



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

Implementing Advanced Cisco Unified Wireless Security v1.0

Keyword: IAUWS

5 Days – List Price \$3,295

Course Description

This course is instructor-led training and includes instructor assisted, hands-on labs. The Implementing Advanced Cisco Unified Wireless Security training class is designed to help you prepare for the CCNP-Wireless certification. The goal of the IAUWS v1.0 is to provide network professional with information to prepare them to secure the wireless network from security threats via appropriate security policies and best practices, as well as ensure the proper implementation of security standards and proper configuration of security components. The IAUWS training class reinforces the instruction by providing you with numerous hands-on labs that range from configuring administrative security on the controller, configuring various EAP authentication options on Cisco Secure Services Client and troubleshooting client wireless connectivity issues, configuring the anchor and internal controllers to support guest access, isolating and resolving problems in a guest access wireless LAN (WLAN), configuring and verify wireless NAC out-of-band operations, configuring Hybrid Remote Edge Access Points (H-REAPs) to provide connectivity if the WAN fails and troubleshoot H-REAP security issues, configuring the controller for management frame protection, implementing access control lists and Identity Based Networking (IBN), identifying, locating, and containing a rogue access point, observing Intrusion Detection System (IDS) alerts on the Cisco Wireless Control System (WCS), as well as configuring Cisco WCS to operate with the Cisco adaptive wireless IPS solution.

Laptops are provided to participate in the hands-on labs. If you desire to use your own laptop, please bring a laptop computer with an available 32-bit CardBus slot and an Ethernet port as well as an internal wireless NIC, 802.11a/b/g. 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:

- Translate organizational and regulatory security policies and enforce security compliances
- Integrate security on client devices
- Design and implement guest access services on the WLAN controller
- Design and integrate a wireless network with Cisco NAC Appliance
- Implement secure wireless connectivity services on the WLAN controller
- Use the internal security features on the WLAN controller and integrate the WLAN controller with advanced security platforms to isolate and mitigate security threats to the WLAN

Who Would Benefit

The Implementing Advanced Cisco Unified Wireless Security course is targeted wireless network professionals with 3-5 years experience in the networking field who will be required to define the security requirements for various deployment models, and any individual wishing to attain the CCNP-Wireless level.

Prerequisites

- Interconnecting Cisco Networking Devices Part 1 (ICND1)
- Interconnecting Cisco Networking Devices Part 2 (ICND2)
- Implementing Cisco Unified Wireless Networking Essentials (IUWNE) v1.0

Follow-On Courses

- Conducting Cisco Unified Wireless Site Survey (CUWSS)
- Implementing Cisco Unified Wireless Mobility Services (IUWMS)
- Implementing Cisco Unified Wireless Voice Networks (IUWVN)

- **Implementing Advanced Cisco Unified Wireless Security v1.0 – continued p.2**

Course Content

Module 0 -- Course Introduction

Module 1 – Organizational and Regulatory Security Policies

- Describing Regulatory Compliance
- Segmenting Traffic
- Lab 1-1: Segmenting Traffic
- Configuring Administrative Security
- Lab 1-2 Configuring Administrative Security
- Managing WLAN Controller and Cisco WCS Alarms
- Identifying Security Audit Tools

Module 2 – Secure Client Devices

- Configuring EAP Authentication
- Describing the Impact of Security on Application and Roaming
- Lab 2-1: Configuring EAP Authentication on the Clients
- Configuring Cisco Secure Services Client
- Lab 2-2: Configuring Cisco Secure Services Client
- Troubleshooting Wireless Connectivity
- Lab 2-3 Troubleshooting Wireless Connectivity

Module 3 – Design and Implement Guest Access Services

- Describing Guest Access Architecture
- Configuring the WLAN to Support Guest Access
- Configuring Guest Access Accounts
- Lab 3-1: Configuring the WLAN to Support Guest Access
- Lab 3-2: Configure a Controller to use the Cisco NAC Guest Server for Authentication
- Troubleshooting Guest Access
- Lab 3-3: Troubleshooting Guest Access Issues

Module 4 – Design and Integrate Wireless Network with Cisco NAC Appliance

- Introducing the Cisco NAC Appliance Solution
- Configuring the Controller for Cisco NAC Out-of-Band Operations
- Lab 4-1: Configuring the Controller for Cisco NAC

Module 5 – Implement Secure Wireless Connectivity Services

- Configuring Authentication for the WLAN Infrastructure
- Lab 5-1: Configuring Local Authentication on the WLAN Controller
- Lab 5-2: Configuring H-REAP for WAN Failure
- Configuring Management Frame Protection
- Lab 5-3: Configuring Management Frame Protection
- Configuring Certificate Services
- Lab 5-4: Configuring Certificate Services
- Implementing Access Control Lists
- Lab 5-5: Implementing Access Control Lists
- Configuring Identity Based Networking
- Lab 5-6: Implementing IBN
- Troubleshooting Secure Wireless Connectivity
- Lab 5-7 Troubleshooting H-REAP Security Issues

Module 6 – Internal and Integrated External Security Mitigations

- Mitigating Wireless Vulnerabilities
- Lab 6-1 Managing Rogue Access Points
- Understanding Cisco's End-to-End Security Solutions
- Lab 6-2 Managing IDS Signatures
- Integrating Cisco WCS with Wireless IPS