

CORSO UFFICIALE DI CERTIFICAZIONE CWNA *CERTIFIED WIRELESS NETWORK ADMINISTRATOR*

Il modulo fondamentale del percorso di certificazione che rappresenta il livello di qualificazione professionale più importante oggi esistente a livello mondiale per progettisti e utenti di reti locali wireless.

Il Programma CWNP

Il programma CWNP è un percorso di certificazione a più livelli che porta il candidato a raggiungere i più alti livelli di competenza nel mondo delle installazioni wireless.

Il programma è stato creato e lanciato nel 2001 da Planet3 Wireless e oggi numerosissimi tecnici nel mondo possono vantare una certificazione internazionale, assolutamente indipendente da qualsiasi soluzione tecnico/commerciale, che attesta la completa padronanza delle problematiche e delle tecniche per operare con professionalità in un settore in forte evoluzione ma ancora caratterizzato da aspetti implementativi molto critici (prestazioni, sicurezza, ecc.). Nonostante il rapido sviluppo, la tecnologia wireless è ancora in fase di forte espansione e la possibilità di dimostrare le proprie competenze attraverso una certificazione autorevole e riconosciuta a livello internazionale, è una delle armi più potenti per far emergere la propria professionalità.

Planet3 Wireless Inc. ha creato questo programma di certificazione simili ad altri disponibili in altre aree tecniche (Cisco, Novell, Microsoft) per fornire ai professionisti del networking una preparazione tecnica che segue schemi standardizzati e misurabili. Nello stesso tempo offre ai datori di lavoro la possibilità di definire precisi livelli di competenza come obiettivo per i propri tecnici o come requisito per nuove assunzioni.

Il superamento degli esami CWNP dimostra il raggiungimento di ben determinati livelli di competenza nel campo delle reti wireless, ma, mentre per le certificazioni Cisco o Novell o Microsoft la competenza raggiunta è riferita all'utilizzo di prodotti specifici dei relativi produttori, la certificazione CWNP è la prova di una preparazione tecnica che può essere applicata su impianti realizzati con qualunque soluzione presente in commercio. E infatti le principali aziende del mondo nel campo delle reti, richiedono o raccomandano la certificazione CWNP.

Il percorso di certificazione CWNP si compone di tre livelli di competenza identificati dalle sigle CWNA, CWSP e CWNE.

La Certificazione CWNA

CWNA rappresenta il primo e più importante gradino del programma di certificazione CWNP. Il programma per l'ottenimento della certificazione CWNA copre un vasto campo di argomenti focalizzati sulla tecnologia descritta dalla famiglia di standard IEEE 802.11 ed è assolutamente indipendente da ogni soluzione commerciale. Un tecnico certificato CWNA è in grado di realizzare e di gestire una rete wireless secondo i più alti standard di affidabilità e sicurezza.



Il Corso CWNA

Spring propone il corso ufficiale per la preparazione all'esame CWNA nella sua forma standard di 5 giorni.

Il corso si compone di una parte teorica e di un laboratorio in cui verranno effettuate esercitazioni pratiche e sulla misura delle prestazioni con diverse soluzioni tecnologiche e architetture, sulla valutazione delle misure di sicurezza e sulle site survey. Il dettaglio del programma teorico e pratico del corso è riportato nelle pagine seguenti.

Il corso è tenuto da un istruttore certificato CWNA, in lingua italiana, mentre tutto il materiale del corso è in lingua inglese.

Prerequisiti

Per accedere alla certificazione CWNA non è necessario possedere alcun prerequisito, sebbene la conoscenza delle informazioni di base sulle reti informatiche può aiutare a comprendere meglio gli argomenti trattati nel corso.

Costo

Corso Spring CWNA: euro 2495,00 + IVA
La cifra comprende:

- 5 giorni di corso teorico/pratico
- coffee break
- colazioni di lavoro
- utilizzo della attrezzatura d'aula
- manuali e documentazione completa
- tassa d'esame internazionale PW0-104

Per saperne di più

Per maggiori informazioni su questo corso: www.spring-italy.it

Certificazione CWNA

Wireless LAN Administration Course Outline 3.0

The Wireless LAN Administration 3.0 course, whether in an academic format or a 5-day fast-track format, provides the networking professional a complete foundation of knowledge for entering into or advancing in the wireless networking industry. From basic RF theory to 802.11 frame exchange processes, this course delivers hands on training that will benefit the novice as well as the experienced network professional.

- Audience:** Novice or experienced networking professionals
- Duration:** 5 days, Classroom. May be taught over 1 academic semester.
- Associated Certification:** CWNA
- Prerequisites:** Basic networking knowledge, including OSI model and IP subnetting.

Introduction to 802.11 WLANs

- Discuss the standards organizations responsible for shaping the 802.11 Wireless LAN protocol
- Learn how standards compliance is enforced for 802.11 WLAN vendors
- Examine the 802.11 standard and various amendments
- Discuss additional networking standards that are commonly used to enhance 802.11 WLANs

Radio Frequency Fundamentals

- Physical aspects of RF propagation
- Types of losses and attenuation that affect RF communications
- Types of modulation used for wireless communications
- How channels and bandwidth are related to each other in wireless networks
- Three types of Spread Spectrum used in wireless networking

RF Power Output Regulations

- Understand international, regional, and local RF spectrum management organizations
- Understand RF channels in the unlicensed 2.4 GHz and 5 GHz frequency ranges
- How power output limitations are enforced by the FCC for Point-to-Multipoint (PtMP) and Point-to-Point (PtP) wireless connections

Power over Ethernet

- Recognize the two types of devices used in Power over Ethernet (PoE)
- Recognize the differences between the two types of Power Sourcing Equipment (PSE)
- Understand the two ways in which power can be delivered using PoE
- Understand the importance of planning to maximize the efficiency of Power over Ethernet

802.11 Analysis and Troubleshooting

- Introduction to 802.11 Protocol Analysis
- 802.11 Data Frames
- 802.11 Control Frames
- 802.11 Management Frames
- Frame Fragmentation
- Power Saving operations
- Transmission Rates

Coordinating 802.11 Frame Transmissions

- Differences between CSMA/CD and CSMA/CA
- Distributed Coordination Function (DCF)
- Quality of Service in 802.11 WLANs

Antennas

- Antenna characteristics and behaviors
- Types of antennas commonly used with WLANs
- Advanced antenna systems
- Antenna placement and mounting
- Antenna safety
- Types of antenna cables, connectors, and accessories

RF Math and System Operating Margin

- RF units of measure
- Basic RF mathematics
- RF signal measurements
- Understand link budgets
- Define and calculate System Operating Margin (SOM)

802.11 Service Sets

- Explain three types of service sets defined for use within 802.11 WLANs
- Roaming within a WLAN
- Load-balancing as a method to improve congestion in WLANs

Wireless LAN Operation

- Ad Hoc networks
- Infrastructure networks
- Bridged networks
- Repeater networks
- Mesh networks
- WLAN switched networks
- Enterprise Wireless Gateway networks
- Enterprise Encryption Gateway networks
- Virtual AP networks
- Evolution of WLAN architectures
- WLAN Management

WLAN Security

- Security Policy and Procedures
- Legacy 802.11 Security Components
- 802.11i Security Components
- WPA-Personal
- WPA-Enterprise
- WPA2-Personal
- WPA2-Enterprise
- Baseline Security Practices (SOHO, SMB, Enterprise)

Site Surveying

- Understanding the need for a site survey
- Defining business requirements and justification
- Facility analysis
- Interviewing network management and users
- Identifying bandwidth requirements
- Determining contours of RF coverage
- Documenting installation problems
- Locating interference
- Reporting methodology and procedures
- Understanding specifics of each vertical market
- Understanding the customer's network topology
- Creating appropriate documentation during and after the site survey
- Understanding safety hazards
- Using appropriate hardware and software to perform the survey
- Understanding the need for spectrum analysis
- Manual RF site surveys
- Predictive site surveys
- Dense AP deployment

Hands-on Lab Exercises**Infrastructure Mode Throughput Analysis**

This lab is built around measuring WLAN throughput under various circumstances that are broken into three separate areas:

- Pure mode throughput (802.11b vs. 802.11g vs. 802.11a vs. 802.11n)
- Mixed mode throughput
- Adjacent and co-channel interference

Understanding the "speeds and feeds" of all Wi-Fi technologies is crucial to optimizing WLAN installations, applications, and good network design. This lab demonstrates the varying throughputs for Wi-Fi connectivity standards by using FTP to transfer large files from client devices to servers. You will see and compare actual throughputs of each different technology, and the impact of using mixed technologies within the same radio spectrum.

These comparisons are done using four different network architectures:

- Autonomous APs and client devices in pure mode
- Autonomous APs and client devices in mixed mode
- WLAN Controller with Lightweight APs and client devices in pure mode
- WLAN Controller with Lightweight APs and client devices in mixed mode

Co-channel and adjacent channel interference affects throughput of Wi-Fi systems dramatically. Proper network design eliminates most channel interference. The affects of channel interference are demonstrated in this exercise.

Wireless LAN Security

The Wi-Fi Alliance has standardized security mechanisms for SOHO and SMB/enterprise environments. Two distinct classes of security mechanisms exist:

- WPA compliant
- WPA2 compliant

Within each class are two categories: Personal and Enterprise. WPA implies a pre-802.11i snapshot that addresses only TKIP encryption. WPA2 implies 802.11i compliant CCMP (default) and/or TKIP (optional). Enterprise implies the use of 802.1X/EAP authentication mechanisms, and Personal implies that passphrases are the authentication mechanism being used.

Wi-Fi Alliance Security Mechanism	Authentication Mechanism	Cipher Suite	Encryption Mechanism
WPA-Personal	Passphrase	TKIP	RC4
WPA-Enterprise	802.1X/EAP	TKIP	RC4
WPA2-Personal	Passphrase	CCMP (default) TKIP (optional)	AES (default) RC4 (optional)
WPA2-Enterprise	802.1X/EAP	CCMP (default) TKIP (optional)	AES (default) RC4 (optional)

Wi-Fi Alliance security mechanisms are only applicable at Layer 2 of the OSI model. Each of these mechanisms will be configured and tested in this lab exercise.

Other security mechanisms for WLANs exists such as VPNs (PPTP, IPSec) and secure applications (FTP/SSH, HTTPS, POP3/SSL). This lab exercise will demonstrate VPN technology using Microsoft's PPTP/MS-CHAPv2/MPPE-128 (RC4).

Site Surveying

Two specific classes of site survey methodology exist and are used in the WLAN market today:

- Manual site surveys (often called the "walkabout")
- Predictive analysis (often hailed as "the site survey method of the future")

Within each class exist two distinct categories. Manual site surveying can be categorized as either active mode or passive mode, and one or both modes can be used at any given time.

Predictive analysis software tools are based on a mathematical model of a facility blueprint and can be performed in two distinct ways. First, importing and AutoCAD (vectorized graphic) drawing allows the predictive analysis software tool to understand detailed complex layers of a facility's construction, including wall attenuation, attenuation between floors, and channel interference. Second, importing of raster graphics, such as .jpg or .bmp, allows for faster but less accurate modeling.

Neither methodology is 100% accurate, since each has its own individual weaknesses. Used together, the surveyor can create a more complete RF snapshot of any facility.

In this exercise, students will conduct both manual and predictive analysis surveying, using software and hardware tools (determined by the instructor or specific class needs).



Per iscriversi al Corso SPRING SPCWNA stampare e compilare il modulo presente ed inviarlo al **FAX: 02 659 5913**

Desidero partecipare al Corso SPCWNA per la Certificazione Internazionale CWNA

Nome

Cognome

Società Settore di attività

Via N°

Cap Città Prov.

Tel Fax e-mail

Codice Corso: **SPCWNA** Sede: Data:

Fatturare a:

Azienda (se diversa dall'intestazione)

Indirizzo
.....

C.F. /P. IVA

Il pagamento dell'importo totale di **€ 2994,00 (€ 2495,00 + IVA 20%)** sarà effettuato a ricevimento fattura tramite Bonifico Bancario su:

Banca San Paolo Intesa - Filiale di Rho (MI) - CIN: C ABI: 03069 CAB: 20502 C/C n°: 612005655981 IBAN: IT86C 03069 20502 612005655981 -- Intestato a: SPRING S.a.s.

La quota di partecipazione comprende quanto indicato nella descrizione del corso, la colazione di lavoro ed i coffee break. Le iscrizioni ed il pagamento devono pervenire, in ogni caso, almeno quindici giorni lavorativi prima della data d'inizio del corso; le iscrizioni eseguite oltre tale data limite sono accettate salvo disponibilità di posti e devono essere accompagnate dalla fotocopia del bonifico bancario.

SPRING S.a.s. si riserva il diritto di annullamento dei corsi programmati. In caso di annullamento si impegna a rimborsare e integralmente la quota versata per la partecipazione al corso annullato. L'esercizio del diritto di recesso unilaterale da parte del Cliente almeno dieci giorni lavorativi prima della data di inizio del corso non determina a suo carico alcuna penale. Trascorso tale termine il Cliente dovrà corrispondere a SPRING, a titolo di penale, salvo il maggior danno, un importo equivalente al 60% del corrispettivo concordato per la partecipazione al corso; nel caso la quota sia stata già versata, sarà trattenuta su quanto ricevuto.

Ai sensi della legge 67/96 a autorizzazione SPRING S.a.s. trattare i dati sopra riportati per la realizzazione delle proprie attività istituzionali, compresa la comunicazione, l'informazione e la promozione.

.....
Data

.....
Firma