



To register for this course, go to www.giga-wave.com, or call 210-375-0085

Cisco Wireless LAN Security v4.0

Keyword: CWLS

4 Days – List Price \$2,695

Course Description

Cisco Wireless LAN Security Class is an advanced interactive seminar on how to secure a Cisco WLAN. This is the most comprehensive seminar on Cisco Aironet wireless security advantages in the industry! Topics include: WLAN security standards, how to mitigate WLAN attacks, WLAN EAP types and security configuration on both autonomous and lightweight access point architectures. Hands-on labs feature how to configure network and client equipment to provide maximum security including how to “Harden the access point”, and build VLANs with different forms of authentication and encryption. Attendees will receive an introduction to Cisco ACS RADIUS attributes and actually configure Cisco ADU for, PEAP and EAP-FAST, and TLS.

To participate in the hands-on labs, please bring a laptop computer with an available 32-bit CardBus slot and an Ethernet port. The laptop's operating systems must be either MS Windows 2000 (SP4) or XP. The laptop should also have a 9-pin serial port or USB to serial adapter. IN ADDITION, you will need administrator rights to the laptop to install drivers for the wireless client used in class.

You Learn...

After completing this course, the student should be able to:

- Describe security policy design and management
- Determine the components and basic configurations of Cisco core feature set
- Discuss how authentication and encryption are used to secure the WLAN
- Describe configuring the Cisco Secure ACS to provide 802.1X authentication for Cisco WLAN devices
- Describe configuring the access point to provide 802.1X authentication for Cisco WLAN devices
- Configure the access point to perform RADIUS authentication and Backup RADIUS authentication
- Set up, install and configure EAP-FAST, Cisco PEAP and EAP-TLS authentication on the ACS server, Active Directory, access points and Cisco Aironet wireless LAN adapters
- Configure VLANs on the access points, using different encryption and authentication methods per VLAN
- Configure the ACS and the access point to allow the ACS to provide VLAN assignment to the client
- Harden the access point
- Use WDS and CiscoWorks WLSE to detect rogue access points
- Determine the components and basic configurations of the Cisco WLAN Controllers and lightweight access points
- Identify the purpose of key security features configured through Cisco wireless administration tools
- Config wireless client cards to connect to the LWAPP network using EAP-FAST authentication w/ AES encryption
- Locate and contain access point as rouge access point through WCS

Who Would Benefit

Cisco Wireless LAN Security is an advanced curriculum for CIO's, IT managers, and technical engineers responsible for managing and securing wireless networks.

Prerequisite

- Aironet Wireless LAN Fundamentals and Site Survey (AWFSS) or Cisco Wireless LAN Fundamentals (CWLf)

Follow-On Courses

- Cisco Advanced Wireless Bridging (CAWBL)
- Aironet Wireless LAN Advanced Topics (AWLAT) or Cisco Wireless LAN Advanced Topics (CWLAT)
- Cisco Voice over Wireless LAN (VoWLAN)

Cisco Aironet WLAN Security – continued pg. 2

Course Content

Chapter 1 – Introduction

- Introduction
- Wireless LAN Security Today
- Introductions

Chapter 2 – Network Security and Cisco

- Network Security
- ISO FCAPS Model
- WLAN Security Standards
- WLAN Security Vulnerabilities
- WLAN Security Best Practices

Chapter 3 – Describing Cisco Aironet Autonomous Access Points

- Features and Components
- Cisco Integrated Services Routers

Chapter 4 – Describing WLAN Authentication and Encryption

- 802.1X Overview
- EAP-Cisco Wireless (LEAP)
- EAP-FAST
- EAP-TLS
- EAP-PEAP
- WPA and 802.11i Encryption
- WPA2/802.11i

Chapter 5 – Configuring Cisco Secure ACS

- Network Configuration
- System Configuration
- External User Database
- Group Setup
- User Setup

Lab 1 – Installing Aironet Desktop Utility

Lab 2 – Configuring Cisco Secure ACS

Lab 3 – Configuring EAP-FAST

Chapter 9 – Configuring Local RADIUS and Backup RADIUS on the Access Point

- Local Authentication
- Configuring a Local Authenticator
- Network Access Servers (AAA Clients)
- Encryption Manager
- Backup RADIUS Configuration

Lab 4 – Configuring Local RADIUS and Backup RADIUS on the Access Point

Chapter 11 – Installation and Configuration for Cisco Protected EAP

- PEAP Prerequisites
- Cisco ACS v4.0 Certificate Setup
- Access Point Setup
- Cisco ADU Setup for PEAP

Lab 5 – Cisco Aironet ADU PEAP Configuration

Chapter 13 – Installation and Configuration for EAP-TLS

- Obtaining a User Certificate
- Configuring ADU for EAP-TLS

- Configuring the Windows Client for EAP-TLS
- Configuring Cisco Secure Service Client

Lab 6 – Cisco Aironet ADU TLS Configuration

Lab 7 – Building VLANs with Different forms of Authentication and Encryption

Lab 8 – Using ACS to Assign VLANs

Lab 9 – Hardening the Access Point

Lab 10 – WDS and Rogue AP Detection using CiscoWorks WLSE

Chapter 19 – Describing the Cisco Unified Wireless Network

- Dynamic RF Management
- Security and VLANs
- Guest Tunnel and Anchor Mobility
- Cisco Enhanced Security Module

Chapter 20 – WLAN Advanced Feature Security

- Local Authentication
- MAC Filtering
- Access Control Lists
- Network Access Control
- Peer-to-Peer Blocking
- Radius Authentication
- Management Frame Protection (MFP)
- WPA, WPA2 and CCKM
- VPN Termination and Pass Through
- Rogue AP and Ad-Hoc Client Detection
- Intrusion Detection Management

Lab 11 – WPA and WPA2 Setup on a WLAN Controller

Chapter 22 – Using WCS to Monitor Security

- Lobby Ambassador
- Monitoring Administrative Accounts
- Rogue Access Points and Clients
- Monitoring CIDS Sensors

Lab 12 – WCS Rogue AP Detection and Mitigation