{††}

Users clearly see benefits and certain industries, such as education and retail, have been proactive on deployment. WLANs can provide mobile, high-speed connectivity when and where needed for IP Telephony, unified messaging and business applications, and extend and leverage the ubiquity of Ethernet networks and the Internet. WLANs extend the plug-and-play nature of Ethernet.

Gartner Group says that, “The notion of the office as a fixed location will give way to a situation where ‘office’ is just the act of paying attention to work through always-on access.”^{††} So why then haven’t enterprises generally embraced WLANs as an intrinsic part of their IT infrastructure?

One of the major issues is **security**. WLAN signals broadcasting and receiving over the air via radio waves have no physical barrier to an unauthorized user. Unfortunately, these signals are subject to interception, exposing the enterprise to the possibility of intrusions and other threats.

Enterprises understand that adding a wireless node to the corporate network must include appropriate security precautions and good security practices. They also need a WLAN solution flexible enough to be deployed in harmony with their current wired infrastructure and as simple as the LAN to manage, even across the air in the RF (Radio Frequency) domain.

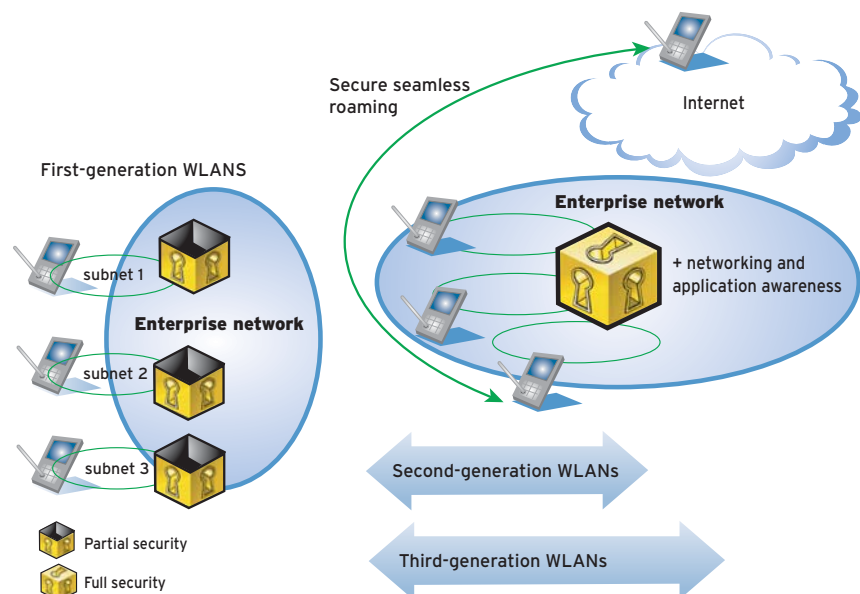
Three generations of WLANs

From an architectural and technological perspective, Nortel sees the evolution of WLANs in the enterprise market over three generations (Figure 1).

First-generation WLAN systems were all about basic connectivity standards and end-user productivity, much the way Ethernet in its early days evolved around ad hoc networking, sharing network resources and unstructured wiring. This is also how the Internet started.

This represents yesterday’s environment. These first-generation systems partially addressed security needs through proprietary designs.

Figure 1. Three generations of WLAN solutions for the enterprise



First generation of IEEE WLAN standards

802.11: Family of WLAN standards that originally operated at 1-2 Mbps.

802.11a: A physical layer extension standard for WLANs supporting 54-Mbps operation in the unlicensed 5-GHz radio band. It solves interference problems encountered in the 2.4-GHz radio band. 802.11a is prohibited in some countries due to conflicting spectrum use.

802.11b: A physical layer extension for WLANs supporting 11-Mbps operation in the unlicensed 2.4-GHz radio band. It is the most deployed technology.

Wi-Fi® Alliance (previously the Wireless Ethernet Compatibility Alliance): A nonprofit international association formed to certify interoperability of WLAN products based on IEEE 802.11 specifications.

Second-generation WLAN systems are all about enhanced standards addressing security, QoS and interoperability, and architected solutions with placement of functionality for optimal price, performance and control. In second-generation systems, the WLAN is as safe as using a LAN. IP mobility opens the door for roaming across the enterprise, not just across a few wireless cells. This phase is quite analogous to the widespread adoption of in-building Layer 2-7 architectures based on switched Ethernet and hierarchical campus networks built around routing switches.

This represents today's opportunity.

Third-generation WLAN systems are all about bringing down the boundaries between enterprise WLAN systems and public wireless systems for seamless roaming, security, consistent service offering, single sign-on and billing. Next-generation (so-called 3G and 4G) public wireless systems and a plethora of new mobility devices will have a dramatic

impact on the way business works, delivering up to 2 Mbps throughput for data. This represents tomorrow's opportunity, driven first by WLAN private network integration with public wireless services.

WLAN Deployment 101

WLAN technologies are implemented using multiple access points (APs) to provide the required coverage and capacity. Generally, the access point is the bridge for the end clients — for example, a notebook PC — to access the enterprise network. An access point has an antenna and RF capabilities, allowing operation predominantly in the 2.4-GHz band with 11 Mbps per radio channel (IEEE 802.11b). A typical ratio of WLAN clients to access points is 10:1, although this varies between technologies and vendors. Overlapping access point cells of coverage are created when multiple access points exist around the floor or building, creating a single coverage area for mobile users.

First-generation WLANs lead to unstructured deployments

In the first generation of WLANs, the world of wireless data networking was dominated by proprietary niche products that targeted specific vertical markets. The development and wide vendor acceptance of WLAN IEEE 802.11 standards has changed this, and resulted in increased availability of PC and PDA interface cards and plummeting prices. Standards such as 802.11a and b (see sidebars on IEEE 802.11 standards) delivered speed and connectivity, and end users loved it. The benefits to end users pushed WLAN deployments in select areas around the enterprise (e.g., executive offices and conference rooms). However, the standards did not solve everything — and in fact, the first standards were found to have many shortcomings. Worse, the deployment of access points and security mechanisms was done in an ad hoc fashion, leaving IT departments with issues on a number of fronts.

First-generation challenges

Lack of security: Security exposures of using WLANs have been well documented, including identifying nonsecure APs by ‘war-driving’ and ‘war-chalking’, the inadvertent insertion of free agent access points and the malicious insertion of rogue access points. Wired Equivalent Privacy (WEP), the primary security mechanism shipped with most WLAN products, has proven to be non-secure and opens up the network to unauthorized access, session hijacking, eavesdropping and other threats.

Limited secure mobility: WLAN users cannot generally move between subnets without re-authenticating themselves with the network. Lack of multi-vendor interoperability across WLAN APs limits roaming to the area covered by one vendor.

Lack of access and bandwidth controls: All WLAN users often have equal privileges on the access point; this precludes handling application traffic in the optimal way to meet performance and security needs such as offering visitors and contractors restricted WLAN access (e.g., for Internet access).

No QoS for multimedia applications and IP Telephony: Mobility and always-on access are one of the drivers behind IP Telephony. As a shared-media LAN topology, first-generation WLANs are a poor infrastructure over which to extend converged networking: lack of QoS and bandwidth controls result in poor fidelity and lost calls.

Requirement for AC powering: Bringing AC power to every AP is a major upfront cost and bottleneck to rapid expansion. The IEEE-802.3af Power over Ethernet standard is a new opportunity not supported by first-generation WLANs.

Unscalable management capabilities:

As unbounded WLAN deployment continues, configuring and managing WLANs is becoming increasingly difficult — a problem exacerbated by the lack of adequate security, access and bandwidth controls. For example, if there is no ability to control users from hogging the wireless bandwidth, overall WLAN performance is impacted and audit trails are non-existent. Sometimes, even knowing where access points are physically located is a challenge.

Proprietary designs: While the initial costs of WLANs are coming down (\$0 for new laptops with built-in WLAN capabilities and under \$100 for low-end APs), the long-term cost of ownership for proprietary solutions is not. Customers are locked-in with one vendor and forced to follow the evolution plan of that vendor — or throw out their original investment and start again.

Escalating cost of ownership: The ongoing system costs are escalating because of an unstructured approach to WLAN deployment. Simply adding more and more processing and memory to WLAN APs distributed on ceilings and walls, and around the office, laboratory and common space adds complexity and cost on an ongoing basis. The cost of locating and eliminating unregistered access points also adds to the cost of ownership (Figure 2).

Security solutions to first-generation challenges

The most burning issue to first-generation WLAN has been WLAN security. It is therefore not surprising that industrious enterprises have adopted various security solutions to their WLAN deployments.

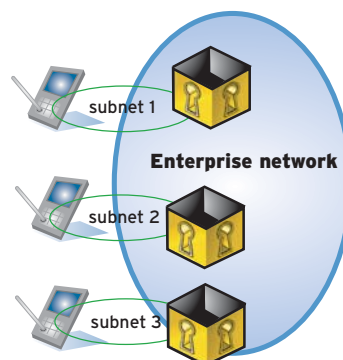
Some examples follow:

DMZ isolation: This approach uses VLANs to segregate the WLAN traffic and connect WLAN users to certain enterprise servers in a DMZ area outside the corporate firewall but separate from the DMZ for public Internet access. This prevents unauthorized users from using the corporate WLAN for Internet access, and protects the corporate LAN. The disadvantages of this approach are many, not the least of which is poor security.

RF isolation: This approach attempts to isolate the WLAN radio signals from the outside world — with a high gain directional antenna, an outsider who wishes to gain unauthorized access to the WLAN can reach a WLAN from many miles away.

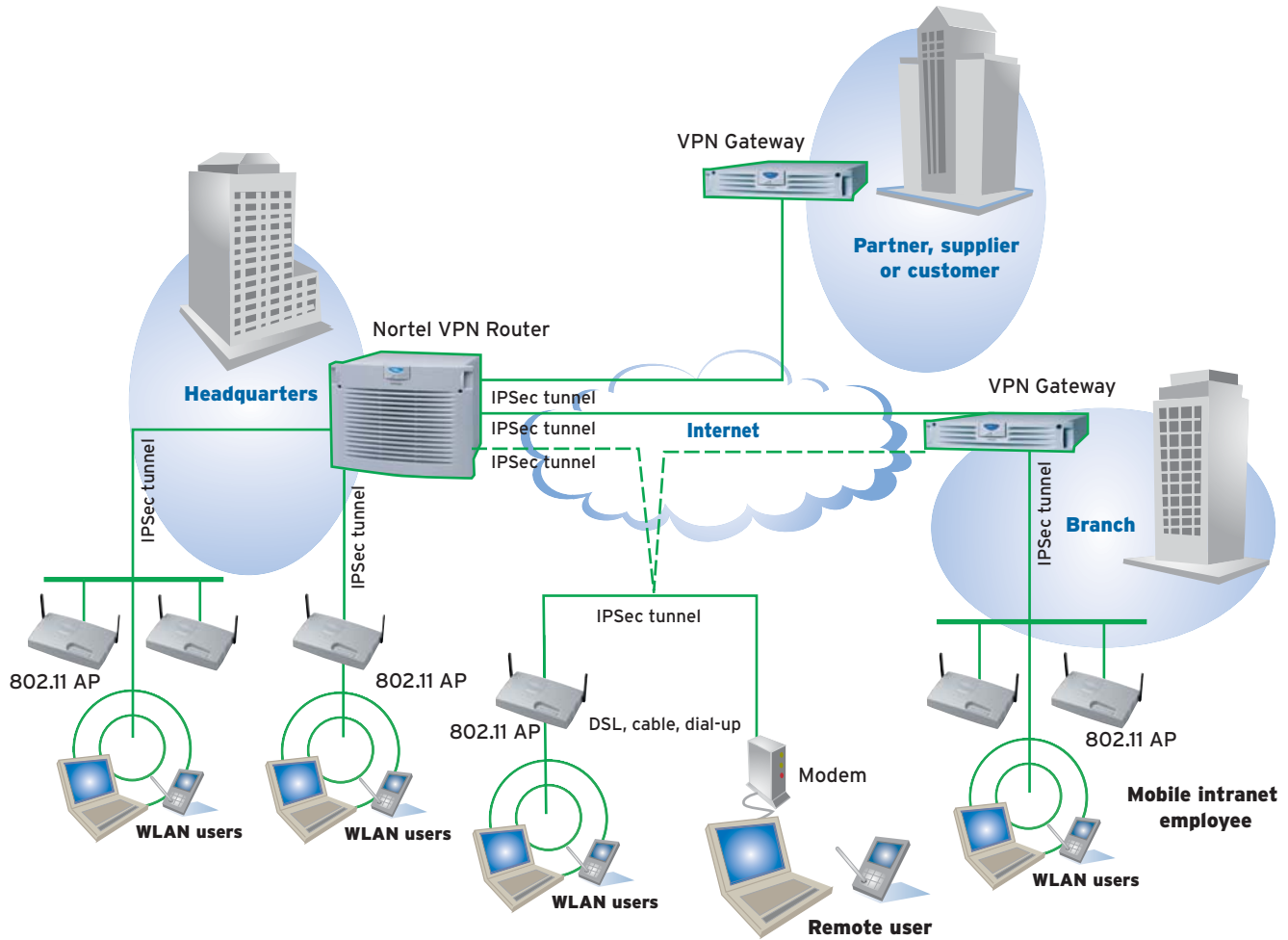
One method of blocking unauthorized outsiders from taking advantage of the open air availability is to provide a secure physical perimeter; another method is to surround the perimeter of the corporate grounds with APs that are not connected

Figure 2. Key challenges with first-generation WLANs



- Lack of security or limited security
- Limited secure mobility
- Lack of access and bandwidth controls
- No QoS for multimedia and IP Telephony
- Requirement for AC powering
- Unscalable management capabilities
- Proprietary designs
- Escalating cost of ownership

Figure 3. IP-VPN solutions — a single solution for remote access and WLANs



to the internal network. An outsider is blocked from seeing the internal WLAN because the outside APs operate at the same carrier frequency as the internal ones and offer a higher signal strength to the outsider, thereby in effect “jamming” the internal signal for the outsider. The disadvantage of this approach is that it is not only expensive, but it cannot be 100 percent effective.

Proprietary security: Some WLAN vendors have developed their own security solutions. Most are vaguely ‘standards based’, are not interoperable with other vendors’ solutions and carry a high price tag. Often these solutions are implemented in the access points themselves, complicating management, increasing

costs and sometimes requiring hardware upgrades. Clearly, these stop-gap approaches incur a total cost of ownership penalty and are costly to maintain and difficult to evolve.

IP-VPNs: IP-VPNs were developed to initially meet the needs of secure remote access over the Internet, and enterprises have favored this technology for adding security to WLAN deployments. Enterprises have either leveraged their investments in Secure IP Services Gateways, such as Nortel VPN Router (formerly known as Contivity*) (there are over 60 million Nortel VPN Routers clients in enterprise networks), or they have deployed additional units close to the WLAN APs.

IP-VPN-based wireless security is platform and radio technology-agnostic; that is, the client system establishes a connection to the network via the WLAN, and the VPN takes over from there. Once the wireless connection is established, users trying to access the network are first authenticated (exactly as if they were accessing the enterprise across the Internet), their information is encrypted and all communication logged by the VPN server. In addition, Nortel VPN Router provides QoS and bandwidth management if required. This approach solves many of the challenges of enterprise WLANs and in fact is a solid standards-based element of Nortel’s second-generation architecture, discussed later in this paper (Figure 3).

Nortel VPN Router highlights

- › Multi-OS client support and single solution for Internet and WLAN access
- › Integrated security services: AAA, IPSec, stateful firewall, NAT
- › Secure Routing Technology, including dynamic routing over secure tunnels
- › Full QoS and adaptive bandwidth management
- › DHCP relay
- › Seamless handling of voice and data
- › Configurations from SoHo to campus supporting up to 5,000 tunnels

WLANs need to be brought into the mainstream of LAN and IT infrastructures as a critical feature-rich resource that can be planned, secured and managed. This drives the development of WLAN standards and a second-generation architecture that is secure, manageable and flexible.

Second-generation WLAN — One secure architecture to put IT back in control

The foundation of second-generation WLAN solutions that meet the needs of enterprises are standards. The IEEE 802.11 committee has responded to the needs of second-generation WLAN users by undertaking the development of a number of new standards which complement IEEE 802.11a and 11b. Most notable among these is 802.11i, which establishes a robust WLAN infrastructure for security. Other standards address WLAN QoS to allow IP Telephony and multimedia application support, and multi-vendor interoperability of roaming handovers across access points.

All these standards present a challenge of determining which standard to use when and where. The second-generation WLAN solutions need to be flexible enough to adapt and support all or part of them.

A layered architecture

Enterprises need one standards-based secure WLAN architecture that supports WLANs as an inherent manageable and secure part of their infrastructure. The requirements of such an architecture must address the issues associated with first-generation WLAN systems, recognizing that a layered approach to WLAN functionality, including security, is required to meet the varying needs of enterprises.

Nortel offers both distributed and centralized architectures to solve the security and flexibility issues of first-

generation WLAN systems (Figure 4).

The distributed architecture is a **stand-alone** solution, consisting of access points directly connected to the LAN. All the security features are processed at this entry point. The centralized architecture goes a step further — solving the management issues and providing greater benefits in terms of flexibility and security — even into the RF domain.

The centralized architecture requires a network platform which centralizes the management and policies for the access points. It even provides additional features.

Figure 4. Nortel solutions



Nortel's second-generation WLAN, when deployed in a centralized architecture, includes two solutions:

> The **Hybrid solution** is based on Nortel WLAN Access Point 2220 and Security Switch 2250. This solution provides a LAN-like experience, extending the reach of the LAN to wireless transparently. It offers a low-cost solution for defined WLAN coverage while providing secure services. As it is compatible with first-generation products, it can be added to existing WLANs to address the issues encountered in first-generation WLAN deployments.

> The **Adaptive solution** is based on Nortel WLAN Access Ports 2230 and Security Switch 2270. This solution extends the LAN and offers RF-specific functions. Thanks to real-time air monitoring, it can perform dynamic coverage, avoiding costly site surveys and maintenance costs in changing environments. Thus the network security starts over the air.

Nortel's centralized WLAN architecture is based on a layered secure approach both physically and functionally. This allows the optimal distribution of functionality and security for performance and low total cost of ownership. It builds on Nortel's Unified Security

Framework, and particularly on the principles of variable depth security, closed loop policy management, and uniform access management.

Nortel's Unified Security Framework provides a conceptual, physical and procedural framework of best recommendations and solutions for enterprise network security and serves as an important reference guide for IT professionals responsible for designing and implementing secure networks.

Access points compose the first layer of Nortel's second-generation WLAN solution, providing secure **wireless connectivity** to roaming mobile users equipped

Second-generation evolving IEEE WLAN standards

802.11d: A supplementary 802.11 standard to allow global roaming clients. It will allow access points to communicate information on the permissible radio channels with acceptable power levels.

802.11e: A supplementary 802.11 standard to provide QoS support, differentiating data streams based on the application used (data, voice...). Wireless Multimedia Extensions (WME) is a subset of 802.11e deployed to support multimedia applications while waiting for the standard to be ratified.

802.11f: This is a "recommended practice" document that aims to achieve access point interoperability within a multi-vendor WLAN network by defining a common IAPP (Inter AP Protocol).

802.11g: A physical layer extension for WLANs supporting 54-Mbps operation in the unlicensed 2.4-GHz radio band. It is backward compatible with 802.11b.

802.11h: A supplementary 802.11 standard to comply with European regulations for 5-GHz WLANs limiting transmit power and selecting the channel for lowest interference with other systems (e.g., radar).

802.11i: A supplementary 802.11 standard to provide highly secure authentication and encryption. Wi-Fi Protected Access (WPA) is the subset of 802.11i deployed while waiting for the standard to be ratified.

802.1x: IEEE 802.1x provides authentication/access control for the access points through the use of the Extensible Authentication Protocol (EAP), which is a set of messages for authentication negotiation and authentication transport method between client and server.

with laptops, PDAs and telephones. These access points, such as Nortel WLAN Access Point 2220 and Access Port 2230, are designed to evolve to support new wireless standards and technologies that allow more effective use of the radio spectrum and provide security over the radio link. Adding functionality to access points above the first or second layer (even if feasible) has a significant impact on TCO, because of the highly distributed nature of AP deployment.

In addition, certain functions, such as enterprise-wide roaming (and ultimately seamless roaming across enterprise and public domains), can be better handled in more centralized devices that support multiple APs.

The second layer of Nortel's solution is **wired Ethernet** networking, which has support for Power over Ethernet, Virtual LAN (VLAN) segmentation and QoS capabilities. In the Hybrid solution, this layer is handled by the WLAN Access Point 2220 whereas in the Adaptive solution, the Access Port 2230 focuses on monitoring the air and adapting accordingly; the layer Wired Ethernet is managed by the Security Switch 2270. Access Points or Access Ports are connected to Ethernet switches which provide Power over Ethernet (using the IEEE 802.3af standard). These Ethernet switches (e.g., Nortel Ethernet Switch 460-24T-PWR [formerly known as BayStack*] or Ethernet Routing Switch 8300 [formerly known as Passport* 8300 Ethernet Switch]) are either dedicated for WLAN aggregation or are shared with the wired LAN network with segregation provided via VLANs. The advantage of using these proven high-performance devices is that the enterprise has the choice of where and how it wants to integrate WLANs into the basic wired Ethernet infrastructure. It also allows a common Power over

Ethernet technology to be used consistently for wired and wireless environments.

The third layer provides **networking and application-aware security** at Layer 3-7 of the OSI model. Nortel calls its product realization of this Nortel WLAN Security Switches 2250 and 2270, WLAN optimized purpose-built Layer 2-7 secure platforms.

WLAN Security Switches interface to the enterprise and to policy management, including directories and policy servers, which constitute the fourth layer of the architecture.

Nortel's four-layer WLAN architecture provides a high degree of flexibility while meeting the needs of the enterprise for secure WLAN access. It is complemented by access control, which authenticates all users and authorizes which network resources are accessible, and by network management for both the wireless and wired portions of the network (Figure 5).

As the deployment of WLANs grows, it becomes increasingly important to establish a comprehensive set of scalable management capabilities that make it easier to plan, configure and operate WLANs in the context of the enterprise environment. These ensure that WLAN solutions grow and adapt to changing network requirements. Continuing to

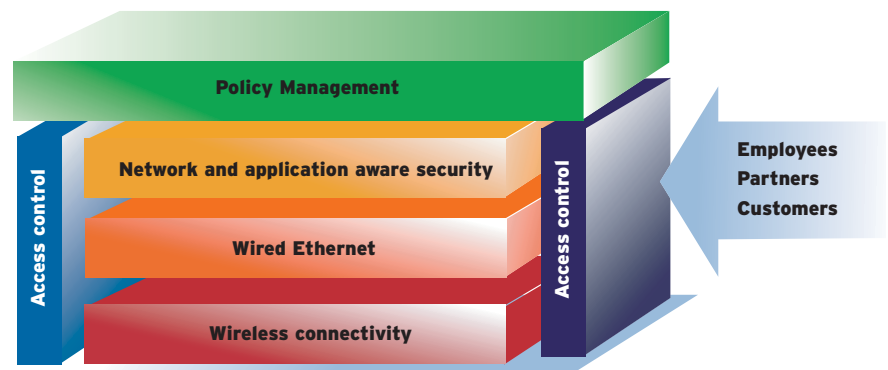
add cost and complexity to APs scattered across the enterprise will exacerbate these management objectives. This layered architecture is designed for business and technology flexibility. It delivers total cost of ownership reduction — achieved by leveraging standards, vendor interoperability, the existing wired management and networking infrastructure — by minimizing the churn on access points, and by establishing an architecture that is easier to plan, configure, secure and operate.

How the Hybrid and Adaptive WLAN solutions address the other challenges of first-generation WLAN systems is further discussed below.

Enterprise security — Authentication: Enterprise security includes flexible device and user authentication, and single sign-on. Authentication can be applied at the radio, networking and/or application layer. User/device authentication is integrated into the enterprise authentication architecture and centralized for ease of management, using standards such as RADIUS.

Once the user has been authenticated, access control mechanisms ensure that the user (perhaps based on the user group membership) only has access to resources specified in the policy server. Enforcing who can access your network via the Wireless LAN is a vital component to any security policy.

Figure 5. Nortel's layered architecture for secure WLANs



In addition, the WLAN Security Switch 2250 captures the user's browser to force the authentication before accessing network resources. Once the session is captured, a portal is displayed allowing the user to enter his/her credentials, and, once received, match it against information in a directory. Users are authenticated via a built-in database or via existing central authentication servers such as LDAP, RADIUS, Windows NT Domain and Active Directory. The WLAN Security Switch 2250 supports a wide range of authentication methods including passwords, smart cards, certificates and tokens, as well as combinations of these methods. If the user fails to authenticate, then custom pages or actions can be taken, such as a personalized error message, a request to contact support or to reset a password.

Detecting unauthorized access points, including free agent APs deployed by well-meaning employees, is done by monitoring the air and the wired network. The WLAN Security Switches 2250 and 2270 can detect unauthorized APs and block the traffic of free agent APs over the LAN. Additionally, the WLAN Security Switch 2270 can perform air containment on access ports not connected to the LAN (rogue access ports), thus preventing users from associating with them.

Enterprise security — Encryption: It will take years before enterprises will develop enough confidence to treat WLANs equivalently to wired desktops. Even IEEE 802.11i is not sufficient as it ensures encryption over the air interface but does not protect against LAN attacks, denial of service attacks over the air or unauthorized access points. Therefore, a layered security approach can address the current installed base weaknesses and RF-specific features can start this protection over the air rather than at the LAN entrance.

Nortel WLAN 2200 Series highlights

- Unified Optivity* management (for wired and wireless)
- Multi-mode operation (802.11a and b) plus TurboMode extensions (108 Mbps on both 2.4- and 5-GHz bands)
- International compliance (IEEE 802.11d)
- Wi-Fi certified: WPA, WME, 802.11f soon 802.11i and 802.11e
- Radio power adjustment
- Highly reliable platforms
- Non-service affecting software upgrades
- Full enterprise-wide mobility (across radio modes, across AP, across IP subnets)
- Unauthorized AP detection and disconnection
- Security filters
- VPN encryption
- User groups management (access rights, QoS)

Additional Adaptive solution features

- Dynamic coverage (hole detection and compensation, RF channels allocation for interference avoidance)
- Unauthorized AP containment
- Accurate location (unauthorized AP, E911 enabler, applications in healthcare or stock inventory)
- Load balancing between access ports

Nortel WLAN Security Switches support a range of encryption protocols, such as IPSec and SSL. IPSec VPNs operate at the network layer, are application agnostic, and require client software. For example, an IPSec-based VPN connection can be used to access e-mail, HR self-serve applications on the intranet and browse the Internet.

The WLAN Security Switch 2250 offers SSL VPNs operating at the session layer, and is designed for Web applications, extranets and limited application access. It doesn't require any special client software.

The SSL VPN approach is particularly attractive for scenarios where the enterprise wants the lowest-cost secure solution for limited application access. It is also useful where the enterprise doesn't own or control the remote access devices as would be the case for visiting customers, contractors or suppliers. With Mobile Adaptive Tunneling, the security level and performance of the connection can be tailored to the application. It detects and enforces access by different types of users (e.g., general employee and restricted guest access) using devices with different security capabilities (e.g., equipped with an IPSec VPN client) and requiring different network resources (Figure 6).

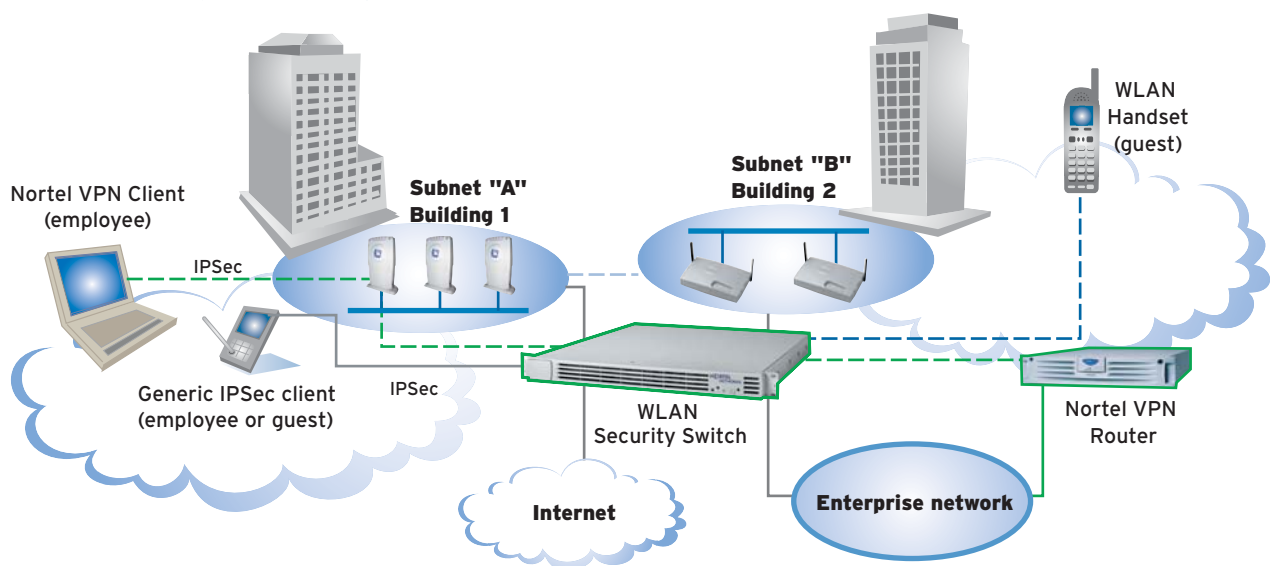
Nortel WLAN Security Switches 2250 and 2270 natively support IPSec VPN clients and provide IPSec passthrough to the installed base of Nortel VPN Routers (formerly known as Contivity). The advantages of this approach are consistency for remote, branch and WLAN users; simplified management; and investment protection. In cases in which IPSec VPN support is the only requirement, the Nortel VPN Router can continue to be used in the architecture.

Enterprise-wide roaming: Roaming allows the users to roam from one radio standard to another, from one cell to another and even from one floor to another in a building or campus, while maintaining the VPN session as they cross IP subnets. As a result, the current tasks such as synchronization of e-mail and streaming sessions are processed without interruption. Given the broad deployment of IEEE 802.11b APs and the increasing availability of multi-mode clients, seamless intra-subnet roaming is provided across IEEE 802.11a and 11b radios. User statistics such as usage, time and byte-based would be aggregated at one point. In addition, roaming is expanded beyond single subnet and single vendor connectivity. Several features enable solutions that meet the needs of the mobile users. The first is the Dynamic Host Control Protocol (DHCP- RFC 2132), which greatly eases the management of IP addresses by dynamically assigning IP addresses as required. The second is mobility. The WLAN Security Switches 2250 and 2270 ensure that authenticated and authorized users do not need to re-login to the existing security domain and that their packet flows and sessions are undisturbed while

moving from one IP subnet to another. This implies single sign-on capabilities and access and bandwidth controls that follow the user. The IAPP standard (Inter-AP Protocol, IEEE 802.11f) allows APs to hand over sessions to other APs while the WLAN Security Switches take care of the inter-IP subnet roaming. In the coming years, seamless roaming between private enterprise WLAN networks and the public networks (WLAN or cellular) will be widely deployed.

Extensive bandwidth and QoS controls: Authenticating users is only the first step in managing WLANs. Controls are enforced, stipulating which protocols, network resources and applications are available to each user. Bandwidth needs to be dynamically allocated depending on user profiles, the protocols used and the applications that are running. The WLAN Security Switches 2250 and 2270 provide comprehensive bandwidth management support at Layer 3-7, to ensure that certain users and applications are optimally served (such as voice calls or multimedia sessions), while other less-critical applications (Web browsing, for instance) and users (such as visitors) are capped from hogging the WLAN bandwidth. Bandwidth over the WLAN

Figure 6. Mobile Adaptive Tunneling





is allocated to ensure equitable and business-driven requirements are met.

In addition, QoS implemented across the enterprise network ensures that real-time applications have priority access to bandwidth resources across the WLAN and across the LAN network. This includes mapping of IEEE 802.11e across the WLAN to DiffServ QoS across the wired network.

RF Domain control for a faster deployment and cost-effective maintenance: IT managers also want to control the RF Domain but with minimum wireless knowledge and time investment. Thanks to fully automated features, Nortel WLAN Adaptive solution answers their expectations. IT managers want auto-detection and auto-configuration for their WLAN equipment.

Once activated, Nortel WLAN Access Port 2230 will automatically attach to the correct WLAN Security Switch 2270 and find the best channel available and appropriate radio power. The WLAN network is deployed and configured with the minimum of intervention.

Coverage is dynamic as the WLAN network evolves (e.g., addition of new access ports or additional users in certain areas), and thanks to permanent real-time air monitoring, interferences can be detected and avoided and coverage holes are automatically corrected.

Nortel WLAN Adaptive solution encourages a balanced user distribution across access ports, allowing customers to optimize the use of the radio resources. Customers define their radio requirements once and then the system adapts on an ongoing basis to match these criteria.

Implementing the second-generation secure WLAN architecture

Nortel's secure WLAN architecture has been defined to support mobile users and their radio-equipped laptops, PDAs and phones. Given that there is a large installed base of 802.11b systems and a growing base of 802.11a systems (within the premises and in hot spots around the world), Nortel WLAN solutions support multi-mode 802.11a/b operation with seamless roaming

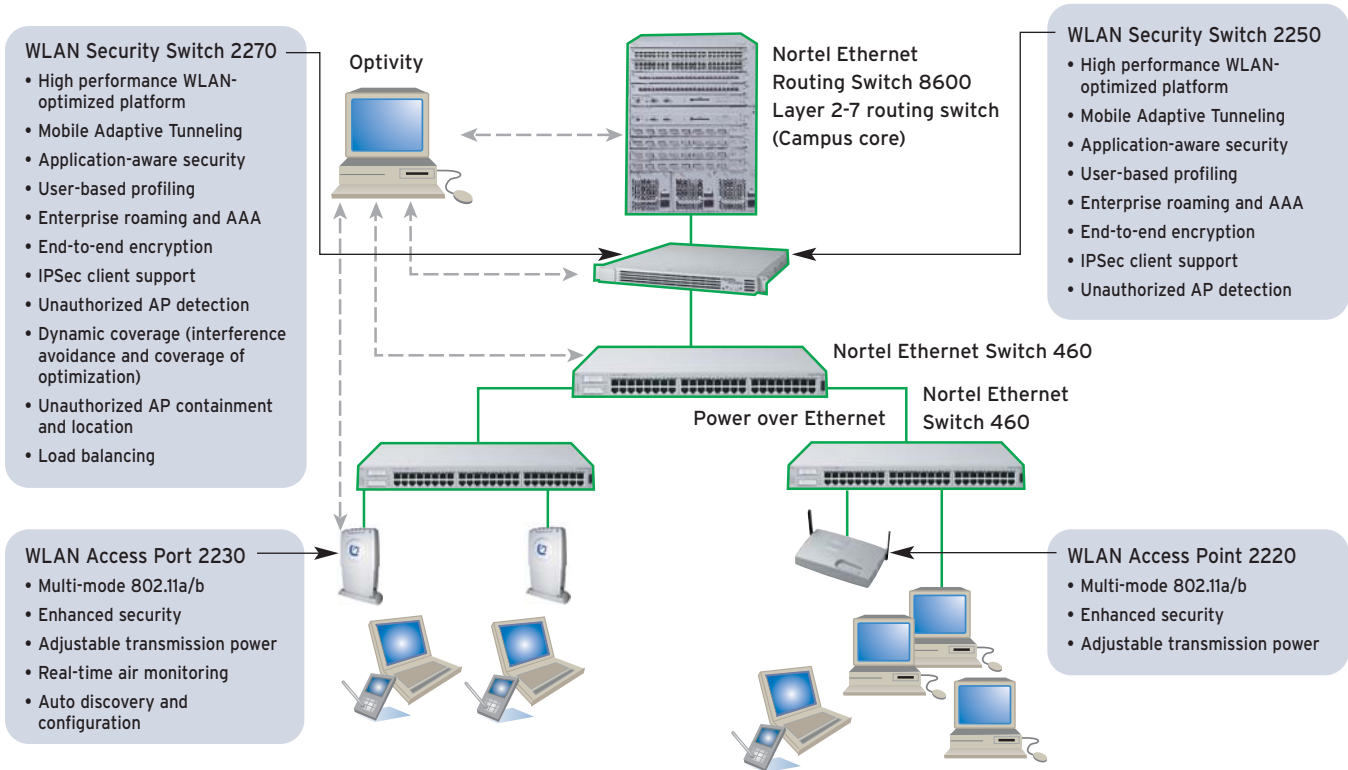
between these standards. These devices also support device and user authentication and encryption capabilities, and, in the case of PDAs and laptops, would include personal firewalls, anti-virus and intrusion detection software.

Access points and ports are optimized for high-performance networking over the radio waves, adjustable power and include the ability to provide seamless roaming across APs within the same IP subnet. While state-of-the-art APs will support both 5-GHz (802.11a) and 2.4-GHz (802.11b) radio bands, the actual radio spectrum configured in a particular AP may be impacted by reach, environment and interference from other sources — another good reason to have dual band mobile units. Access points and access ports also have to participate in enforcing user access control and QoS mechanisms, but to keep the total cost of ownership low, should otherwise be as simple as possible when it comes to heavy-duty security functions, bandwidth management and Layer 3-7 processing.

Wired Ethernet switches are deployed in secure wiring closets, which are within 100 meters of every AP and provide effective AP aggregation and VLAN-based segregation to the next layer of the architecture. These Ethernet switches participate in QoS handling, deliver Power over Ethernet technology and ensure that inter-mobile user communications is barred unless authorized by the WLAN Security Switches.

The WLAN Security Switches 2250 and 2270 integrate the functions of networking and application-aware security and access control. They support Authentication/Access Control/Auditing (AAA); heavy-duty security in the form of traffic encryption, firewalls, key management and secure adaptive tunneling tailored to the application and application-aware

Figure 7. WLAN 2200 Series



bandwidth management. The WLAN Security Switches 2250 and 2270 are also the focal point for mobility, providing roaming support across IP subnets enterprise-wide, and ultimately seamless mobility into the public wireless network. They also interface into the fourth layer of the architecture comprised of enterprise directories, policy servers and management systems.

The WLAN Security Switches 2250 and 2270 interface into policy management, which ensures that security parameters are set consistently across multiple nodes — and multiple policies for different administrative domains all reflect enterprise-wide policy and interdomain consistency. Policy management addresses the full realm of security components — firewalls, authentication techniques and more — along with a system-wide view of network environments, such as

data center, remote office, WLAN and campus networks.

Network management (e.g., Nortel Optivity* solutions) provides a common management infrastructure for both the wireless and wired enterprise network, with resulting operational and budgetary efficiencies, by delivering auto-discovery and fault, real-time performance and inventory management.

The realization of this architecture (Figure 7) delivers layered security, enterprise-wide roaming, extensive access, enhanced RF Domain control, bandwidth management, network management and QoS for converged, scalable WLANs. It allows the enterprise to optimally distribute WLAN functionality in a highly robust, secure environment for high performance and low total cost of ownership and maintenance.

Why Nortel Wireless LAN

Nortel understands the challenges faced by businesses in embracing WLANs for extended business connectivity, increased employee mobility, responsiveness and productivity. IT infrastructure including WLANs is no longer an adjunct support structure; it is the essential foundation for corporate performance.

How information is obtained, validated, stored, accessed and distributed — these issues are central to organizational survival and profitability.

Nortel has defined a vision for the enterprise network. One integrated network supports infrastructure convergence and eliminates boundaries between wired and wireless networks. The total solution delivers options on how enterprises integrate technologies to extend these capabilities across the enterprise,

and ultimately across public wireless networks as well. The vision is of a converged network that answers the critical business realities that strain and constrain today's networks. This includes a broad range of business connectivity solutions including Layer 2-7 wired and wireless campus solutions, metropolitan optical networks and secure routing solutions for the WAN.

Nortel WLAN 2200 Series, including the Hybrid solution (Mobile Adapter 2201 and 2202, Access Point 2220, Security Switch 2250) and Adaptive solution (Mobile Adapter 2201 and 2202, Access Port 2230, Security Switch 2270), deliver second-generation WLAN solutions that allow seamless roaming for voice and data within and across IP subnets and between IEEE 802.11 environments (a or b). Absolutely central to Nortel's vision is the principle that security is inherent to all applications and services — intrinsic to the very DNA of the network, whether wired or wireless. The WLAN 2200 Series delivers high-end enterprise-class security at both the network and application levels, consistent with Nortel's layered Unified Security Framework. This includes IEEE 802.1x, enhanced WEP with key rotation and WPA for added security. This portfolio also supports an extensive set of QoS, bandwidth management and access controls for wireless users. The control can be extended to the RF Domain for an adaptive WLAN network and protection starting over the air interface. Comprehensive network management is provided, complemented by fail-safe business continuity through redundant access point and Security Switch configurations. Nortel WLAN 2200 Series is complemented by a number of advanced business connectivity products, including:

- › The Nortel Ethernet Switch 460-24T-PWR, supporting Ethernet switching, QoS and delivering standards-based Power over Ethernet to WLAN APs. These can be used on a dedicated WLAN basis or, through VLANs, provide segregated WLAN aggregation on an integrated wireless and wired LAN infrastructure.
- › The Nortel VPN Router portfolio (including the Nortel VPN Client [formerly known as the Contivity Multi-OS VPN Client]), providing branch and remote access IPsec VPN, security and routing capabilities. These can be deployed behind the WLAN Security Switches with IPsec passthrough.
- › The Nortel Ethernet Routing Switch 8600 (formerly known as Passport 8600), deployed in campus backbones with its redundancy, high-capacity IP networking, Layer 2-3 switching and Layer 4-7 application switching, serving both wired and wireless users and servers.
- › Optivity Network Management, providing a common fault, performance and inventory management infrastructure for both the wireless and wired enterprise network, with resulting operational and budgetary efficiencies.

Nortel's vision consists of access points or access ports spread across the enterprise with the WLAN Security Switches 2250 and 2270 functionalities integrated into the enterprise infrastructure (e.g., into campus routing switches), with seamless roaming and mobile adaptive tunneling between the enterprise and public wireless networks. Look for third-generation WLAN systems from Nortel to deliver new levels of scalability and mobility for the enterprise.

Nortel WLAN solutions allow enterprises to realize operational savings and productivity for its users, without compromising security and control demanded of its networking infrastructure.

Inherent in our WLAN solutions are business-class capabilities that allow ease of management, scalability, service quality, seamless roaming, integrated security and future interworking with public wireless networks. Nortel is uniquely equipped to combine its unmatched breadth of expertise, its standards-based data networking solutions, its leading position across a broad security portfolio and its understanding of reliable converged networks to bring secure and scalable WLANs to businesses.

References:

“Wireless LANs in the Enterprise” (Nortel white paper: NN101960)

† “Monthly Market perspective — January 2004,” InfoTrack for Enterprise Mobility

†† “Key Technology Advances from 2003 to 2012,” Gartner Group report (4Q02)

In the United States:

Nortel
35 Davis Drive
Research Triangle Park, NC 27709 USA

In Canada:

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

In Caribbean and Latin America:

Nortel
1500 Concorde Terrace
Sunrise, FL 33323 USA

In Europe:

Nortel
Maidenhead Office Park, Westacott Way
Maidenhead Berkshire SL6 3QH UK

In Asia Pacific:

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

In Greater China:

Nortel
Sun Dong An Plaza
138 Wang Fu Jing Street
Beijing 100006, China
Phone: (86) 10 6528 8877

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

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

This is the Way. This is Nortel, Nortel, the Nortel logo, the Globemark, BayStack, Contivity, Optivity and Passport are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2004 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel assumes no responsibility for any errors that may appear in this document.

