

Intel and Cisco

Deploy Wireless LANs with Confidence: A Guide to Secure, End-to-End Wireless LAN Solutions

In a recent study of mobile PC users, research firm, NOP World Technology, reported that notebooks with wireless capabilities contributed to time savings of almost 80 minutes per employee per workday.¹ The implication of this time savings is clear — wireless mobile computing helps increase productivity.

How can a small- or medium-sized business (SMB) benefit from a wireless local area network (WLAN)? While an SMB can choose from numerous WLAN solutions, some of these solutions may be missing components that are critical for business environments. With security, interoperability, manageability, employee acceptance, and more at stake, it is vital that SMBs research their options before making a purchase decision.

This document outlines best-known practices and areas that SMBs should consider when choosing and deploying WLAN solutions. This guide will assist you in choosing a WLAN solution to meet your goals, whether your emphasis is employee productivity or protection of sensitive data.

SMBs require integrated, cost-effective, end-to-end network security solutions — whether wired or wireless — that provide outstanding value and predictable results. As Strategic Alliance Partners, Intel and Cisco® Systems are working together to enhance the availability of secure WLAN solutions that are appropriate for SMBs. The two companies are creating standards-based solutions through the Cisco® Compatible Extensions Program and the Intel Wireless Verification Program.

The Cisco Compatible Extensions Program is a global Cisco initiative to share technology and accelerate WLAN adoption in business environments. The technical features Cisco distributes to program members supplement Wi-Fi Alliance® certifications with Cisco innovations in areas such as security, mobility, and management. Support for Cisco Compatible Extensions features is built into Intel® Centrino™ mobile technology-based notebooks and other wireless devices to make sure they work smoothly with Cisco WLAN infrastructure products.⁵ As a lead collaborator of the Cisco Compatible Extensions Program, Intel Centrino mobile technology-based systems are compatible with Cisco WLAN products.

The Intel Wireless Verification Program tests Intel Centrino mobile technology with Cisco access points and third-party access points to verify compatibility. Intel Centrino mobile technology is verified to support leading wireless solutions such as the Cisco Wireless Security Suite, and Wi-Fi Protected Access* (WPA and 802.11i/WPA2).⁵ Verification means that access points have been tested and verified to work with notebooks built on Intel Centrino mobile technology. Through this Program, more than 56,000 hotspots worldwide have been verified.[†]

Recommendation #1: *To reap the productivity gains and long-term value that are possible with WLAN technology, choose wisely. Basic, off-the-shelf WLAN products may not offer the complete, interoperable, and secure solutions you need.*



Working Together to Enhance WLAN Security

Enhancing WLAN security requires going beyond deploying simple WLAN solutions and choosing current solutions that offer advanced management, encryption, and authentication technologies. Companies need to implement security best practices to protect their WLANs and keep their network secure.

Wired Equivalent Privacy (WEP), the IEEE 802.11 protocol for securing the original 802.11 standard, has been proven to be insecure and leaves networks vulnerable. Access points typically ship in open mode and require that the WLAN security features be enabled when they arrive. Companies need to ensure that this critical step is performed. Additionally, at some companies, employees (or occasionally intruders) may set up rogue or unauthorized access points that put the entire network at risk. As a result, WLANs that don't comply with current industry-standard security certifications such as WPA and companies that don't deploy WLAN security best practices leave their networks prone to the consequences of unauthorized access and vulnerable to network attacks.



Cisco SMB Class Mobility Solutions, in combination with Intel Centrino mobile technology-based notebooks, offer strong, built-in security with best practice guidelines. Together, they form an end-to-end solution that

includes support for the Cisco Wireless Security Suite, WPA, and WPA2.

WPA and WPA2 are Wi-Fi Alliance certifications that address known vulnerabilities in WEP to help ensure WLAN data integrity and provide protection from network

Recommendation #2: *If you're using older WLAN technologies that are limited to WEP support, consider upgrading to hardware with enhanced security that supports WPA or WPA2. At a minimum, today's business WLANs should support the WPA certification.*

attacks. Both WPA and WPA2 provide per-user, per session 802.1X/EAP mutual authentication using Extensible Authentication Types (EAP) like Cisco LEAP, EAP-FAST, PEAP or EAP-TLS for a high level of assurance that only authorized users can access the network. Data encryption, for data privacy, is provided for WPA via Temporal Key Integrity Protocol (TKIP) and for WPA2 via Advanced Encryption Standard (AES). WPA2 supports IEEE 802.11i.

Strong data encryption enhances security so that data remains protected and secure during the sending and receiving process. Both WPA and WPA2 are secure solutions. Companies can select the solution that works best for their deployment – WPA or WPA2.

Intel Centrino mobile technology and Cisco SMB Class Mobility Solutions support WPA and WPA2.

The Business Case for Intel and Cisco Technology-Based WLANs

When you choose notebooks based on Intel Centrino mobile technology and you deploy them in a Cisco SMB Class WLAN environment, you gain the confidence that comes with an interoperable solution.⁵ What's more, you obtain technologies that support IEEE standards and the Wi-Fi Alliance WPA and WPA2 certifications. You also gain flexibility plus greater investment protection by adopting solutions that provide a clear migration path to new WLAN standards as they are released.

Recommendation #3: *Choose a secure, enterprise-class, end-to-end WLAN solution that is Cisco Compatible Extensions certified and is verified by Intel Centrino mobile technology.*

Intel Centrino mobile technology was designed specifically for mobility and enables what mobile users want out of their notebook PCs – breakthrough

mobile performance, great battery life, integrated WLAN capability, and thinner, lighter designs.[†] There are three main components in Intel Centrino mobile technology:

- ▶ **Intel® Pentium® M processor:** Intel's first mobile processor built using Intel's most advanced manufacturing process (the 90nm process), the Intel Pentium M processor features a 2 MB power-optimized Layer 2 cache, clock speeds up to 2 GHz or greater, a 533 MHz power-optimized system bus, and other architectural enhancements such as Micro-Ops Fusion and a dedicated stack manager for faster execution of instructions at lower power.[†]
- ▶ **Mobile Intel® 915 Express chipset family:** A family of chipsets that delivers breakthrough performance at lower power levels, offered as a discrete memory controller hub (Intel 915PM chipset) or an integrated graphics memory controller hub (Intel 915GM chipset) that supports high-speed 333 MHz DDR memory technology and 400/533 MHz DDR2 memory technology.

▶ Find a wireless hotspot near you: intel.jwire.com

- ▶ **Intel® PRO/Wireless Network Connection:** Integrated wireless networking capabilities in dual mode (Intel PRO/Wireless 2200BG Network Connection supporting 802.11b/g) or tri mode dual band (Intel PRO/Wireless 2915ABG Network Connection supporting 802.11a/b/g) configurations.*

Cisco SMB Class Mobility Solutions lead the industry in addressing customers' business challenges of creating a more protected and responsive workforce. With Cisco SMB Class Mobility Solutions, which include Cisco Series access points and the Cisco Wireless Security Suite — a standards-based, WLAN security solution — SMBs can obtain the products they need to establish secure, manageable, and scalable WLANs. Cisco features integrated, consistent services across its product portfolio, enabling the intelligence that maximizes performance, the modularity and flexibility to meet your budget or capacity requirements, and investment protection you can count on.

Cisco SMB Class Mobility Solutions can help you increase productivity and improve efficiency by securely extending network connections to employees who use unwired links or who work in remote locations. Integrated security management simplifies the setup and operation of firewalls, WPA, WPA2 and other security measures such as Virtual Private Networks (VPNs) that can be used for remote or teleworking employees.

Together, Intel Centrino mobile technology and Cisco SMB Class Mobility Solutions offer the following security features and support for industry-standard and industry-leading security solutions:

- ▶ **Wi-Fi-CERTIFIED* for WPA and WPA2[®]:** Certifications[^] help to ensure interoperability with other Wi-Fi Alliance WPA or WPA2-certified products.¹ WLAN access control is supported via per-user, per-session mutual authentication and data privacy is provided via strong dynamic encryption.
- ▶ **Cisco Compatible support:** Tested compatibility and interoperability with licensed Cisco infrastructure innovations that go beyond the current IEEE standards and Wi-Fi Alliance certifications.

SMB WLAN Security: What to Look for

- ▶ **Standards support:** *Complies with the most current IEEE 802.11 protocols.*
- ▶ **Cisco Compatible Extensions support:** *Indicates compatibility and interoperability with licensed Cisco infrastructure innovations like QoS, radio management, WiFi Multimedia, etc.*
- ▶ **End-to-end data protection:** *Keeps intruders at bay by protecting traffic across the network.*
- ▶ **Extended perimeter security:** *Permits or denies access to the network or applications.*
- ▶ **Intrusion protection:** *Monitors and blocks attacks at the network element and network host levels.*
- ▶ **Security management and policy:** *Manages, monitors, and analyzes traffic and devices for adherence to established security policies.*
- ▶ **Identity services:** *Provides authentication, authorization, and accounting (AAA) of users, using 802.1X-based per-user, mutual authentication.*
- ▶ **VPN capabilities:** *Remote access for teleworking or traveling employees. VPN runs a tunnel through a wireless connection, creating an authenticated, encrypted connection between remote clients and company servers.*
- ▶ **Security above and beyond default settings:** *Cisco and Intel offer support for advanced security features like WPA and WPA2. This offers customers flexibility in designing a secure WLAN solution that meets their individual needs.*

Together, Cisco SMB Class Mobility Solutions and Intel Centrino mobile technology-based notebooks and tablets offer enhanced wireless security solutions for your business — end-to-end solutions that can be deployed easily and can help safeguard your SMB environment for years to come.

- ▶ *For more information, visit the Cisco and Intel Alliance Web site at www.cisointelalliance.com*
- ▶ *For additional information on Cisco, visit www.cisco.com/go/smbclass*
- ▶ *For additional information on Intel, visit www.intel.com/smallbusiness*

Glossary

AES: Advanced Encryption Standard. A strong, symmetric 128-bit block data encryption technique used in highly secure environments. Part of the IEEE 802.11i security standard for WLANs. AES has already been adopted as an official government standard by the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST). AES is included in the WPA2 certification.

EAP: Extensible Authentication Protocol. A flexible, point-to-point protocol that supports multiple authentication methods. Support for EAP types depends on the operating system, database and supplicants supported.

IEEE 802.11: The IEEE family of standards for WLANs that was first introduced in 1997. Products based upon these standards are tested and branded as Wi-Fi* by the Wi-Fi Alliance. Wireless networks based on the 802.11b standard are the most common. There are also 802.11a and 802.11g WLAN networks that provide greater throughput up to 54 Mbps.

IEEE 802.1X: A port-based network access control method for wired and wireless networks. It was adopted as a standard by the IEEE in August 2001. It is included in WPA and WPA2 certifications.

LEAP: Cisco Extensible Authentication Protocol. An 802.1X EAP authentication type developed by Cisco to provide dynamic per-user, per-session mutual authentication.

MIC: Message Integrity Check. The MIC function provides effective frame authenticity to mitigate man-in-the-middle vulnerabilities. MIC prevents an attacker from capturing, altering, and resending data packets. A component of TKIP.

PEAP: Protected Extensible Authentication Protocol. An 802.1X EAP authentication type that takes advantage of server-side EAP-TLS and supports several authentication methods, including logon passwords and one-time passwords (OTPs). PEAP provides a secure channel established without requiring a client-side certificate.

TKIP: Temporal Key Integrity Protocol. Part of the IEEE 802.11i encryption standard for WLANs. TKIP provides per-packet keying, message integrity check (MIC), and a rekeying mechanism, fixing the flaws of WEP. Designed to be deployed with existing Wi-Fi CERTIFIED devices, TKIP is also included in the WPA certification. TKIP replaces WEP's single static key with a dynamically generated per-packet key.

VPN: Virtual Private Network. "Tunneling" mechanism that creates an authenticated, encrypted connection between remote clients and company servers; generally supported by wired or wireless networks for remote or traveling users.

WEP: Wired Equivalent Privacy. The original IEEE 802.11 security encryption. It had modest security goals, including native authentication — where users are required to prove they are authorized for access — and encryption to provide data protection. The protocols in WEP are now easily defeated and WPA or WPA2 are now recommended for WLAN deployments.

Wi-Fi: Short for wireless fidelity, the most common wireless networks in use today.

WPA: Wi-Fi Protected Access certification. Developed to replace WEP, it is a subset of the ratified 802.11i standard. WPA can secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, both multiband and multimode. WPA uses TKIP for encryption and 802.1X/EAP or pre-shared key (PSK) for authentication.

WPA2: Wi-Fi Protected Access 2 certification based on the ratified 802.11i standard. WPA2 strengthens WPA security with AES encryption, and 802.1X/EAP or pre-shared key (PSK) for authentication. WPA2 may require a hardware or firmware upgrade for some products.



Wireless connectivity and some features may require you to purchase additional software, services or external hardware. Availability of public wireless LAN access points is limited, wireless functionality may vary by country and some hotspots may not support Linux-based Intel® Centrino™ mobile technology systems. System performance measured by MobileMark® 2002. System performance, battery life, wireless performance and functionality will vary depending on your specific operating system, hardware and software configurations. See http://www.intel.com/products/centrino/more_info for more information.

*Some security solutions may not be supported by your PC's operating system and may require additional software and/or certain hardware as well as wireless LAN infrastructure support. Check with your PC manufacturer for details. Other names and brands may be claimed as the property of their respective owners.

*Wireless functionality may vary by country and Wi-Fi certification is not supported on Linux-based Intel Centrino mobile technology notebooks. Check with your PC manufacturer for details.

*Dual-band 802.11a/b WLAN supports low-band capabilities (5.15 to 5.35 GHz). Low-band capabilities are not supported in all countries, contact your PC manufacturer for more details. New platforms designed with the Intel® PRO/Wireless 2100A (802.11a/b) solution may not be eligible for Wi-Fi certification after January 1, 2004.

*NOP World Technology: "2003 Wireless LAN Benefits Study"

Information in this document is provided in connection with Intel® products no license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document except as provided in Intel's terms and conditions of sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or limited warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.

*Other names and brands may be claimed as the property of others.

Copyright © 2005 Intel Corporation. All rights reserved.

Intel, the Intel logo, Intel Centrino, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Cisco, Cisco Systems, the Cisco Systems logo, and Aironet are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Printed in USA

0305/EW/OCC/XX/PDF

Please Recycle

302740-003US