Certified Wireless Technology Specialist (CWTS)

Course Summary

Description

Given by Certified Wireless Network Expert (CWNE) #1, who founded the Certified Wireless Network Professional (CWNP) Program, the Certified Wireless Technology Specialist (CWTS) is a certification that validates the knowledge and skillset of IT sales and support professionals on the basics of Enterprise 802.11 wireless networks. This comprehensive certification was designed to prove your understanding of Wi-Fi technology and pre-requisite data networking and to help put you on a track to continued success in the industry.

In this broad-based foundational course, you will learn the basics of networking devices, management systems, protocols, routing and switching, and common security threats and solutions. You will experience demonstrations of a broad scope of networking devices and diagnostic tools. Attending this course will prepare you to tackle networking tasks such as design, installation, configuration, and troubleshooting.

The CWTS certification is a sales and support level wireless LAN certification for the Certified Wireless Network Professional (CWNP) Program. To earn a CWTS certification, you must take the exam at a Pearson Vue Testing Center and pass with a score of 70% or higher. Instructors must pass with a 80% or higher. The CWTS is a lifetime certification. Because CWTS is an entry-level certification, no re-certification is required.

Topics

- The OSI Model
- Device Addressing
- Switching
- IPv4 Routing
- Internet Gateways
- Network Protocols
- Device Management and Security Threats
- Device Management and Internet Bandwidth
- Device Management
- Troubleshooting
- Wireless Technologies, Standards, and Certifications
- Hardware and Software
- Radio Frequency (RF) Fundamentals
- Site Surveying and Installation
- Applications, Support, and Troubleshooting
- Security and Monitoring

Audience

This course is for those wanting to obtain Certified Wireless Technology Specialist (CWTS) certification that validates the knowledge and skillset of IT sales and support professionals on the basics of Enterprise 802.11 wireless networks.

Prerequisites

There are no prerequisites for this course because CWTS is an entry-level certification

Duration

Four days

Certified Wireless Technology Specialist (CWTS)

Course Outline

I. **The OSI Model**
   A. OSI Model Layers, Physical Layer, Data Link Layer, Network Layer, TCP/IP Model
   B. Transport Layer, Ports, TCP, UDP, Session and Presentation Layers, Application Layer, Peer Communication, Encapsulation

II. **Device Addressing**
   A. Mac, IP, Local Addressing
   B. Packet Structure, Subnetting
   C. Host, Broadcast and Network
   D. Default Gateway, IP, Subnet, Public vs. Private Addresses

III. **Switching**
   A. Ethernet Hub, Switch, Bridge
   B. Virtual LANs

IV. **IPv4 Routing**
   A. Routing, Router Interfaces, Routing Table
   B. Routing Protocols, Routing in SOHO and SMB, Diagnostics

V. **Internet Gateways**
   A. SOHO and SMB, Gateways, NAT, PAT
   B. Port Redirection and DMZ Ports, Virtual Servers, VPN, Load Balancing
   C. SPI Firewall Features, Inter-VLAN Routing

VI. **Network Protocols**
   A. TCP, UDP, DHCP
   B. DNS, NTP
   C. NTP, TFTP, SYSLOG, FTP
   D. FTP, WebDAV, RTSP, RTP, SSH2 and Telnet

VII. **Device Management And Security Threats**
   A. Firewalls, Default Passwords, Insecure Management Protocols, Insecure Virtual Servers, Console Ports

VIII. **Device Management And Internet Bandwidth**
   A. Internet Bandwidth Per User, Local Storage, Cloud Storage, Cloud Backups
   B. Streaming and Social Media, Consumer Electronics, Computing Devices, Application Layer Visibility and Control (AVC)

IX. **Device Management**
   A. Device Management, Environmental Conditions, Cables and Cable Management, Console Ports
   B. Transport Layer, Ports, TCP, UDP, Session and Presentation Layers, Application Layer, Peer Communication, Encapsulation

X. **Troubleshooting**
   A. Diagnostic Tools, Rogue DHCP Servers, IP Address Conflicts
   B. Packet Structure, Subnetting

XI. **Wireless Technologies, Standards, and Certifications**
   A. Define the roles of the following organizations in providing direction and accountability within the wireless networking industry
      1. IEEE
      2. Wi-Fi Alliance
      3. Local regulatory authorities
   B. Define basic characteristics of and concepts relating to Wi-Fi technology
      1. Range, coverage, and capacity
      2. Frequencies/channels used
      3. Channel reuse and co-location
      4. Certified Wireless Technology Specialist
      5. Infrastructure and ad hoc modes
      6. BSSID, SSID, BSS, ESS, BSA, IBSS
      7. Network discovery via active and passive scanning
      8. 802.11 authentication and association
      9. Data rates and throughput
      10. The distribution system and roaming
      11. Protection Mechanisms
      12. Power saving operation
      13. Dynamic rate switching
   C. Summarize the basic attributes of the following WLAN standards, amendments, and product certifications
      1. 802.11a
      2. 802.11b
      3. 802.11g
      4. 802.11n
      5. Wi-Fi Multimedia (WMM) certification
      6. WMM Power Save (WMM-PS) certification
      7. Wi-Fi Protected Access (WPA/WPA2) certification

Certified Wireless Technology Specialist (CWTS)

Course Outline (cont'd)

   8. Enterprise
   9. Personal

D. Explain the role of Wi-Fi as a network access technology
   1. WPAN, WLAN, WMAN, WWAN
   2. The OSI reference model

XII. Hardware and Software

A. Identify the purpose, features, and functions of the following wireless network components. Choose the appropriate implementation or configuration steps in a given scenario.
   1. Access Points
   2. Controller-based
   3. Autonomous
   4. Cooperative
   5. Mesh
   6. Wireless LAN Routers
   7. Wireless Bridges
   8. Wireless Repeaters
   9. WLAN Controller
   10. Distributed and centralized data forwarding
   11. Power over Ethernet (PoE) Devices
   12. 802.3af and 802.3at
   13. Midspan
   14. Endpoint

B. Identify the purpose, features, and functions of the following client device types. Choose the appropriate installation or configuration steps in a given scenario.
   1. PC Cards (ExpressCard, CardBus, and PCMCIA)
   2. USB2
   3. PCI, Mini-PCI, and Mini-PCIe, and Half Mini PCIe cards
   4. Workgroup Bridges
   5. Client utility software and drivers

C. Identify the purpose, features, and proper implementation of the following types of antennas.
   1. Omni-directional / dipole
   2. Semi-directional
   3. Highly-directional

D. Describe the proper locations and methods for installing RF antennas
   1. Internal and external (to the AP) antennas
   2. Pole/mast mount
   3. Ceiling mount
   4. Wall mount

XIII. Radio Frequency (RF) Fundamentals

A. Define the basic concepts and units of RF measurements, identify when they are used, and perform basic unit conversion.
   1. Watt (W) and milliwatt (mW)
   2. Decibel (dB)
   3. dBm
   4. dBi
   5. RSSI
   6. SNR

B. Identify and explain RF signal characteristics
   1. Frequency
   2. Wavelength
   3. Amplitude
   4. Phase

C. Identify factors which affect the range and rate of RF transmissions
   1. Line-of-sight requirements
   2. Interference (Wi-Fi and non-Wi-Fi)
   3. Environmental factors, including building materials
   4. Free Space Path Loss

D. Define and differentiate between the following physical layer wireless technologies
   1. 802.11b HR/DSSS
   2. 802.11g ERP
   3. 802.11a OFDM
   4. 802.11n HT

E. Define concepts which make up the functionality of RF spread spectrum communication
   1. 802.11 channels
   2. Co-location of 802.11a/b/g/n systems
   3. Adjacent-channel and co-channel interference
   4. WLAN / WPAN co-existence
   5. CSMA/CA operation
   6. Half duplex communications

F. Understand and apply basic RF antenna concepts
   1. Passive Gain
   2. Beamwidth
   3. Simple diversity
   4. Polarization

G. Identify the use of the following WLAN accessories and explain how to select and install them for optimal performance and regulatory domain compliance
   1. RF cables

Certified Wireless Technology Specialist (CWTS)

Course Outline (cont'd)

2. RF connectors
3. Lightning Arrestors and grounding rods

XIV. Site Surveying and Installation

A. Understand and describe the requirements to gather information prior to the site survey and do reporting after the site survey
   1. Gathering business requirements
   2. Interviewing stakeholders
   3. Gathering site-specific documentation including existing network characteristics
   4. Identifying infrastructure connectivity and power requirements
   5. Understanding RF coverage requirements
   6. Understanding application requirements

B. Define and differentiate between the following WLAN system architectures and understand site survey concepts related to each architecture. Identify and explain best practices for access point placement and density.
   1. Multiple Channel Architecture (MCA)
   2. Single Channel Architecture (SCA)

C. Describe the primary purpose and methodology of manual and predictive site surveys

D. Define the need for and the use of a manual site survey tool and differentiate between the following manual site survey types
   1. Active surveys
   2. Passive surveys

E. Differentiate between manual and predictive site surveys
   1. Advantages and disadvantages of each site survey methodology

F. Define the need for and use of site survey software or a protocol analyzer in a manual site survey as it relates to identifying, locating, and assessing nearby WLANs

G. Differentiate between site survey methods for indoor and outdoor wireless service

H. Define the need for and use of a spectrum analyzer in a site survey
   1. Identification and location of interference sources
   2. Differentiation of Wi-Fi and non-Wi-Fi interference sources

I. Understand industry best practices for optimal use of directional and omni-directional antennas in site surveys

XV. Applications, Support, and Troubleshooting

A. Identify deployment scenarios for common WLAN network types and suggest best practices for these scenarios.
   1. Small Office / Home Office (SOHO)
   2. Extension of existing networks into remote locations
   3. Building-to-building connectivity
   4. Public wireless hotspotsCarpeted office, education, industrial, and healthcare
   5. Last-mile data delivery – Wireless ISP
   6. High density environments

B. Recognize common problems associated with wireless networks and their symptoms, and identify steps to isolate and troubleshoot the problem. Given a problem situation, interpret the symptoms and the most likely cause.
   1. Throughput problems
   2. Connectivity problems
   3. RF coverage or capacity problems
   4. Interference from Wi-Fi or non-Wi-Fi sources
   5. Application performance problems
   6. RF performance problems, such as multipath and hidden nodes

C. Identify procedures to optimize wireless networks.
   1. Infrastructure hardware selection and placement
   2. Identifying, locating, and removing sources of interference
   3. Client load-balancing and infrastructure redundancy
   4. Analyzing infrastructure capacity and utilization

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Certified Wireless Technology Specialist (CWTS)

Course Outline (cont'd)

XVI. Security & Monitoring

A. Identify and describe the following legacy WLAN security technologies.
   1. SSID Hiding
   2. WEP
   3. MAC Filtering

B. Understand the basic operation of and implementation best practices for the following WLAN security technologies.
   1. WPA- and WPA2-Personal
   2. WPA- and WPA-2 Enterprise
   3. 802.1X/EAP
   4. AAA and RADIUS
   5. Encryption – TKIP/CCMP

C. Understand the basic functions and implementation best practices for the following WLAN
   1. Security technologies.
   2. Role Based Access Control (RBAC)
   3. Virtual Private Networking (VPN)
   4. Wireless Intrusion Prevention Systems (WIPS)
   5. Captive Portals
   6. Network management and monitoring systems