

# Wireless 5

(Exam 212-50)

## Course Outline

### Module 01: Introduction to Wireless Communications

- Common Terminologies
- History of Wireless Communication
- Wired vs. Wireless Networks
- Types of wireless networks: Based on connection
- Types of wireless networks: Based on geographical area covered
  - WLAN
  - WWAN
  - WPAN
  - WMAN
  - Comparison Between WLAN, WWAN, WPAN and WMAN
- Advantages and Disadvantages of Wireless Network
- Limitations of Wireless Network
- Generations of Wireless Technology
  - 2 G
  - 2.5 G
  - 3 G
  - 4 G
- Uses of Wireless Technology
  - Satellite
  - Cellular phone networks
  - Laptop
  - Personal Digital Assistant (PDA)
  - Blackberry
  - Remote control
  - M-Commerce

### Module 02: Wireless Signal Propagation

- Common Terminologies
- Analog and Digital signals
- Radio Waves

**Course Outline**

- Infrared Light
- Transmission Speed
- Components of a Radio System
  - Filter
  - Mixer
  - Amplifier
- Transmission Direction
  - Simplex Transmission
  - Half-duplex Transmission
  - Full-duplex Transmission
- Switching
- Signal strength
- UWB
- Modulation
  - Analog Modulation
    - Amplitude Modulation(AM)
    - Frequency Modulation (FM)
    - Phase Modulation
  - Digital Modulation
    - Amplitude Shift Keying
    - Frequency Shift Keying
    - Phase Shift Keying
- Spread Spectrum
  - Frequency Hopping Spread Spectrum
  - Direct Sequence Spread Spectrum

**Module03: Wireless Communication Standards**

- Common Terminologies
- Institutes offering Wireless Communication Standards
- IEEE
- IEEE Standards
- 802. Architecture
- 802.1X
- 802.11 (Wi-Fi Standard)
  - 802.11 Architecture
  - 802.11 Standards
  - 802.11a

**Course Outline**

- 802.11b
- 802.11e
- 802.11g
- 802.11h
- 802.11i
- 802.11j/ 802.11k
- 802.11m/ 802.11n
- 802.15
- 802.16
  - Wi-MAX
- P1451.5
- ETSI Standards
- HIPERLAN (High Performance Radio LAN)
  - HIPERLAN/1
  - HIPERLAN/2
  - HiperAccess (High Performance Access Network Technology)
  - HiperLink
- HIPERMAN (High Performance Radio Metropolitan Area Network)

**Module 04: WLANs and Operations**

- Introduction to WLAN
- Advantages of using WLAN
- Basic components of a WLAN
- How to access a WLAN
- Types of WLAN
  - Ad Hoc Networks
    - Mobile Ad Hoc Networks (MANET)
  - Infrastructure Networks
  - Repeater Networks
  - Bridged Networks
  - Mesh Networks
  - Enterprise Wireless Gateway Networks
  - Enterprise Encryption Gateway Networks
  - Virtual AP Networks
  - WLAN Array
- Roaming
  - Steps for Association

**Course Outline**

- Steps for Re-association
- Campus Topologies
- Virtual LAN
- Distributed Coordination Function/ Enhanced DCF
- Transmission Opportunity (TXOP)
- Proxy Mobile IP
- WLAN Management
- Setting up a WLAN
- Configuring WLAN: Prerequisites
  - Configure Computers For Automatic Addressing
  - Enable Automatic Wireless Network Configuration
- Run the Wireless Network Setup Wizard
- Configuring Firewall on WLAN
- Connecting to an Available Wireless Network
- WLAN Security: Passphrase
- Troubleshooting WLAN
- WLAN Diagnostic Tool: CommView for WiFi PPC
- WLAN Diagnostic Tool: AirMagnet Handheld Analyzer

**Module 05: Wireless Technologies**

- Common terminologies
- Wireless Technologies
- IrDA
- Bluetooth
- Wibree
- Wi-Fi
  - Hotspot
  - WISP
- GSM
  - GPRS
  - EDGE
- FDMA
- TDMA
- CDMA
- CDMA vs. TDMA
- ZigBee
  - ZigBee Stack Architecture

**Course Outline**

- ZigBee Devices
- ZigBee Network Model
- Characteristics of ZigBee/IEEE 802.15.4 Standards
- Benefits of ZigBee
- ZigBee Security Issues
- Fixed wireless Broadband Technologies
  - LMDS
  - MMDS
  - LMDS vs. MMDS
- IDEN
- CDPD
- HSCSD
- PDC-P
- FRS and GMRS
- BSS and IBSS
- HPNA and Powerline Ethernet

**Module 06: Wireless Protocols and Communication Languages**

- Common Terminologies
- Wireless Protocols
  - WAP
    - WAP Micro Browser
    - WAP Model
  - TKIP
  - SWAP
  - EAP
    - LEAP
    - PEAP
  - LDAP
  - RADIUS
  - WRAP and HDTP
  - CCMP
  - SIP
  - SOAP
  - RSN
- Programming languages Used for Wireless Communication
  - J2ME

- CLDC
- MIDP
- J2ME Schema
- WML
- BREW
- cHTML
- HDML
- VoiceXML

### Module 07: Wireless Devices

- Common Terminologies
- Wireless Infrastructure
- Antennas
  - Types of Antenna
    - Directional/ Omnidirectional Antenna
    - Aperture Antennas/ Leaky-wave Antennas
    - Reflector Antennas
  - Antenna Functions
  - Antenna Characteristics
- Access Points
  - Operating Modes of Access Points
- PC Cards
- Wireless Cards
- Wireless Modem
- Wireless Router
- Using a Wireless Router as an Access Point
- Wireless USB
- Wireless Game Adapter
  - Wireless Game Adapter: WGE111- 54 Mbps
- Wireless Print Server
- Wireless Range Extender
- Wireless Internet Video Cameras
- Bluetooth Connectivity Devices: Air2Net Bluetooth PC Card
- Bluetooth Connectivity Devices: Bluetooth Combo Print Adapter
- Wireless Media Gateway: WMG80
- Wireless Presentation Gateway: D-Link DPG-2000W
- Hotspot Gateway

- GSM Network Devices
  - Mobile Station (MS)
    - Mobile Station Application Execution Environment (MexE)
  - Base Station Subsystem (BSS)
    - Base Station Controller (BSC)
    - Base Transceiver Station (BTS)
  - Network Subsystem (NS)
    - Mobile Switching Center (MSC)
    - Mobile Switching Center Databases
- Mobile Switching Center
- Add Wireless To a Wired Network

### **Module 08: Fundamentals of RFID**

- RFID
- Components of RFID Systems
  - RFID System Architecture
  - RFID Tags
    - Passive RFID Tags
    - Active RFID Tags
  - RFID Tag Reader and Antenna
  - RFID Controller, Premises Server and Integration Server
- Chipless RFID Tag
- RFID Stations
- RFID Frequencies
- Applications of RFID Systems
- RFID Standards
  - ISO RFID Air Interface Standards
  - EPC Standards
- RFID Collisions
- RFID Security and Privacy Threats
  - Protection against RFID Attacks
- RFID Malware
  - RFID Exploits
  - Defending against RFID Malware
- RFID Security
- RFID and Privacy Issues
- RFID Vendors

### **Module 09: Wireless VoIP**

- Overview of VoIP
  - VoIP Technology
  - Software Support for VoIP
- Mobile VoIP
- VoIP over BreezeACCESS VL
- Voice over WLAN (VoWLAN)
  - Characteristics Of VoWLAN
  - Limitations of VoWLAN
- Wireless VoIP
  - Wireless VoIP Deployment
  - Advantages of Wireless VoIP
  - Limitations of Wireless VoIP
  - Standards and Protocols
    - ITU-T and H.323
    - Session Initiation Protocol (SIP)
    - Media Gateway Control Protocol (MGCP)
    - Real-time Transport Protocol (RTP) / RTP Control Protocol (RTCP)
  - MediaPro: VoIP and Video Analyzer
  - 323Sim: H.323 Simulator
  - Unlicensed Mobile Access (UMA)
  - Wireless VoIP Gateway: AH1038
    - Wireless VoIP Gateway: D-Link DVG-G1402S
    - Wireless VoIP Gateway: Motorola HH1620 DSL
  - Wireless IP Phone
    - Wireless VoIP Phone: EZLoop
    - Wireless VoIP Phone: P-2000W\_V2
    - Wireless VoIP Phone: Shenzhen WP10W-S
  - Challenges to Build Successful Wireless VoIP Product
- VoIP Vendors
- Attacks on Wireless VoIP

### **Module 10: Wireless Security**

- Wired vs. Wireless Networks
- Business and Wireless Attacks
- Types of Wireless Attacks



**Course Outline**

- Man-in-the-Middle Attack
- Denial-of-Service Attack
- Terminology
- WEP
  - Cracking WEP
  - WEP Tool: WEPCrack
- SSID (Service Set Identifier)
  - Beacon Frames
  - Authentication Modes
- MAC Address
  - MAC Sniffing and AP Spoofing
  - Tool to Detect MAC Address Spoofing: Wellenreiter v2
- Rouge Access Points
- Stream Cipher
  - PAD Collection Attacks
- Steps for Hacking Wireless Networks
  - Tool: NetStumbler
  - Tool: Kismet
  - WEP Tool: AirSnort
- WPA
- DMZ
- MIC
- WTLS
- Mobile Security through Certificates
- Certificate Management through Public Key Infrastructure (PKI)
- Tool: WifiScanner
- Tool: BTScanner
- Wireless Network Security Checklist
- Securing Wireless Networks