

HP Mobility and
Wireless Solutions

psg ww marcom

June 2003



white paper

benefits of Cisco compatibility for HP business notebooks

contents

introduction	3
authentication	3
data encryption.....	4
Cisco LEAP	4
Cisco Compatible	
Extensions program	4
how does the	
program work?	5
customer benefits	6
frequently asked	
questions.....	6
innovative features	7
third-party testing	8
Cisco Compatible	
Extensions logo	8

abstract: As businesses discover the productivity gains inherent in mobile computing, the number of Wireless LAN (WLAN) deployments is increasing. WLAN growth, however, is dampened by concerns over security and manageability.

Industry standards such as IEEE 802.1x are addressing these security and manageability issues. Extensible Authentication Protocol (EAP)-Cisco® Wireless (LEAP), a feature of Cisco WLAN infrastructure products, has emerged as a leading 802.1x implementation.

The Cisco Compatible Extensions program helps provide assurance of compatibility between Cisco Aironet® WLAN infrastructure products and third-party wireless client devices, such as those from HP.

HP participation in the program brings broad support for Cisco wireless LAN products to HP business notebooks. Ultimately Cisco compatibility will address customer concerns about WLAN security and manageability and provide confidence of compatibility with Cisco Aironet WLAN products.

notice

©2003 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

June 2003
5981-7093EN

introduction

WLAN devices can improve the mobility and productivity of notebook users. However, to be truly productive, today's mobile worker requires network access for applications such as e-mail, Internet, or corporate databases. With a WLAN-enabled notebook, in-the-office productivity is available anywhere the worker is covered by a compatible WLAN access point – throughout a corporate building or campus, in airports, hotels, or other public wireless hotspots.

Businesses have recognized the benefits of wireless technology and are responding. Worldwide sales of WLAN technology are increasing from \$0.6B in 2000 to an estimated \$4.9B in 2006¹.

Other benefits of WLAN solutions include:

- Reduced infrastructure — With no need to run cables for each client device, WLANs are feasible in areas where cabled access is either impractical or too expensive.
- Flexibility – A WLAN implementation facilitates temporary set-ups, relocation, and in general makes the workplace more adaptable to changing needs.
- Cost – In many cases, deploying access points and WLAN client devices may be less expensive than running LAN cables.
- Specialized applications – A WLAN allows applications to take advantage of workers' ability to roam (as in retail stores, schools, or warehouses, for example).

However, WLAN deployments also have weaknesses, primarily in the area of security – in both authentication and data encryption.

authentication

Many early WLAN deployments were subject to security vulnerabilities that continue to be addressed by emerging industry standards. Issues that have plagued WLANs in the past include:

- Lack of security – Users may not be authenticated prior to gaining access to the network.
- One-way authentication – In some deployments, authentication is not mutual; the authenticating service – a Remote Authentication Dial-In User Service (RADIUS) server, for example – authenticates the client but the client does not authenticate the server, making the client vulnerable to “rogue” or hostile access points.
- Inconsistency – The authentication process may not be centralized. Each access point may independently authenticate clients associating with it; some access points may authenticate using MAC addresses while others use shared encryption keys.

¹ Source: Synergy, February, 2002

data encryption

The security standard for data encryption in a WLAN is Wired Equivalent Privacy (WEP), which uses a symmetrical 40-bit key to encrypt text messages. WEP was designed to provide the same level of security as in wired LANs; however, certain limitations still exist:

- Key distribution – When the WEP standard was first introduced, all users on a WLAN shared the same key, making it difficult to control key distribution and ensure only authorized users received the key. Changing keys frequently to address this risk presented key management and rotation issues.
- Cryptography – The cryptographic methods used by WEP are weak and can be broken by analyzing a sufficient amount of network traffic. Rotational-based keying can mitigate this risk; further security enhancements may be delivered by a Virtual Private Network (VPN) deployment or by taking advantage of emerging standards such as Wi-Fi² Protected Access (WPA) or Advanced Encryption Standard (AES).

Cisco LEAP

802.1x was introduced to address network security vulnerabilities related to client authentication – vulnerabilities that are particularly problematic in a WLAN environment. 802.1x uses a flexible authentication scheme based on the Extensible Authentication Protocol (EAP), which offers the customer a selection of authentication types such as MD5, TLS, TTLS, PEAP, and LEAP. Each of these EAP types has merits; however, the most widely deployed authentication type in today's WLAN environments is LEAP, a feature of Cisco WLAN infrastructure products.

The benefits of LEAP include:

- A two-way challenge-based password for mutual authentication
- The generation of per-session WEP keys to improve data encryption
- A solution for key distribution and management issues
- Relative ease of deployment (in that the credential used for authentication is password-related rather than a digital certificate, which can be more complex to implement).

Cisco Compatible Extensions program

Innovations such as LEAP have helped position Cisco as a leader in the WLAN infrastructure market. The popular Cisco Aironet Series of WLAN infrastructure products delivers mobility and flexibility with enhanced throughput and security for an enterprise environment. Combining WLAN standards compliance and Wi-Fi certification with innovative features such as the 802.1x-based Cisco Wireless Security Suite, the Aironet Series offers a complete line of access points, bridges, antennas and accessories.

² Wireless Fidelity

The Cisco Compatible Extensions program announced in February 2003 helps ensure interoperability³ between participating WLAN clients and Cisco Aironet WLAN products. This interoperability helps deliver the confidence IT managers need to deploy WLAN technology in their networks today.

HP and other WLAN client suppliers participating in the Cisco Compatible Extensions program license Cisco technology innovations, design their products to meet Cisco specifications, and allow the products to undergo extensive third-party testing. By participating in the program, these suppliers help ensure their products interoperate with standards-based Cisco Aironet products. The result is an easy-to-implement, end-to-end WLAN security and manageability solution.

Initially, Cisco compatible notebooks will feature the Cisco Wireless Security Suite, which includes the LEAP 802.1x authentication type. Other Cisco innovations will be added to the program in the future.

how does the program work?

HP works with leading WLAN chipset partners to deliver high-performance wireless clients with industry-standard security support and the additional security and manageability features offered by innovative Cisco technologies. A third-party test house validates the interoperability of HP clients with Cisco WLAN infrastructure.

Figure 1 shows the flow of technology through the Cisco Compatible Extensions program.

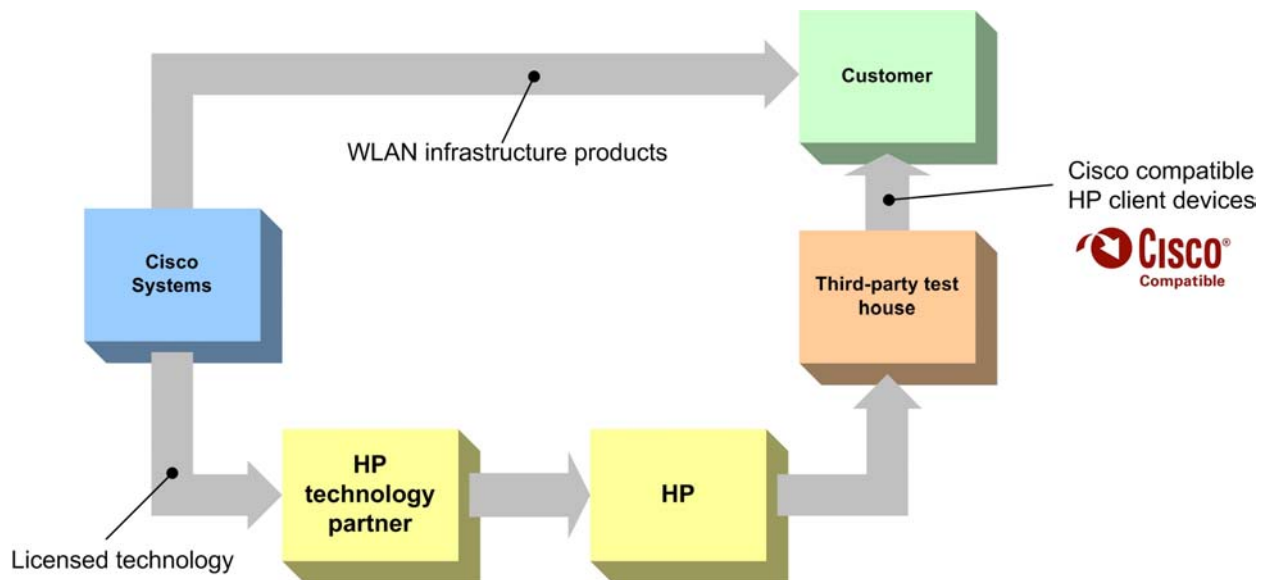


Figure 1: Technology flow in the Cisco Compatible Extensions program

³ Cisco uses "compatibility" in the same sense as "interoperability."

customer benefits

Since HP and Cisco are both leaders in IT technology and, in many cases, share the same customers, HP support of the Cisco Compatible Extensions program is a natural outgrowth. This partnership between HP and Cisco better serves common customers, addressing their need for end-to-end WLAN security and manageability solutions embedded into business notebooks from HP.

Customers can deploy HP Cisco-compatible notebooks in a Cisco WLAN infrastructure with confidence of interoperability and Cisco feature support—even in mixed client environments. Interoperability is validated through extensive testing at a third-party test house, taking the guesswork out of selecting secure, manageable client devices.

The Cisco Compatible Extensions program offers HP customers the following key benefits:

- Delivers important, innovative security and manageability features
- Gives confidence of interoperability with industry-leading Cisco WLAN infrastructure
- Demonstrates compliance with industry standards
- Offers investment protection with a path to future enhancements

frequently asked questions

What does the Cisco Compatible Extensions program for wireless clients achieve?

The program helps provide assurance of compatibility between Cisco WLAN infrastructure products and HP wireless clients.

When will HP begin shipping Cisco compatible clients?

HP plans to begin shipping Cisco compatible business notebooks in mid-2003. HP expects to expand its portfolio of Cisco compatible clients in the future to include Tablet PCs and handhelds.

How can I identify a Cisco compatible client?

A list of Cisco compatible HP clients is available at www.hp.com/go/ciscocompatible. Each Cisco compatible HP client carries the Cisco Compatible logo; in addition, the documentation and specifications for each HP mobile product identify whether or not it is a Cisco compatible client.

Does the Cisco Compatible Extensions program compete with Wireless Fidelity (Wi-Fi)?

No. Wi-Fi compliance is at the core of the Cisco Compatible Extensions program.

Do Cisco compatible clients comply with industry standards that are important to HP business notebooks?

Yes, Cisco compatible clients comply with both 802.11b and Wi-Fi. In addition, Cisco compatible clients are qualified under the Microsoft® Windows® Hardware Quality Labs (WHQL) program, helping to ensure that users receive a high-quality computing experience with the Windows XP operating system.

Which operating systems are supported on Cisco compatible clients?

Currently, Cisco compatible clients from HP support Microsoft Windows XP or Windows 2000.

Where can I find more information on the Cisco compatible Extensions Program?

More information on the Cisco Compatible Extensions program is available at www.cisco.com/go/ciscocompatible/wireless.

innovative features

The Cisco Compatible Extensions program features Cisco technologies that deliver important security and manageability enhancements and more. Benefits include:

- **LEAP and Cisco Key Integrity Protocol (CKIP)**

LEAP and CKIP can boost security for demanding enterprise customers. LEAP provides robust user authentication with dynamic WEP; CKIP delivers a strong encryption system to help protect against professional hackers.

- **Proven compliance with WLAN standards, Wi-Fi and Microsoft WHQL**

To protect the customer's investment in existing WLAN infrastructure and wireless clients, Cisco compatible devices comply with important industry standards, such as 802.11b, Wi-Fi and the WHQL program.

- **Future WLAN support**

To help future-proof Cisco compatible devices, future releases will include Cisco enhancements and support for emerging industry standards such as WPA.

third-party testing

The [KeyLabs](#) Independent Testing Center has been designated as the only test house authorized to perform interoperability testing for Cisco compatible products. KeyLabs provides the testing and consulting services necessary to verify that wireless clients meet the criteria of the Cisco Compatible Extensions program.

With experienced engineers and leading-edge technology, KeyLabs can perform independent, confidential and secure testing services to help ensure that products can withstand the rigors of today's e-business environment.

KeyLabs is ideally qualified to help program participants through the testing process.

Cisco Compatible Extensions logo

The Cisco Compatible Extensions program ensures that a wide selection of interoperable wireless client devices is available from HP and other suppliers. All product offerings can take full advantage of the enhanced security and manageability offered by a Cisco WLAN infrastructure.

The customer can recognize Cisco Compatible devices through the Cisco Compatible logo (shown in Figure 2).



Figure 2: The Cisco Compatible logo, used to identify Cisco compatible product offerings