CCNP Wireless IAUWS Quick Reference

William G. Daniel

Cisco Press

Chapter 1

Describing Regulatory Compliance

Failure to secure a WLAN makes it vulnerable to attack. To properly secure your network, you must be able to identify common threats to wireless and know how to counteract them.

Identifying Wireless Vulnerabilities

Rogue access points and clients

Cisco WLAN controllers identify access points (APs) outside their mobility group as rogue APs. Rogues are *friendly* if they do not pose a threat, such as APs belonging to neighbors. A rogue is *malicious* if it poses a threat to the network, such as an AP added to the wired network without permission from the IT department; such an AP could be used for illegitimate access to network resources. Malicious APs can also be external and used to disrupt your network; they include honeypots and evil twins. Honeypots are usually unsecured and set up to lure unsuspecting clients into giving up sensitive information or to infect them with a virus or worm. Evil twins mimic APs from your network. They are used to fool clients into connecting to a network that looks legitimate and then trick users into giving up sensitive information. Rogue clients are devices connected to rogue APs or to other clients in an ad hoc manner.

Denial-of-service attacks

Wireless denial-of-service (DoS) attacks keep users from connecting by overwhelming the AP’s radios. Wireless DoS attacks are usually committed by spoofing management frames, through jamming, or by infecting a client with a virus that floods the network with spurious traffic.

Over-the-Air Attacks

Over-the-air attacks include reconnaissance attacks (used to map out the network) or replay attacks (user data is captured and re-transmitted). Replay attacks work better in networks that use unencrypted or weakly encrypted data.

Securing client access

You need mutual authentication to properly secure client access to the network. Mutual authentication uses Extensible Authentication Protocol (EAP) to make the client identify itself to the network and the network identify itself to the client. Wireless clients accessing the network from outside the WLAN (for example, from a hotspot in a coffee shop) should use a VPN.

Securing guest access

We let guests access our WLANs so that they can connect to the Internet or to services we offer, but at the same time we must protect company traffic from accidental or unauthorized access. We also need to ensure that only authorized guests get to use our network.

Industry Standards and Associations

International Organization for Standardization (ISO)

The ISO has members from organizations in 159 countries, and they create standards for the computing industry. The following is a list of published standards from the 27000 series, which relates to information security:

- **ISO/IEC 27001:2005**. Specification for information security management systems
- **ISO/IEC 27002:2005**. Code of practice information security
- **ISO/IEC 27005:2008**. Information security risk management
- **ISO/IEC 27006:2007**. Guidelines for accrediting organizations that certify/register of information security management systems

Institute of Electrical and Electronics Engineers (IEEE)

The IEEE is an international organization that creates standards for IT and other engineering fields, including the following:

- **802.11-2007**: Combines 802.11a, b, d, e, g, h, i, and j with the base 802.11 standard
- **802.11i**: Created scalable security based on EAP-based authentication and Advanced Encryption Standard (AES) encryption
- **802.11r**: Draft standard for fast secure roaming intended to support voice
- **802.11u**: Draft standard for internetworking with non-802.11 networks
- **802.11w**: Draft standard for implementing management frame protection

Internet Engineering Task Force (IETF)

An international group interested in the continued growth and smooth operation of the Internet. They have created multiple RFCs affecting the wireless industry, including the following:

- **RFC 3579**: *RADIUS Support for EAP*
- **RFC 4017**: *EAP Method Requirements for WLANs*
- **RFC 4346**: *TLS v1.1*

- **RFC 4851**: *EAP-FAST*
- **RFC 5169**: *Handover Key Management and Re-authentication Statement*

Payment Card Industry Data Security Standard for Wireless Networks

An international standard designed to protect credit card information, personal data, and cardholder identities.

Wi-Fi Alliance

International nonprofit organization made up of Wi-Fi manufacturers. They test interoperability of Wi-Fi gear and create interim support measures for customers while waiting for a needed standard. The Wi-Fi Alliance created the following:

- **Wi-Fi Protected Access (WPA)**

  Authentication via EAP or WPA-PSK

  Encryption using Temporal Key Integrity Protocol (TKIP)
- **Wi-Fi Protected Access 2 (WPA2)**

  Authentication via EAP or WPA-PSK

  Encryption using AES

Cisco Compatible Extensions (CCX)

Cisco has written extensions enhancing client performance with Cisco wireless equipment and has made these extensions available to Wi-Fi manufacturers.

TABLE 1-1 CCX enhancements

CCX Version	V1	V2	V3	V4	V5
Security enhancements	Static WEP 802.1X LEAP Cisco TKIP	PEAP-GTC WPA	WPA2 EAP-FAST	NAC EAP-TLS PEAP-MSCHAPv2 MFP-v1	MFP-v2
Mobility and management enhancements		CCKM w/ LEAP Proxy ARP	CCKM w/ EAP-FAST SSO w/ LEAP, EAP-FAST	CCKM w/ PEAP-GTC, PEAP-MSCHAPv2, EAP-TLS	

Regulatory Compliance

Governments around the world have defined laws to protect sensitive information, including the following:

- **EU Directive on Data Protection 95/46/EC**

  Protects personal data used by multinational organizations within EU boundaries

  Prevents unauthorized disclosure of data by transmission, including location data

- **Health Insurance Portability and Accountability Act (HIPPA)**

  Requires organizations within the United States to use reasonable safeguards to protect electronic protected health information (EPHI)

  Includes access and audit controls, user and entity authentication, integrity mechanisms, and data encryption

- **Gramm-Leach-Bliley Act (GLBA)**

  Requires U.S. financial institutions to protect financial information