

# **Executive Briefing: Wireless Network Security**

**White Paper**

**[www.docs.hp.com](http://www.docs.hp.com)**



**Manufacturing Part Number : T1428-90017**

**September 2003**

U.S.A.

© Copyright 2001-2003 Hewlett-Packard Development Company, L.P.

---

## Legal Notices

The information in this document is subject to change without notice.

*Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.* Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

**Warranty.** A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

**Restricted Rights Legend.** Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY  
3000 Hanover Street  
Palo Alto, California 94304 U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only.

**Trademark Notices.** UNIX is a registered trademark of The Open Group.

**Copyright Notices.** ©Copyright 2001-2003 Hewlett-Packard Development Company, L.P., all rights reserved.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

This document originally authored by Mike Klein and published by Interlink Networks.

**2003 Interlink Networks, Inc. All Rights Reserved.** This document is copyrighted by Interlink Networks Incorporated (Interlink Networks). The information contained within this document is subject to change without notice. Interlink Networks does not guarantee the accuracy of the information.

Interlink Networks, Inc.  
775 Technology Drive, Suite 200  
Ann Arbor, MI 48108 USA

[www.interlinknetworks.com](http://www.interlinknetworks.com)

## **Wireless Network Security**

Introduction . . . . .	5
Security is the Main Concern . . . . .	6
Layered Wireless LAN Security . . . . .	7
Three Levels of Wireless Security . . . . .	8
1 — Physical Layer Encryption . . . . .	8
2 — 802.1X User Authentication . . . . .	9
3 — VPN Security . . . . .	10
Conclusion . . . . .	12
Five Rules for WLAN Security . . . . .	12



# Wireless Network Security

---

## Introduction

Wireless network (WLAN) technology is the fastest growing segment of the communications market. According to Gartner Research, worldwide shipments of WLAN units are forecasted to grow at an annual rate of 42% through 2007.

The major driver fueling this growth is the strong return on investment afforded by much lower installation costs, higher availability, and mobile data connectivity. Another significant advantage of WLAN technology is that there is no “killer app” required to deploy wireless networks. WLAN components plug into the existing infrastructure as simply as extending a phone line with a wireless phone.

Unlike traditional network technology adoption that starts with enterprises and moves to the SOHO and home markets as the technology matures, WLANs are being adopted in the opposite order. While many corporations and businesses are adopting wireless LANs, the SOHO and home users are adopting WLANs at a much faster pace.

By removing the need to wire a network in the home, the cost of adoption and benefit of mobility within the home and low cost of components make wireless networking a low-cost and efficient way to install a home network. This segment of the market is much less aware and concerned about the security implications associated with wireless networks.

At the same time, wireless adoption within the corporate and medium-sized businesses has been severely inhibited by security concerns associated with placing sensitive corporate data over the air. While home users are less aware and less concerned about the security implications associated with wireless networks, WLANs have struck a nerve with security conscious IT departments.

Until recently, there has been no straightforward, cost effective way to deploy wireless security. IT departments have been forced to either forbid the deployment of wireless networks, overlook the security concerns, or install costly VPN solutions to build protected data tunnels between each wireless user, and the core network.

This paper discusses the 3 layers of wireless security and the options available for securing the network:

- Physical layer encryption, including WEP which has proven ineffective against hackers and intentional intruders;
- 802.1X standards-based security which provides cost effective, easy to use network security; and
- VPN-based security for the most security conscious requirements.

## Security is the Main Concern

Wireless access points (APs) translate the hardwired electronic signals in the network to radio signals that are sent across the air. Plugging an access point into the existing network and a wireless interface card directly in the PC can extend networks quickly and easily. With very little configuration, one is able to set up a wireless network, and roam anywhere within a 300 foot region without the traditional network ethernet.

Unfortunately, this also makes the same network available to any other PC that is also equipped with a wireless network card. Without proper security precautions, intruders can freely access your network. While IT managers would never think of installing an Ethernet drop outside the front door of the building, unprotected wireless access is virtually the same approach, with two significant differences. With a small amplifier and antenna, a hacker can sit undetected in a more remote location than the front door of the building, and hackers are posting unsecured networks and their positions on the Internet for others to access.

Unprotected wireless networks essentially “open the front door” of your network to intruders that can access shared drives and data, sniff every packet on your network, read emails, access web sites, and capture data for further analysis, and take as long as they need to crack the rest of your system.

Three real-world experiences illustrate the reality of WLAN vulnerabilities:

- At a seminar on WLAN security, an instructor showed the entire class how to find the open wireless LAN access points with freeware available on the Web. Within 15 minutes, students were able to sniff and record all of the network traffic and monitor Web pages and email packets sent to the network.
- An IT consultant, scheduled to install new software on a customer's IT servers over the weekend, was able to begin the installation process and shut down the servers from the parking lot, while waiting for the customer to arrive, through the company's wireless network. While this was an authorized user, an unauthorized intruder could have done the same thing.
- The well publicized network intrusion at a major commercial retail center earlier this year where an intruder captured credit card numbers in the parking lot using tools available over the Internet.

Capturing unsecured data anywhere in the range of a wireless LAN is very easy. The issue of security isn't limited to the standard wireless range of 300 feet indoors and 1000 ft. outdoors. Wireless hackers with antennas and power amplifiers can access your network completely out of sight, and usually without your knowledge.

While the advantages of wireless are tremendous, the security issues are real. Without physical security that can be used to protect wired networks, wireless users need to protect their networks with other tools that can provide the same level of security as wired networks. These solutions can be layered to provide the level of security required for any user or organization.

## Layered Wireless LAN Security

Like all IT-based security, WLAN security should be handled in layers. This provides several advantages: stronger overall security, the ability to block access at multiple layers of the network, and flexibility in selecting the cost/benefit ratio of the desired solution.

By building security in layers, protection can be provided at each layer in the network model. Each layer provides inherent protection against specific attacks for higher layers of security, correlating to the layers of the ISO network model.

One of the benefits of 802.1X is the additional strength of layered security. If an intruder is able to break the security at one level, he is presented with an entire new level of security to break again. This allows significantly longer time to detect and foil the intruder.

The layered security approach also provides the benefit of selecting the desired level of security, compared against the costs of adding additional layers. Layer 1 - Physical layer security is built into wireless equipment, and is essentially free (except for the cost of configuring and maintaining encryption keys) and may be adequate for a home user who wants to keep out the casual intruder. 802.1X-based security provides strong corporate security at an incremental cost. 802.1X dramatically increases the security protection of the network and provides the level of protection needed by most business and corporate users. In specific vertical segments such as financial and government users where triple-DES encryption is required, VPNs over 802.1X provide the highest level of wireless security, albeit with a cost increase on the order of \$30 - \$100 per user.

Each layer adds additional protection on top of the layers below it. The first two layers (physical layer encryption and 802.1X user authentication) are generally recognized as the minimum requirements for strong wireless LAN security, now specified in the Wi-Fi Protected Access (WPA) standard. An additional third layer (VPN) can be added to increase the security levels, if the traffic is sent unencrypted over the Internet, or contains highly sensitive information.

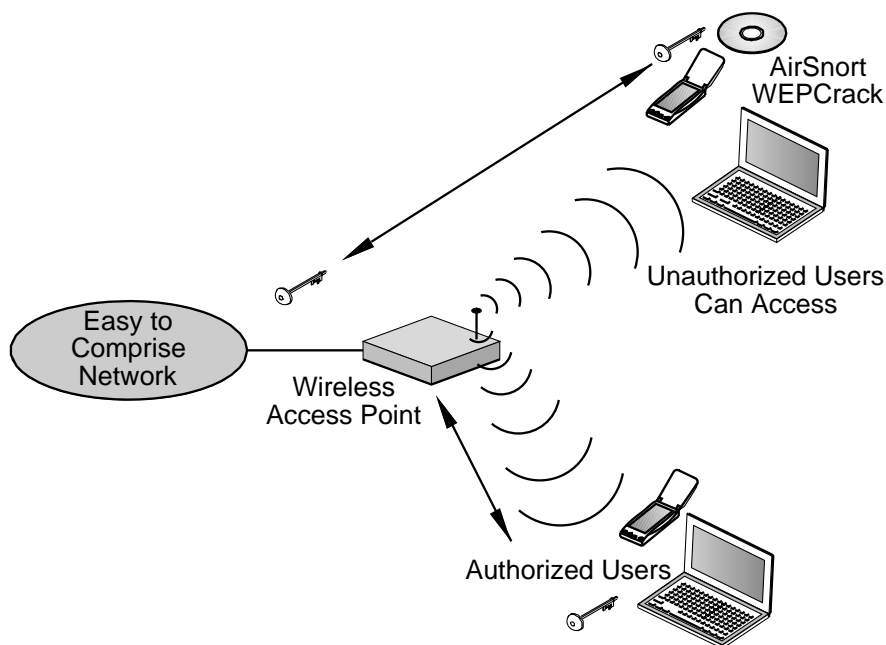
---

## Three Levels of Wireless Security

### 1 — Physical Layer Encryption

The lowest level of security that can be deployed in a wireless network is the Wired Equivalent Privacy standard (WEP). WEP allows for 40-bit or 128-bit keys to be entered in both the access point and the clients to encrypt the traffic between the PC and the access point.

**Figure 1** WEP Standard for Securing Wireless Networks



**Figure 1** depicts the WEP standard. Unauthorized users can gain access with easy-to-find software. Also, all authorized users must use the same encryption key.

The challenge however, is the inherent weakness of WEP security. With a little digging, unauthorized users can easily find software on the Internet that can be used to crack WEP encryption by capturing the network traffic over the air and deciphering the key (figure 1). Once the WEP key is deciphered, the traffic can be read in the clear, overcoming the encryption on the network traffic.

Another challenge of WEP-only encryption is the need to key each client device and each access point with the same encryption key (figure 1). In environments with more than ten users, the management of these keys, and manual re-keying whenever a user is removed from the network can be burdensome.

To address the inherent flaws of WEP, the Wi-Fi Alliance has created a new standard called Wi-Fi Protected Access (WPA). WPA combines two components to provide strong security for wireless networks. The first component is called Temporal Key Integrity Protocol (TKIP), which replaces WEP with a much stronger protocol. TKIP provides data encryption enhancements including a key mixing function, a message integrity check, and a re-keying mechanism that rotates through keys faster than any sniffer software can decode the

encryption keys. Through these enhancements, TKIP addresses all of WEP's known encryption vulnerabilities. TKIP software upgrades are expected to be available from wireless LAN component suppliers in 2003.

A more robust replacement for TKIP being debated in the IEEE standards committees is a new encryption standard called 802.11i. This standard will require new hardware components and is not expected to be implemented in production by WLAN equipment providers until the end of 2003.

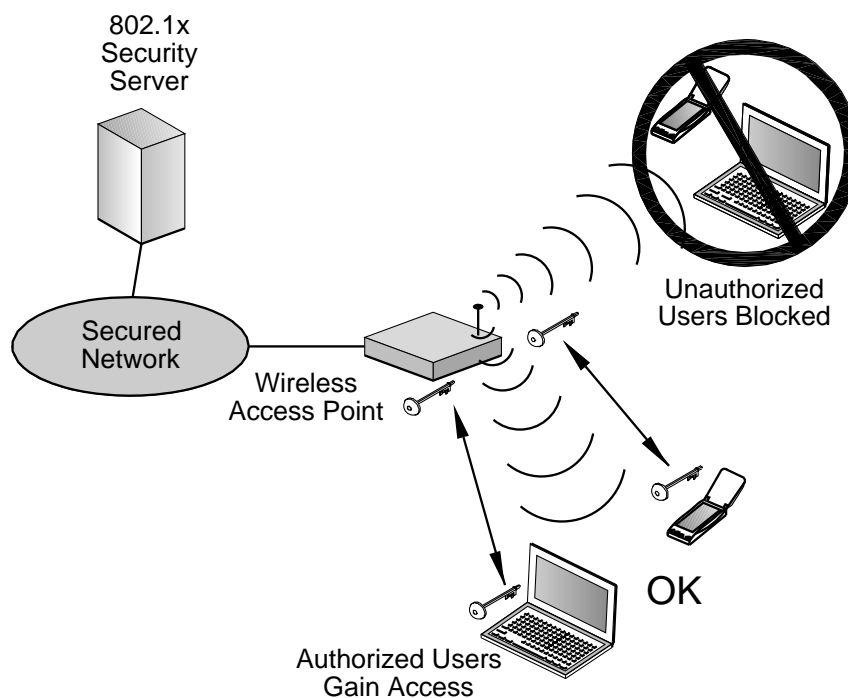
The second component of WPA is 802.1X security, which addresses the key management issue with user authentication. 802.1X is the second layer of security which, when combined with TKIP, provides a strong level of wireless security. 802.1X provides a security mechanism through which a user must be authenticated before he is allowed access to the network.

## 2 — 802.1X User Authentication

WEP and TKIP have no user authentication mechanism. Any user that has the encryption key (whether legitimately or illegally obtained) can get free access to the network and the traffic data. To overcome this weakness, 802.1X security is layered on top of the physical layer security.

The more recent physical layer security protocols, Wi-Fi Protected Access (WPA) and the emerging 802.11i standard, both specify 802.1x security as a framework for strong wireless security.

**Figure 2** 802.1x Authentication



**Figure 2** shows how a security server verifies that the access point is part of the network and requires users to provide unique credentials to verify their identity.

802.1X user authentication as shown in Figure 2, requires a user to provide credentials to the security server before getting access to the network. The credentials can be in the form of user name and password, certificate, token, or biometric. The security server authenticates the user's credentials to verify that the user is who he or she claims to be, and is authorized to access the network.

If the user is both authenticated and authorized to access the network, and the access point is verified as being part of the network, then the security server communicates directly with the access point to authorize the user's access to the network. The security server also creates a unique pair of encryption keys for this user session, which are sent to both the access point and the client to securely and uniquely encrypt the wireless communication between the two.

The security server also verifies that the access point is a valid part of the network. This is done to protect the user from connecting to an unauthorized access point that may have been set up to fraudulently capture network data.

802.1X security overcomes two significant limitations that physical layer security alone presents. It provides unique encryption keys for each user each time they sign onto the network, and eliminates the key management issues associated with maintaining common encryption keys across all access points and users.

The security server allows network access to be managed on a user basis. It can tie in to other corporate user databases or directories to authenticate the user against a common set of user credentials, eliminating the need for replicating and maintaining separate databases.

Combining 802.1X user authentication with physical layer security provides robust, strong security that cannot be broken with any known off-the-shelf software tools. It can provide wireless LAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network.

While no security mechanism can be considered "absolutely secure," the protection given by 802.1X security is strong enough to prevent most sophisticated attacks. As such, layer 2 security offers a pragmatic, economical security mechanism to meet the requirements of most corporate environments. Gartner Research believes this level of security will meet the needs of most businesses through 2005.

In some cases where higher levels of data security is required, VPNs can be layered on top of the security servers to provide an additional level of encryption of the IP data.

### **3 — VPN Security**

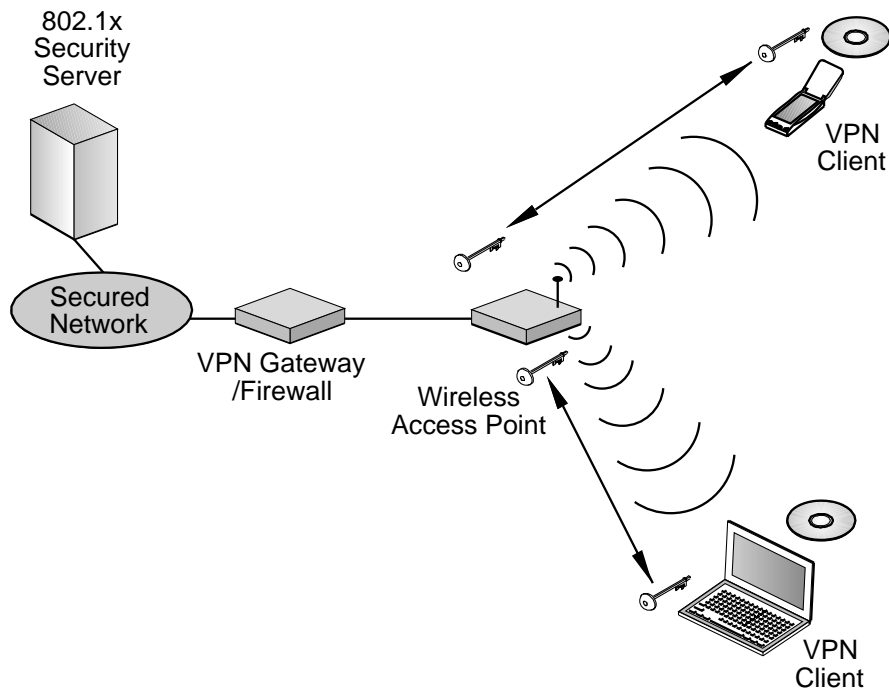
In environments where triple DES encryption is required, or the data on the wireless network may be passed through the Internet, VPNs may be used to provide another layer of security over 802.1X based solutions.

A word of caution on VPN implementations for wireless security: early wireless implementations used VPNs as the only security layer for wireless LANs. This practice leaves open security vulnerabilities. VPNs only encrypt data between the IP packets, leaving the wireless network vulnerable to a number of lower level attacks on the MAC and IP headers, such as wireless session hijacking and rogue AP, or man-in-the-middle attacks.

802.1X-based security should be used to prevent unauthorized access to the network, and to prevent the sniffing and stealing of IP and MAC addresses. It should also be used to prevent session hijacking and man-in-the-middle attacks through rogue access points. VPNs, while providing very strong IP data encryption, cannot prevent these types of lower level attacks.

If VPN security is required, a layered approach in conjunction with an 802.1X security server is the predominately recommended approach, as shown in Figure 3.

**Figure 3** VPN Security and 802.1x Authentication Used Together



**Figure 3.** VPN security used in conjunction with 802.1X authentication.

Another consideration that must be weighed is the additional costs and administration overhead associated with VPNs. Traditionally, VPNs have been used for remote access to corporate networks in a low throughput environment. With a wireless network, one should plan for much more traffic, as a result of a local presence, direct access, network environment. Consideration should also be given to the scalability costs and requirements as the wireless access, traffic, and number of users expand in future months.

## Conclusion

The benefit of wireless networks is driving the explosive growth of the WLAN market. Where security has been the single largest concern for wireless network deployment in the corporate setting, strong security solutions are available to make wireless networks as secure as wired networks.

Wi-Fi Protected Access (WPA) overcomes the inherent flaws of early wireless networks. WPA uses TKIP at the physical layer, and 802.1X security for user authentication create the basis for strong wireless network security. WPA is capable of preventing most sophisticated attacks on wireless networks, and there are no known tools available to crack this level of wireless security.

It's best to think about a layered approach for wireless security. WPA using a combination of physical layer security (TKIP) combined with 802.1X user authentication offers a pragmatic, economical security mechanism to meet the requirements of most corporate environments. For environments that require a more robust security, such as triple DES encryption, VPN tunnels can be layered on top of 802.1X security for a more comprehensive solution.

This approach offers a pragmatic solution to wireless security and can resolve the single largest barrier to WLAN deployment for IT managers. A cost-effective solution using 802.1X security can be deployed to deny access to any user without the proper credentials, and provide strong security for wireless networks.

## Five Rules for WLAN Security

1. **Activate Physical Layer Security.** While WEP has its weaknesses, TKIP, specified as part of WPA, provides a base level of security. When combined with 802.1X (see rule 3) it provides a very strong level of security.
2. **Don't Broadcast or Use Default SSIDs.** By changing the default SSID and configuring the access point not to broadcast the SSID, the most common sniffing tools can be rendered useless.
3. **Use 802.1X User Authentication.** When access points are configured to support 802.1X, users are not allowed on the network without proper credentials (user name/password or certificates). Once authenticated, the client and access point are provided with unique, random session keys to encrypt the data transfers.
4. **Implement Personal Firewalls.** Even if a hacker is able to associate with an access point, the personal firewall will prevent them from accessing files on a user device on the same WLAN.
5. **Use VPNs Where Triple DES Encryption is Required.** Specific environments like government and financial industries require 3DES security for all network transmissions. In these environments, VPNs should be used on top of 802.1X security.