

Technology White Paper

# IEEE 802.11 SECURITY CONSIDERATIONS

---

## A Primer on Enterprise WLAN Technologies

Jae Lee

Sr. Product Marketing Engineer



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
408 745 2000 or 888 JUNIPER  
[www.juniper.net](http://www.juniper.net)

**Date: 3-24-2005**

---

---

## Contents

Introduction .....	3
Data Transport Protection .....	3
Data Frame Privacy .....	5
Device Validity .....	9
User Identification .....	10
Summary .....	13

## Introduction

Wireless LAN security has evolved considerably since 2002, when 802.11b products started shipping. Unlike then, encryption and authentication mechanisms now ensure adequate enterprise-grade security when properly implemented. One unfortunate side effect accompanying the relative success of billions of venture capital dollars invested in 802.11 developments has been slow convergence of streamlined standards, and a glut of acronyms and techniques to control data protection, frame encryption, user authentication, and even transport.

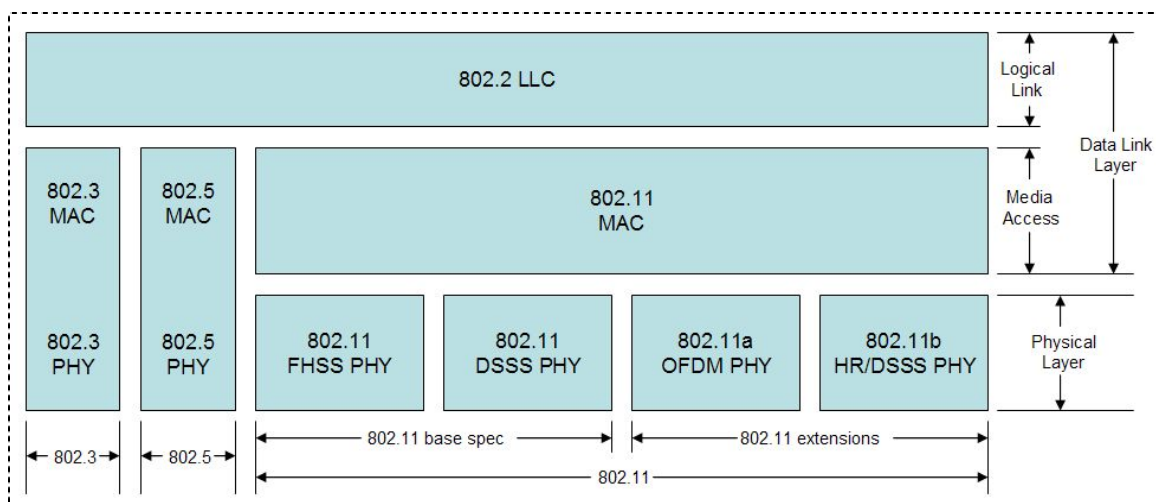
This paper is intended to provide a technical overview of IEEE 802.11 technology security issues, and to establish the importance of understanding these issues. Vendors must be cognizant of how to mitigate tradeoff risks involving ease-of-deployment, performance, interoperability, and other factors. Users must be knowledgeable to ensure adequate asset protection today while provisioning for emerging standards. Most importantly, all parties must be knowledgeable about 802.11 security issues during initial implementation and while scaling existing deployments.

It is assumed that the reader has a basic knowledge of both 802.11 and Ethernet concepts and nomenclature.

## Data Transport Protection

### PHY & MAC IN OSI

802.11 is a link layer protocol that can use 802.2/LLC encapsulation (**Figure 1**).



**Figure 1:** 802.11 in relation to the lower layers of the OSI model.

There are only two physical layers in the base 802.11 specification, FHSS (frequency-hopping spread-spectrum) and DSSS (direct-sequence spread-spectrum). Other layers were added in subsequent phases of evolution from the base specification. Note that these physical layers (which make up the bulk of difference from link layers 802.3 and 802.5) result from the necessity to use radio waves as a transmission medium. These layers deem physical security for 802.11 (often viewed as “virtual Ethernet”) a complex notion.

The following extensions are 802.11 transport protocols used in the bulk of shipping WLAN products:

802.11b – signal transmission occurs within the 2.4GHz ISM RF band and specifies a high-rate direct-sequence physical layer (HR/DSSS), and uses complementary code keying (CCK). 802.11b products started shipping in 1999.

802.11a – operates in the 5GHz unlicensed band, and specifies a 52-subcarrier orthogonal frequency division multiplexing (OFDM) physical layer. 802.11a products started shipping in 2002.

802.11g – like 802.11b, signal transmission occurs within the 2.4GHz ISM RF band. 802.11g also specifies OFDM. 802.11g products started shipping in 2003.

From a security perspective, it's misleading to assert 802.11 as being "just another layer for 802.2, like Ethernet". 802.11 requires capabilities at the MAC layer to accomplish mobile access, including mechanisms to maintain reliable signal strength despite physical environmental challenges associated with communicating via radio waves in open air, such as congestion and interference (which are more straightforward to manage within modern conductive copper or optical waveguide networks). The resulting operational challenges and low-level protocol vulnerabilities stemming from PHY- and MAC-level complexity represent technical security challenges that are non-existent or negligible in the wired domain.

## **MEDIUM AVAILABILITY & ACCESS**

### **RF Jamming**

RF domains exist within an open shared medium, allowing for DoS-type RF jamming. Broadcasting high-power electromagnetic-spectrum radiation across 802.11 frequency ranges would saturate those bands, rendering useless nearby 802.11 devices. An RF jamming attack typically requires costly radio jamming equipment, such as mil-spec tactical electronic countermeasure wide-band spectrum transmitters designed to defeat frequency hopping and spread spectrum (mechanisms to deter eavesdropping and reduce DoS risk). Additionally, sophisticated and targeted RF jamming requires training for effective operation and precision. For example, single-frequency omni-directional spot jamming is less intricate than directional barrage-style blocking of multiple frequency band ranges. Yet these types of attacks occasionally occur. In contrast, targeted electromagnetic energy bursts rendering countless Ethernet segments ineffective never happen, except in rare cases of power grid surge.

### **Collision Avoidance vs. Collision Detection**

Similar to the medium, 802.11-based network devices, which use CSMA / CA (carrier-sense multiple access with collision avoidance), are more susceptible to denial of service conditions than devices on Ethernet networks, which use CSMA / CD (collision detection).

CSMA / CD – a station stops transmission and broadcasts a jam signal upon collision detection resulting from a simultaneous transmit attempt by another station. In the case of CSMA / CD, the jam signal indicates collision has occurred and resulting station behavior is to wait before transmitting, for a random delay calculated by a binary exponential algorithm (Ethernet backoff).

CSMA / CA – a station broadcasts a jam signal to indicate that the station intends to transmit data – when other stations receive the jam signal, they will stop any current transmission and delay for a period (determined by a distributed control function or DCF), which applies inter-frame spacing intervals to all transmissions by any station) before again attempting to transmit.

The above comparison describes how Ethernet-connected devices interpret jam signals differently – while the resulting behavior is identical (hosts delay transmission for a period of time), the significance of the mechanism is not similar at all – in the CSMA / CD case, the jam signal is reactionary to an event happening within the medium, while in the CSMA / CA case, the jam signal is transmitted to communicate host-initiated intent.

### **DSSS / CCA DoS Vulnerability**

Practical exploitation of the collision avoidance principle has been demonstrated in certain 802.11 devices that use DSSS PHY. These devices rely on the Clear Channel Assessment (CCA) procedure to identify open channel

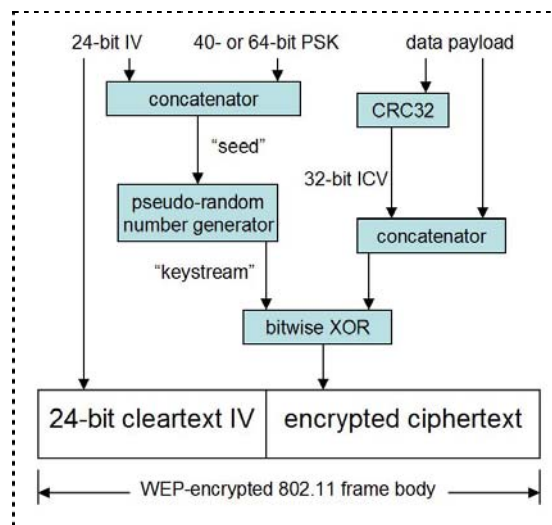
states that indicate the medium is clear for transmission. The discovery of the CCA vulnerability in 5/04 was significant in that it highlighted an “indefensible” DoS-type attack that requires a fraction of the capital expenditure for gear and training required in RF jamming. An attacker only needs a commercially available 802.11 adapter, the appropriately crafted hardware driver, and knowledge of how to configure a specific test mode of DSSS operation (PLME\_DSSSTESTMODE) on the adapter to introduce a steady stream of “jabber” signal into a target channel, deeming it constantly busy and therefore unavailable to all proximate devices for the duration of attack. Unfortunately, the new 802.11i standard (see below section **NEXT-GENERATION 802.11 SECURITY**) does not mitigate this vulnerability, as the attack happens at the Packet Layer Convergence Procedure (PLCP) layer – below the MAC Packet Description Unit (PDU) layer, where the bulk of 802.11i protective mechanisms are specified. Fortunately, 802.11 devices that use FHSS or OFDM are not affected by the DSSS vulnerability. Higher-rate 802.11g is not vulnerable either, as it uses OFDM at throughput rates above 20Mbps and FHSS for rates below 20Mbps. 802.11 devices operating in b/g mixed-modes are vulnerable.

## Data Frame Privacy

Because the wireless medium lacks an equivalent privacy level inherent to wired medium, cryptographic techniques are used to secure data transmission. These techniques are designed to mitigate unauthorized snooping during traversal through the wireless medium only, and are not applied within the wired portion of the network.

### WIRED EQUIVALENT PRIVACY (WEP)

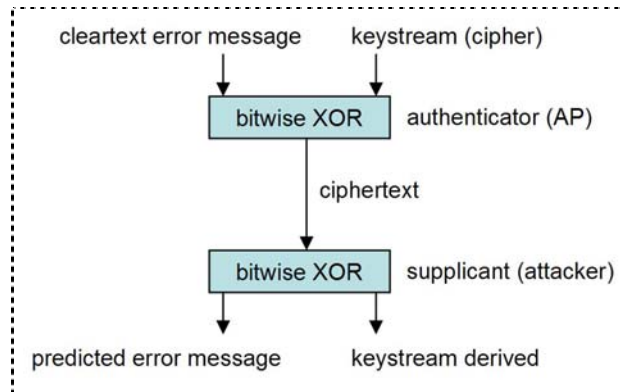
WEP, originally marketed as the security for wireless LANs, is considered flawed – the WiFi Alliance and most vendors do not recommend WEP for enterprise use. WEP is based on the RC4 symmetric stream (secret-key) cipher. WEP uses RC4 with 40-bit or 104-bit keys, 24-bit initialization vector (IV), and string CRC32 polynomial calculation for packet integrity check (some 802.11 clients specify WEP as 64-bit or 128-bit, denoting key length + IV length). WEP is known for its insufficient IV length and key space as well as its static key characteristic, resulting in likely frame IV recurrence inside relatively short durations. Collection of enough frames with the same IV followed by analysis of the frames with similar keystreams yields the shared values among these frames – the keystream or PSK (see **Figure 2**). The Prabhu Goel Research Centre for Computer and Internet Security has developed a tool (PickPacket) that cracks a 64-bit WEP key using this method. A 64-bit WEP key cracks in a few seconds after 4 hours of sniffing traffic. Cracking a 128-bit WEP key requires approximately 50 hours and about 15 hours of sniffed traffic.



**Figure 2:** WEP frame assembly and key scheduling.

### Bit-Flipping and Replay Attack

In the bit-flipping and replay attack (see **Figure 3**), a single encrypted WEP frame is sniffed from which its plaintext IV is determined. Then a bit within the WEP frame is flipped, and from this bit-flipped frame CRC32 integrity check value (ICV) is recalculated (WEP lacks keyed data authentication). The bit-flipped frame is then transmitted along with the known IV and proper ICV to the target AP, which forwards the frame into the Layer 3 switching infrastructure. A Layer 3 device will send a predictable response indicating rejection of the frame based on invalid source IP, which the AP will encrypt and forward to the attacker, who can now guess from a number of known Layer 3 switch error messages to derive the stream cipher. Unfortunately WEP has no protective mechanism to prevent this attack.



**Figure 3:** WEP bit-flipping and replay attack. Target AP forwards encrypted frame since ICV checksum is intact.

### WEP Key Scheduling

The selection process for the WEP ciphering engine focused scrutiny on the RC4 protocol, which was then generally considered secure. It is now known that the RC4 key scheduling algorithm does not obfuscate or discard the initial portion of stream output from its pseudo-random number generator (the core of RC4), allowing for key predictability. Mitigation options include hashing, encrypting, or discarding the first 256 bytes of the pseudo-random output, but this introduces required proprietary elements and increases incompatibility risk. Hence, most products use standard WEP and are therefore vulnerable. This vulnerability fortunately does not apply to SSL-based RC4, as encryption keys used in SSL are generated via MD5 and SHA1 hashing, so different sessions will have unrelated keys. Additionally, SSL maintains RC4 state from the end of one encrypted packet to the start of the next, eliminating per-packet re-keying.

### Practical WEP

Although WEP was only recently officially upgraded, it is seldom deployed in enterprise environments for data privacy. The primary motivator for WEP enterprise support is backward compatibility. Some network devices have 802.11 clients with only WEP-level encryption, such as certain print server and Wi-Fi phone handset models. There also exist 152- and 256-bit proprietary WEP implementations that use longer key lengths to mitigate IV recurrence-based PSK derivation attempts, although these devices typically do not exhibit adequate interoperability characteristics.

### Dynamic WEP

Dynamic WEP is the practice of dynamically generating session-specific WEP keys, which mitigates impact from WEP key derivation techniques that exploit static PSK usage. Dynamic WEP key generation with EAP requires an EAP method (EAP-TLS, EAP-PEAP, or EAP-TTLS, see section **PORT-BASED ACCESS CONTROL AUTHENTICATION METHODS**) that is capable of generating master keys (PMKs).

### WI-FI PROTECTED ACCESS (WPA)

WPA, a subset of the 802.11i security specification, was developed by the Wi-Fi Alliance as an interim solution until 802.11i ratification. WPA is forward compatible with 802.11i and replaces WEP's RC4-based ciphering

engine with Temporal Key Integrity Protocol (TKIP), which alleviates the privacy issue found in WEP for pre-shared keys. Certain WPA implementations also support AES encryption. These implementations differ from WPA2 (see section **WPA2** below), which is also AES-based, in that WPA2 requires CCMP-enhanced AES encryption.

**Temporal Key Integrity Protocol (TKIP)**

TKIP, an enhancement to WEP, was the result of effort by the 802.11i Task Group (TGi) to provide stronger security on the then-installed base of 802.11 hardware. Like WEP, TKIP uses the RC4 stream cipher, but with 128-bit encryption keys and 64-bit authentication keys.

**Rekeying** – TKIP features a re-keying mechanism to generate new encryption and integrity keys per packet, mitigating the threat of IV recurrence-based PSK derivation attempts.

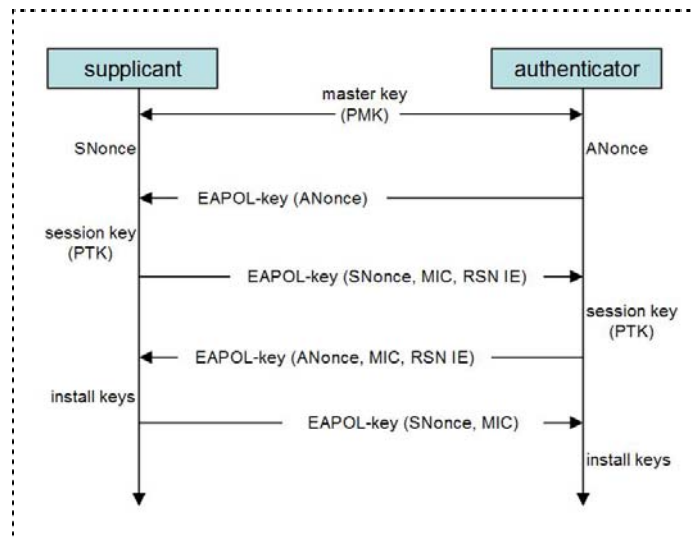
**Key Mixing** – TKIP also adds an IV sequence enforcement discipline that protects from replay attempts, as well as per-packet key mixing that prevents correlation of cleartext IVs with weaker keys.

**MIC** – TKIP uses a message integrity check (referred to as Michael) that performs a similar function to the block cipher-based CBC-MAC (CBC message authentication check) that is used in certain financial applications (see CCMP and WRAP below), or the HMAC mechanism used in conjunction with MD5 or SHA to provide keyed-hash message authentication codes or integrity check values within IPSec. Unfortunately, Michael MIC thwarts only most forgery attempts and has no countermeasure for packet replay forgery attempts ([http://www.nowires.org/Papers-PDF/WPA\\_attack.pdf](http://www.nowires.org/Papers-PDF/WPA_attack.pdf)).

TKIP started appearing in AP firmware upgrades near the end of 2002.

**4-Way Handshake and Group Key Handshake**

WPA implements a new key handshake (4-Way Handshake and Group Key Handshake) for generating and exchanging data encryption keys between Authenticator and Supplicant. These handshakes verify that both Authenticator and Supplicant have master session keys, and they are identical regardless of the selected key management mechanism (only the method for generating master session key changes, see **Figure 4**).

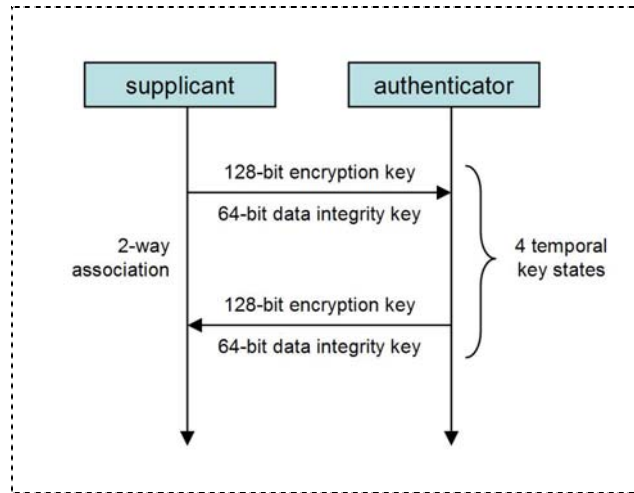


**Figure 4: WPA 4-Way Handshake**

**Key Management**

Keys can be managed using two different mechanisms. WPA can either use an external authentication server (e.g., RADIUS) and EAP (like IEEE 802.1X) or pre-shared keys (PSK), for deployments where separate

authentication servers are unavailable. Wi-Fi labels these "WPA-Enterprise" and "WPA-Personal", respectively. The *wep keyid*, a 2-bit state indicator, manages assignment of 4 temporal keys created per full-duplex association between supplicant and authenticator (see **Figure 5**).



**Figure 5:** Temporal keys per association.

**WPA-Personal Passive Dictionary Vulnerability**

WPA-Personal has been demonstrated to be vulnerable to a passive offline dictionary attack. In WPA, a master key (PMK) is derived via the pre-shared passphrase and SSID. The supplicant and authenticator then each create and install a session key (PTK) derived from the PMK, MAC addresses, and nonces. An attacker only need derive the PMK, which can be done easily via sniffing two EAPOL packets after deriving a PMK via passphrase guessing.

**WI-FI PROTECTED ACCESS 2 (WPA2)**

The Wi-Fi Alliance has adopted IEEE 802.11i as WiFi Protected Access 2 (WPA2), an upgrade to WPA. WPA2 fully supports IEEE 802.11i, of which AES-CCMP encryption complies with the FIPS 140-2 specification. Most of the installed base of 802.11 products will require hardware upgrades for AES-CCMP encryption/decryption. WPA2 is backwards-compatible with WPA. WPA2 will not support WEP or interoperate with WEP-enabled devices. WPA2-Personal (PSK) is designed so no additional authentication server is needed. The design of IEEE 802.11i mechanisms not included in WPA completed in 5/04 and ratified as an amendment to IEEE 802.11 a month later. WPA2 supports a more robust encryption algorithm to replace TKIP, and includes optimizations for handoff (reduced number of messages in initial key handshake, pre-authentication, and PMKSA caching) to improve roaming.

**CCMP and WRAP**

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is the preferred encryption protocol in the 802.11i standard. The RSN (Robust Secure Network, see Appendix G) component of the 802.11i standard recommends replacing TKIP with CCMP. 802.11i also allows TKIP for backwards compatibility (RC4 in TKIP will run on legacy 802.11 hardware), which is necessary as most legacy 802.11 hardware lacks CPU capacity to run the CCMP AES algorithm without unacceptable performance impact. CCMP is based upon the CCM mode of the AES encryption algorithm. The Counter Mode (CM) component of CCMP provides data privacy via 128-bit key, 48-bit IV lengths and Cipher Block Chaining Message Authentication Code (CBC-MAC) for packet integrity and authentication.

WRAP (Wireless Robust Authenticated Protocol) is based on the offset codebook (OCB) mode of AES. Intellectual property rights issues resulting from three separate patent-filing parties spurred the IEEE to bring CCMP into 802.11i. Unlike CCMP, WRAP is an optional component of RSN.

Some 802.11 vendors already provide support for CCMP in WPA products. No official interoperability certification yet exists for CCMP and/or mixed modes using both TKIP and CCMP for WPA, so interoperability issues can be expected even though vendor combinations may initially appear to exhibit basic compatibility. WFA interoperability testing for WPA2, including CCMP, started in September 2004.

### **802.11 Data Privacy vs. Ethernet**

It seems intuitive that ensuring privacy on an 802.11 network would be more difficult than on an Ethernet segment. 802.11 networks lack the protection provided by physical barriers such as walls or an isolated and unadvertised building or data center locale. Physical gates for access-level control to resources and data, human security guards, and locks or cardkey readers do not prevent unauthorized access or “exposure” to 802.11 networks. The greater risk of data privacy or confidentiality increases the likelihood of unauthorized data tampering. Hardware-level exposure presents new 802.11-specific risks such as malicious associations, forced supplicant disassociation, MAC forgeries, and other exploits.

In an ideal minimum-requirement design, data would actually be safer in 802.11 networks than Ethernet networks, because unlike in copper or fiber, real-world concerns with data privacy extend all the way into the wireless medium. These concerns have resulted in data protection all the way to the 802.11 frame level, such as frame body encryption (which even WEP contains), integrity check sequences for data validation, and stronger PSK-based station authentication. Unfortunately, the reality is that the protocol-level implementation is not sufficient. Following certain guidelines for compatibility, network design, and device configuration are required practice to secure the 802.11 transmission environment in as equivalent a manner as a wired Ethernet switch pad-locked in a wiring closet.

## **Device Validity**

The impact of masquerade-type attacks in 802.11 networks is potentially much greater than for traditional wired networks. For example, MAC address spoofing is based on changing client MAC to either hide presence on the target network, or to impersonate an authorized client on the target network. In contrast, IP spoofing typically does not even involve awareness by the target network of an existing (let alone attacking) source IP. Unlike IP spoofing, MAC address spoofing presumes some level of granted access privilege, and cannot be prevented. We explore other areas of 802.11 device-level security.

### **MAC ACCESS CONTROL LISTS**

Permissive-mode MAC ACLs are commonly implemented in wireless LANs to enforce hardware-level access policies – unfortunately, sole reliance on MAC addresses for device authentication (particularly for larger-scale deployments) is strongly not recommended, due to the relative ease for an unskilled attacker to impersonate an AP and hijack an authorized user identity. Mitigation options include monitoring for the presence of multiple instances of a unique MAC address, or verifying MAC-derived vendor ID (fingerprinting).

### **ARP CACHE POISONING**

ARP cache poisoning attacks, which happen at the MAC layer within switched or bridged networks, require that the attacker be on the same local segment as target devices. Many 802.11 APs act as transparent MAC-layer bridges, allowing ARP packet transmission between wired and wireless networks. Such APs are susceptible to enabling ARP cache poisoning attacks to reach wired hosts.

### **EAVESDROPPING**

802.11 data frames contain higher-layer protocols and data in the frame body, while management frames contain specific information used to establish link between supplicants (clients) and authenticators (APs), authenticate supplicants, maintain wireless association, and manage deassociation (termination). All 802.11 frames contain source/destination/AP MAC addresses, a frame sequence number, the frame body, and a frame check sequence for error detection. Unfortunately, the structure of 802.11 management frames makes successful eavesdropping on an open 802.11 network a trivial matter.

802.11 management frame types include:

- ◆ Beacon
- ◆ Disassociation
- ◆ Association request
- ◆ Association response
- ◆ Reassociation request
- ◆ Reassociation response
- ◆ Probe request
- ◆ Probe response
- ◆ Authentication
- ◆ Deauthentication

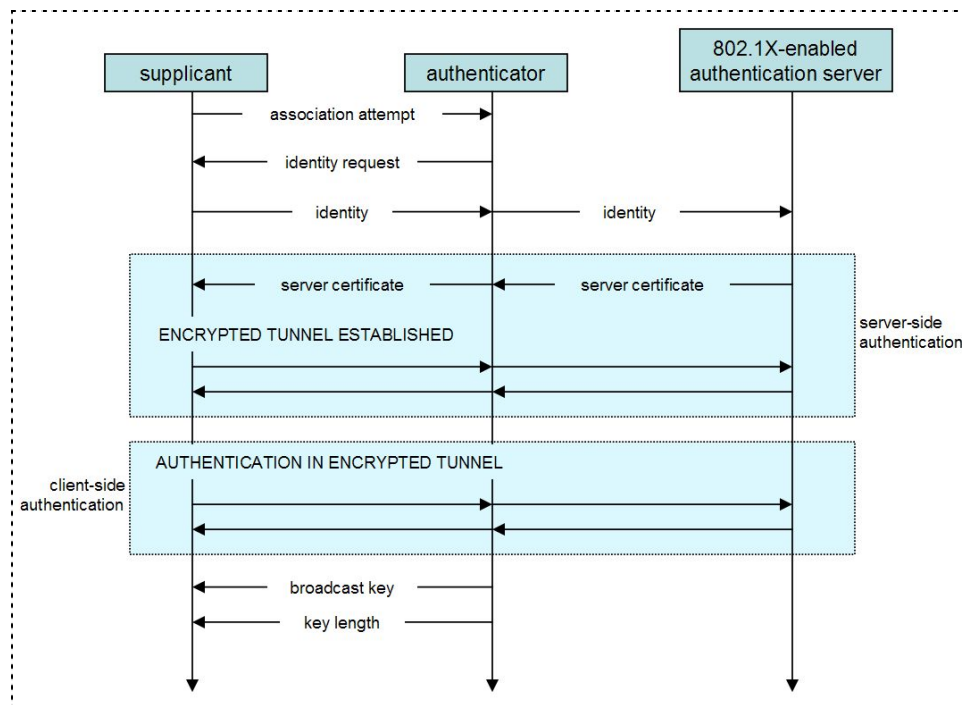
A common 802.11 vulnerability stems from false perception of elevated security from MAC ACL usage. Unless management frames are authenticated based on a more secure credential than MAC address, those frames can easily be monitored to aid unauthorized association. A beacon frame, for example, will yield beacon interval, timestamp, SSID, supported rates, parameter sets, capability information, and traffic indication map. For mitigation, IEEE 802.1X pre-authentication (see section below, **IEEE 802.1X AUTHENTICATION AND KEY MANAGEMENT**) reduces the risk of management frame spoofing by enabling authentication and key derivation prior to frame exchange.

### **MALICIOUS ASSOCIATION**

Unauthorized and undetected sniffing on the typical modern wired LAN requires physical access to a switch port or administrative privilege on a networking device, along with skill in applying IDS / IPS evasion or insertion techniques, such as IP header field / options manipulation, or TCP control block (TCB) forgery, and could require understanding of details such as the manner in which local IDS / IPS monitoring is tuned for TCB initiation (full 3-way handshake or allowed partial). Or if DNS cache poisoning were a selected alternative method, the attacker would need capabilities in DNS query / reply packet falsification, or be practiced in applied methods for exploiting inconsistencies in random TCP sequence number generation within BIND. Even the knowledge required to conduct a DNS Birthday attack is not trivial – in modern well-maintained DNS topologies, split-split configurations with recursive querying disallowed on external nameservers can thwart the majority of DNS spoofing attempts, except in poorly configured cases such as nameserver daemons bound to an unprotected interface. In contrast, redirecting traffic or intercepting data via malicious 802.11 association requires relatively much less technical skill. Using any 802.11 network adapter whose chipset features master mode (such as Intersil PrismII with HostAP or Atheros MadWiFi), an attacker can coax an 802.11 supplicant to deassociate from a legitimate AP and reassociate with a spoofed instance of the legitimate SSID from a masquerading AP. Subsequent full control of that client's traffic then requires minimal effort.

## **User Identification**

There are two primary issues with user-level authentication. One is the need for interoperability with an authentication server, and the other is secure transmission of the credentials to and from that server. **Figure 6** shows the anatomy of a generic secure 802.1X-based authentication.



**Figure 6:** Generic authentication mechanism for IEEE 802.1X-based protocols.

### IEEE 802.1X AUTHENTICATION AND KEY MANAGEMENT

IEEE 802.1X is an IEEE standard (ratified 6/01) that enables authentication and key management for IEEE 802 Local Area Networks including Ethernet, Token Ring, and FDDI. 802.1X does not describe mechanisms for 802.1X and 802.11 state machine coupling, due to timing considerations in the development of the framework. The definition of those mechanisms is the responsibility of the 802.11 Task Group.

802.1X is not a single authentication method, utilizing Extensible Authentication Protocol (EAP) as its authentication framework. Surprisingly, 802.1X does not mandate any specific methods of authentication. Thus, 802.1X-enabled switches and access points can support a wide variety of authentication methods (certificate-based authentication, two-factor smartcards or token cards, one-time passwords). The basic EAP pass-through used by 802.1X-enabled switches and APs allows for new authentication methods to be added without firmware upgrades.

Another benefit of 802.1X is that unlike encryption schemes like PPPoE or IPSec that require encapsulation, 802.1X adds no per-packet overhead. However, the majority of existing switches will require firmware upgrades for LAN-based support. On hosts, 802.1X can be implemented in the network adapter hardware driver, so OS compatibility is likely not an issue.

802.1X can be managed via RADIUS. Through RADIUS, 802.1X permits management of authorization on a per-user basis. Per-user services include Layer 2 and 3 filtering, various forms of tunneling, dynamic VLAN assignment, and rate limiting.

### PORT-BASED ACCESS CONTROL AUTHENTICATION METHODS

802.1X is a management protocol defining port-based access control for LANs, developed as a solution for dynamic networks where management of MAC ACLs could not meet scaling requirements. 802.1X is an extensible authentication framework for port-based access control. This framework can be used with a number of authentication methods, including:

EAP (Extensible Authentication Protocol), defined in RFC 2284 – PPP-based EAP is the original 802.11 standard for authentication. There are several authentication methods with varying authentication transport strategies associated with EAP.

EAP-TLS (Transport Layer Security) – RFC 2716: PPP EAP TLS Authentication Protocol, created by Microsoft (implemented in Windows XP), requires mutual certificate-based authentication (certificates on both client and server). EAP-TLS is the de facto standard for authentication in 802.11i WLAN topologies. EAP-TLS includes log-off and start commands, premature successful connection messages, failure messages, and other EAP modifications.

EAP-TTLS (Tunneled Transport Layer Security) – currently in Internet-Draft stage, extends TLS by requiring certificates on the server only, with only password-based client sub-authentication. Tunneled Transport Layer Security (EAP-TTLS) is a proprietary protocol which was developed by Funk Software and Certicom.

EAP-MSCHAPv2 – Microsoft EAP CHAP (challenge handshake authentication protocol, originally used over PPP connections) Extensions Version 2 (EAP MSCHAPv2) protocol allows mutual authentication between an authenticator and a peer seeking authentication. EAP-MSCHAPv2 extends the MSCHAPv2 protocol defined in RFC 2759, requiring only client authentication and no server authentication.

PEAP (Protected EAP Protocol) – also in Internet-Draft, PEAP is designed to overcome vulnerabilities in other EAP methods, providing secure mutual authentication and legacy sub-authentication. PEAP is a proprietary protocol developed by Microsoft, Cisco, and RSA Security.

LEAP (Lightweight EAP) – Cisco-proprietary EAP variation (AiroNet product line), provides mutual authentication based on password challenge-response. LEAP has yet to gain notable traction; therefore, Cisco is increasingly supporting PEAP efforts.

PEAP and EAP-TTLS make it possible to authenticate wireless LAN supplicants without requiring client certificates. PEAP and EAP-TTLS both utilize Transport Layer Security (TLS) to set up an end-to-end tunnel to transfer user credentials without the need for a client-side certificate. EAP-TTLS within 802.11 networks enables wireless LANs to communicate securely without need for client encryption certificates.

### **802.1X IN 802.11**

IEEE 802.1X plays a central role in IEEE 802.11i (see below section NEXT-GENERATION 802.11 SECURITY) for enhanced WLAN security, enabling authentication and key distribution. Mainstream interest in supporting 802.1X with PEAP in future 802.11 products is increasing. Widespread PEAP usage will likely eliminate any need for further LEAP development.

802.1X is not an alternative for WEP or WPA (or any encryption-based framework). 802.1X is only focused on authentication and key management. 802.1X doesn't specify details regarding service delivery using derived keys, although it can be used to derive authentication and encryption keys for use with any encryption cipher. 802.1X can also be used to periodically refresh keys and re-authenticate to deter key derivation attempts.

802.1X is interoperable with open standards for AAA (authentication, authorization and accounting) such as RADIUS and LDAP. 802.1X is non-disruptive to legacy infrastructure for managing dialup networks, VPN tunnels, and 802.11 station ports. RADIUS servers (including Windows 2000 IAS) that support EAP can be used to manage 802.1X network access.

### **RADIUS IN 802.11**

RADIUS is the most common authentication protocol used in 802.11 networks. The 802.11i security standard (see Next-Generation 802.11 Security section below) extends the life of the decade-old AAA protocol by implementing RADIUS as the core of its authentication philosophy (like its precursor WPA).

The RADIUS protocol uses a shared secret authentication mechanism and is known to be subject to off-line dictionary attacks when not implemented as recommended by the RFCs. The RFCs make recommendations that are often overlooked by administrators, including that shared secrets should be as large and unguessable as a well-chosen password, and that IP Security (IPSec) should be used to encrypt RADIUS shared secrets.

An Internet-Draft has been submitted to the IETF that recommends stronger language in RADIUS-related RFCs for protecting the RADIUS communications now ubiquitous to modern security architectures. The motivation behind this draft includes the desire to mitigate conceivably vulnerable scenarios involving RADIUS implementation, such as the following:

Wireless encryption keys – these are transported in cleartext within the RADIUS protocol, enabling an attacker access to both wireless and wired networks if RADIUS communication were sniffed and decrypted on the segment between AP and RADIUS server, which would reveal wireless packet details and authentication information.

802.11's distributed encryption / decryption architecture (as opposed to a centralized model) increases the potential entry points for attackers to target dictionary or key derivation attempts.

Exploiting a poorly configured rogue AP, an attacker could sniff and passively decrypt EAP credentials and Layer 2 encryption keys, then decrypt wireless traffic.

The above issues again stem from the lack of physical privacy inherent to 802.11 operation, and also from the fact that RADIUS is in fact a wired network AAA mechanism. The potential new vectors for attack introduced by RADIUS AAA usage on networks where no authentication is used on the wired portion highlight a critical contrast – the practice of using easily remembered passphrases suffices for AAA services in a wired environment but introduces vulnerability in the 802.11 context. Dictionary attacks deem long binary keys a requirement in order to mitigate the relative ease from which sniffed traffic can yield keys. In general, RFC-level compliance for enterprise RADIUS implementations is optimal to mitigate dictionary password guessing and other vulnerabilities.

## Summary

### NEXT-GENERATION 802.11 SECURITY

The previous discussions illustrate that 802.11-based products are rapidly evolving to improve security and deployability for enterprise administrators. Other noteworthy standards or working groups defined within IEEE 802.11 include:

802.11i (WPA2) – IEEE 802.11i, ratified in 6/04 as the new 802.11 wireless LAN security standard, is the first official 802.11 security upgrade from the original WEP standard. 802.11i complies with FIPS 140-2 data encryption requirements via AES-CCMP, and guarantees packet integrity. 802.11i also improves credential privacy and enables lower-level policy extension via capabilities such as secure fast handoff, secure de-authentication and disassociation, key-caching, and pre-authentication for optimized secure roaming.

802.11n – focused on enhancing data throughput to over 100Mbps, currently, two primary proposal groups exist for draft selection at IEEE 802.11 Task Group N (formed 1/04). WWiSE members include Broadcom, TI, and Nokia, while TGn Sync members include Atheros, Cisco, and Intel. A TGn Sync draft currently has provisional support with 56 percent of votes in favor of selection as the “first draft proposal of 802.11n” for refinement / ratification. Without 75% supermajority in favor of a May proposal revision, the selection process regresses to the 50% vote for provisional support. TGn Sync draft enhancements include:

Efficient Header Compression  
Frame Aggregation  
LongNAV, Pairwise, and Single-Ended Protection Mechanisms

Multiple Receiver Aggregation  
Pure MAC Aggregation Framing  
Reverse Direction Data Flow Signaling  
Single and Multiple Responder Aggregation Exchange Protocols  
Timed Receive Mode Switching Power Management

802.11e – currently on draft 13.0, Task Group e (formed in Jan 2001) is chartered with QoS standards definition for 802.11 networks. Proposed mechanisms include Enhanced Distribution Coordination Function (EDCF), used to prioritize based on multiple traffic categories. Higher-priority categories would have shorter Arbitration Interframe Spaces (AIFSEs, or wait periods) than lower-priority categories, enabling earlier initiation of random-number selection and countdown at the beginning of a contention window, at the end of which data would be transmitted (higher-priority categories) or a device would wait for the next idle period to transmit (lower-priority categories). Another proposed mechanism, hybrid coordination function (HCF), enhances 802.11 MAC Point Coordination Function (PCF, used for AP-coordinated contention-free transmission instead of DCF collision avoidance, see above section **MEDIUM AVAILABILITY & ACCESS**), by adding traffic classification capability.

802.11r – this Task Group is developing fast roaming for 802.11. However, 802.11i contains optional components that may alleviate roaming latency. For example, if both a supplicant and authenticator indicate that they have cached a PMK from a previous association, the supplicant skips a full 802.1X authentication cycle. 802.11i also allows pre-authentication, which decreases dropout probability by allowing a supplicant to background-authenticate with one station while associated with another.

#### **SYSTEM DESIGN CRITICALITY**

These working groups provide further support the assertion that despite accelerated 802.11 development pace and emergence of application-oriented 802.11 standards and draft proposal groups pushing continued base spec evolution, there remain significant challenges for the 802.11 industry in the realm of highly interoperable secure connectivity, policy management, and service assurance. Assumptions regarding physical access, level of user secrecy and data privacy, and ability to predictably deliver packets that generally apply within a wired Ethernet network are not applicable in 802.11 wireless LANs. Thus for 802.11 security vendors, sound system architecture and thoughtful subsystem integration become primary critical success factors for responsible implementation of emerging 802.11 standards and delivery of enterprise-class security capabilities without sacrifice to performance, usability, or interoperability.

---

Copyright © 2005 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.  
1194 N. Mathilda Ave. Sunnyvale, CA 95014 ATTN: General Counsel