Course ID
WIFI-DIVE
Course Duration
2-5 days

Course Title

WiFi Training in Depth: Technology, Security, Deployment; Relationship with M2M, IoT, 5G

Aimed At

Engineers, technicians, managers, marketing/sales, and other professionals who need to understand the WiFi technology.

Prerequisites

Background in Information Technology or Telecommunications.

Course in a Nutshell

WiFi Training in Depth: Technology, Security, Deployment; Relationship with M2M, IoT, 5G, a 2-to-5 day course, provides comprehensive coverage of the entire set of IEEE 802.11 specifications, including 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ad, 802.11af, 802.11ah, 802.11ax, 802.11ay, 802.11az, and 802.11mc.

We discuss the technology, design, optimization, deployment, security, coexistence, and network attack/defense methods. We also examine the evolution and relationship of WiFi to the emerging M2M, IoT, and 5G wireless technologies.

Customize It!

Two-to-five day subsets of the course *WiFi Training in Depth: Technology, Security, Deployment; Relationship with M2M, IoT, 5G* with content catering to the needs of various audiences -- such as developers; network design, deployment, trouble-shooting, and security professionals; and marketing/sales professionals or others who need a less technical course -- are available. We can add a design or troubleshooting lab as needed and calibrate the technical level of this course to your team's backgrounds.

Course Outline

WiFi Training in Depth: Technology, Security, Deployment
Part 1: IEEE 802.11 Overview

- **WiFi: Market Landscape**
  - Market for Wi-Fi
  - Manufacturers
  - Uses of Wi-Fi
  - Installed base and projections
  - Chipset manufacturers
  - Device manufacturers
- **Short-Range Wireless Characteristics**
  - Wired vs wireless
    - Comparison of networks
    - Comparison of security challenges

        - Short-range wireless systems
    - Available short range wireless systems
    - Local area and personal area networks
    - LAN and PAN players
- **Introduction to Security Attacks and Countermeasures**
    - Layered security attack methods
    - Shared key and public key cryptography
- **Categories of Information Transmission**
    - Asynchronous, isochronous, and synchronous requirements
    - Voice and data
- **IEEE 802.11 Network Architecture**
    - General IEEE 802.11 architecture
    - Basic, extended, and independent service sets
    - Examples of implementations
- **Overview of IEEE 802.11 and Wi-Fi**
    - General architecture
    - Wi-Fi Alliance
    - IEEE 802.11 task groups

WiFi Training in Depth: Technology, Security, Deployment Part 2: IEEE 802.11 Physical Link

- **Radio Frequency (RF) Basics**
    - The electromagnetic spectrum
    - RF propagation and fading
    - RF modulation techniques
    - Reflection, refraction, and diffraction
    - Basics of digital RF communication
    - Free space loss
- **Link Budget and Path Loss**
    - Review of decibels
    - Calculating maximum range
    - Multipath characteristics and mitigation
- **Multipath**
    - Doppler and delay spread
    - Diversity combining
- **Basic Modulation Techniques**
    - Amplitude, frequency, and phase shift keying (ASK, FSK, PSK)
    - Complementary Code Keying (CCK)
- **Error Control**
    - Error characteristics
    - Cyclic Redundancy Check(CRC)
    - Convolutional coding
    - Automatic Repeat ReQuest (ARQ)

- **Overview of Older IEEE 802.11 Technologies**
  - Overview of 802.11b
  - Overview of 802.11a
  - Overview of 802.11a/g
  - Packet structure
    - DSSS methods
    - Processing gain
    - Complementary Code Keying (CCK)
    - IEEE 802.11a/g radio requirements
    - IEEE 802.11a/g jamming vulnerability
    - IEEE 802.11a/g PHY packet structure
    - Quadrature Amplitude Modulation (QAM)

WiFi Training in Depth: Technology, Security, Deployment Part 3: IEEE 802.11 MAC and Management Operations

- **MAC Methods**
  - Carrier-sense multiple access
    - Basic concept and operation
    - Avoiding network instability
    - CSMA and Denial-of-Service (DoS) attacks
  - Distributed Coordination Function (DCF) operation
    - Channel access and backoff
    - DCF and Man-in-the-Middle (MITM) attacks
  - Point Coordination Function (PCF) operation
    - Channel access and scheduling
  - Operation in an independent basic service set (ad-hoc)
- **MAC Frame Construction and Examples**
  - Management, control, and data frames
  - Throughput comparisons
  - IEEE 802.11e Quality-of-Service (QoS) operation
- **802.11 Management Operations**
  - Physical Layer Management Entity (PLME)
  - MAC Layer Management Entity (MLME)
  - Connection process
  - Addressing and traffic flow
- **Throughput Capabilities**
  - Frame transmission times
  - Throughput analysis
- **Roaming**
  - Layer 2 and Layer 3 roaming
  - Overview of 802.11r Fast BSS Transition
- **Mesh Networking**
  - Deployment scenarios

- Overview of 802.11s Mesh Networking

WiFi Training in Depth: Technology, Security, Deployment Part 4: IEEE 802.11n

- **Introduction to IEEE 802.11n**
  - Multiple Input, Multiple Output (MIMO)
    - MIMO channel model
    - MIMO signal model
    - MIMO transceiver design
    - Capacity limits of MIMO systems
    - Space–Time Block Coding (STBC) principles
- **IEEE 802.11n PHY Overview**
  - Channel bandwidth
  - MIMO in IEEE 802.11n
    - Un-coded signals
      - MIMO receivers for Un-coded Signals
    - MIMO receivers for Coded Signals
  - MAC efficiency enhancements
  - IEEE 802.11n operating channel frame structure
  - IEEE 802.11n modulation and coding (MCS)
    - MCS rates
  - IEEE 802.11n transmission modes
    - High Throughput (HT) Mode
    - HT Duplicate Mode
    - Short Guard Interval
    - Legacy Duplicate Transmission
  - IEEE 802.11n operation models
    - Legacy field
    - Greenfield
    - Mixed mode
  - PHY Layer Convergence Protocol (PLCP) and Physical Media Dependent (PMD) principles
  - PHY service specifications
  - PHY interfaces
  - PLCP packet format
  - The High Throughput Preamble
  - QAM Mapping STBC
  - Pilot subcarriers
  - IEEE 802.11n channelization
  - Transmit Out of Band Emission (OOBE) and Spectral Mask
  - IEEE 802.11n packet alignment
  - Reduced Interframe Space (RIFS)
  - Beamforming

- Non-Compressed Steering Matrix Feedback
- Compressed Steering Matrix Feedback
- High Throughput Preamble Format for Sounding PLCP Protocol Data Units (PPDUs)
  - Sounding with a zero length packet
  - Sounding PPDU for calibration
  - Sounding PPDU for channel quality assessment

- **IEEE 802.11n MAC**
  - Frame formats
    - MAC frame formats
    - Control frames
    - Block ACK (BA) MAC Protocol Data Unit (MPDU)
    - Management frame formats
    - Management action frames
    - MIMO Power Save Management Action Frame
    - MIMO Channel Measurement Frame
    - MIMO Channel State Information (CSI) Matrices Frame
    - MIMO Uncompressed Steering Matrices Frame
    - Compressed Steering Matrices Feedback Frame
    - Antenna Selection Indices Feedback Frame
    - Aggregated MPDU (A-MPDU) Format
  - MAC functional description
  - Protection mechanisms
  - Aggregation exchange sequences and related rules
  - Link adaptation
  - Probe response rule
  - Coexistence management
  - Channel management
  - STAtion (STA) Asking for MIMO Power Save Support
  - Channel management at the Access Point (AP)
- **IEEE 802.11n Planning and Deployment**
  - IEEE 802.11n network design
  - AP frequency assignments
  - 802.11n capacity design
  - Extensive measurements design
  - 802.11n propagation and coverage
    - Complete coverage of the area
    - MIMO considerations in capacity and coverage
    - Interference sources
  - Network scenarios

WiFi Training in Depth: Technology, Security, Deployment Part 5: IEEE 802.11ac

- **802.11ac Core Concepts and Requirements**
  - IEEE 802.11ac-2013 usage models
  - Feature requirements and evaluation methodology
  - Channel model
  - Specification framework
  - Backwards compatibility
  - Coexistence
  - Single-STA (station) throughput
  - MAC Service Access Point (SAP)
  - Multi-STA throughput (measured at the MAC SAP)
- **Introduction to IEEE 802.11ac**
  - Enhancements for Very High Throughput for operation in bands below 6GHz
  - Operation in the 5 GHz spectrum
  - Configurable frame length
  - OFDM-MIMO in IEEE 802.11ac
  - RF channel issues
- **IEEE 802.11ac PHY**
  - Channelization
  - OFDM frame structure
    - Subcarrier Rotation per Signal Bandwidth
  - Frame format
    - Very High Throughput (VHT) Mixed
  - 802.11ac Data Field for Single User with Binary Convolutional Coding (BCC)
    - 802.11ac modulation
    - 802.11ac interleaving and coding architecture
    - 11ac Single User MCS Indices
- **IEEE 802.11ac MAC**
  - MAC Changes in IEEE 802.11ac
  - MAC-layer Frame Aggregation
  - Aggregate MAC Service Data Unit (A-MSDU) vs. A-MPDU
  - RTS/CTS operation
  - MAC framing
  - Management frames
  - Medium access procedures
  - Clear-Channel Assessment (CCA)
- **IEEE 802.11ac Transmitter Specification**
  - OOBE and Spectral Mask
  - Transmit Spectral Flatness
  - Transmit Center Frequency and Symbol Clock Leakage and Tolerance
  - Packet alignment
  - Modulation accuracy
  - Transmitter Constellation Error

  - Error Vector Magnitude (EVM)
- **IEEE 802.11ac Receiver Specification**
  - Receiver minimum input sensitivity
  - Adjacent and nonadjacent channel rejection
  - Receiver maximum input level
- **IEEE 802.11ac Operation Scenarios and Testing**
  - Operation scenarios
  - Burst Detection failed
  - Time Sync failed

WiFi Training in Depth: Technology, Security, Deployment Part 6: IEEE 802.11af (White-Fi)

- **Introduction**
  - Coverage and gap analysis for co-channel deployment
  - Benefits of IEEE 802.11af, White-Fi
  - IEEE 802.11af propagation characteristics
  - Systems operating the TV white spaces
  - Frequencies below 1 GHz
  - Components of IEEE 802.11af architecture
  - TV White Space (TVWS) band in the United States and Canada (54 MHz to 698 MHz)
  - TVWS band in Europe
- **802.11af Physical Layer**
  - TV Very High Throughput (TVHT) STA PHY structure
  - Format of individual frame types
  - Frame formats
    - PHY service specification
    - MAC frame formats
    - Management frames
    - Beacon frame format
    - Probe Request frame format
    - Probe Response frame format
  - Operation under Geolocation Database (GDB) control
  - Layer management
  - TVWS functions
  - TVHT PHY functions
  - PHY management entity (PLME)
  - TVHT PHY service interface
  - Modulation and coding scheme (MCS)
- **IEEE 802.11af MAC layer**
  - MAC sublayer functional description
  - MAC architecture
  - TVHT MAC features
  - MLME SAP interface

  - Management frame body components
  - HCF
  - Extensible TLV parsing
  - MLME
  - TVHT PLME
    MAC protocol capabilities
  - QoS base functionalities
- **IEEE 802.11af Data Rates**
  - Multi-rate support
- **802.11af Spectrum Regulation**
  - Radio measurement procedures
  - Spectrum management extensions

WiFi Training in Depth: Technology, Security, Deployment Part 7: IEEE 802.11ah

- **Introduction to IEEE 802.11ah**
  - IEEE 802.11ah use cases
    - Internet of Things (IoT)
    - Internet of Everything (IoE)
    - Home/building automation
    - Smart grid
    - Automotive
    - Wearable consumer electronics
    - Low-power sensors and meters
    - Extended range Wi-Fi
    - Environmental/agricultural monitoring
    - Healthcare
    - Smart city
  - Issues for sub-one-gigahertz (900MHz) band
  - IEEE 802.11ah requirements
    - Functional requirements
    - System performance
    - Supporting band
    - Coverage and data rate
    - Coexistence
    - Enhanced power saving
  - Internet of Things (IoT) and Machine to Machine (M2M) communications.
  - One-hop network topologies
  - Short and infrequent data transmissions
  - Dense AP deployment number of stations
    - Traffic Indication Map (TIM) stations
    - Non-TIM stations
- **IEEE 802.11ah PHY and MAC**

- Extended range Wi-Fi by IEEE 802.11ah
- IEEE 802.11ah global ISM spectrum allocation
- IEEE 802.11ah bandwidths
- Downlink Multi-User MIMO-OFDM (DL MU-MIMO)
- IEEE 802.11ah PHY optimization
  - Extended range
  - Power efficiency
  - Scalable operation
- IEEE 802.11ah link-budget
  - Transmission range and data rates
- IEEE 802.11ah coexistence with other systems
  - IEEE 802.15.4 (Zigbee)
  - IEEE P802.15.4g
  - 6LoWPAN,
  - Bluetooth,
  - Traditional Wi-Fi
- IEEE 802.11ah channel model
  - Urban Micro (UMi)
  - Suburban Macro (SMa)
  - Urban Macro (UMa)
  - Indoor Hotspot (InH)
  - Rural Macro (RMa)
  - Line of Sight (LoS)
  - Non Line of Sight (NLoS)
  - Outdoor to Indoor
  - Spatial Channel Model (SCM)
  - Outdoor Path Loss Models
  - Outdoor Device to Device Models
  - Indoor MIMO Channel Models
- IEEE 802.11ah implementation and deployment
  - 802.11ah transmission modes
  - 802.11ah MAC throughput enhancements
  - Compact MAC header format
  - The QoS and High Throughput, HT fields
  - MAC power saving and channel access
  - Target Wake Time and Restricted Access Window (RAW)
  - Bi Directional TXOP
  - Sectorization

WiFi Training in Depth: Technology, Security, Deployment Part 8: IEEE 802.11ax

- **Introduction to IEEE 802.11ax**
  - IEEE 802.11ax basics
  - Frequency bands

  - 802.11ax PHY enhancements
    - MU-MIMO
    - OFDMA building block
- **IEEE 802.11ax PHY Layer**
  - High Efficiency (HE) Physical Layer
    - HE data field
  - 802.11ax modulation and coding (MCS)
    - LDPC coding scheme in the HE PPDU data field
    - MCS levels
  - Multi-user features
    - DL OFDMA and UL and DL MU-MIMO
    - MU RTS/CTS procedure
    - UL OFDMA-based random access
  - Sounding protocol
  - GCR BA operation
- **IEEE 802.11ax MAC Functions**
  - Target Wake Time (TWT)
  - Power save
  - Fragmentation
  - Frame formats
  - Sounding feedback
  - Overlapping Basic Service Sets (OBSS) and OBSS interference handling
- **IEEE 802.11ax Network Planning**
  - 802.11ax channel models
    - Spatial Channel Models (SCM)
    - Indoor and outdoor spatial channel models
    - Outdoor spatial channel models
    - UMi and UMa channel models
    - Path Loss model
  - 802.11ax coverage and capacity objectives
  - 802.11ax capacity planning
  - Propagation models
  - Site surveys: Predictive and manual

WiFi Training in Depth: Technology, Security, Deployment Part 9: Other IEEE 802.11 Technologies

- **IEEE 802.11ad**
  - Wireless Gigabit Alliance (WiGig)
  - WiFi in millimeter range
- **IEEE 802.11ay**
  - License-exempt above 45 GHz
  - High speed coexistence with WiGig
- **IEEE 802.11az**

  - Next generation positioning
- **IEEE 802.11mc**
  - Packet collision for Heterogeneous MIMO-Based WiFi

WiFi Training in Depth: Technology, Security, Deployment Part 10: Wi-Fi Security

- **Wired Equivalent Privacy (WEP)**
  - Shared key and public key cryptography
  - Cryptanalysis attack methods
  - WEP encryption process and weaknesses
  - WEP data integrity process and weaknesses
  - WEP access control process and weaknesses
  - Denial-of-service (DoS) attack methods
  - Bluetooth security overview and comparison to WEP
- **IEEE 802.11i Access Control and Key Management**
  - Wired Equivalent Privacy (WEP) weaknesses
    - Desired security criteria
    - WEP operation
    - Weaknesses: Authentication, data confidentiality, data integrity
  - Introduction to Robust Security Network (RSN)
    - RSN security layers
    - Methods of authentication
    - IEEE 802.11i operational phases
  - IEEE 802.1X Port-Based Network Access Control
    - IEEE 802.1X authentication and key distribution
    - Digital certificate
    - Challenge-response using a RADIUS server
  - Extensible Authentication Protocol (EAP)
    - EAP request/response
    - EAP over LAN (EAPOL)
    - Key derivation and exchange
  - Transport Layer Security (TLS)
    - TLS handshake exchange
    - TLS and IEEE 802.11i
    - TLS over EAP
  - Security while roaming
    - Pre-authentication
- **IEEE 802.11i Encryption**
  - Temporal Key Integrity Protocol (TKIP)
    - TKIP implementation
    - Encapsulation and de-capsulation processes
    - TKIP message integrity
    - TKIP attack countermeasures

  - Advanced Encryption Standard (AES)
    - Requirements for WEP replacement
    - AES operation
    - AES modes and algorithms
    - 802.11i counter/cipher block chaining with message authentication code (CCM) protocol
  - Other 802.11i aspects
    - Access control
    - Data security
    - IEEE 802.11i and IPsec
    - IEEE 802.1X port based authentication
    - Portal/web based authentication
- **Wi-Fi Protected Access (WPA)**
  - IEEE 802.11i and Wi-Fi Protected Access (WPA)
    - Comparison of 802.11i and WPA
  - Versions of WPA
    - WPA Personal vs WPA Enterprise
    - WPA vs WPA2
  - WPA and RSN key hierarchy
    - Pairwise and group keys
    - Key hierarchy
    - Key derivation
  - WPA implementation requirements
    - Access points
    - Network adaptors
    - Client software
  - WPA certification
- **Wi-Fi Network Attack and Defense Methods**
  - Specific attack methods
    - Planning and executing an attack
    - Summary of specific attack methods
    - Disclosure, integrity, Denial-of-Service (DoS)
  - General methods for enhancing Wi-Fi security
    - AP placement
    - AP setup
    - Security outside of WPA/802.11i
  - Network analysis tools
    - Spectrum analyzer
    - Protocol analyzer
    - Other analyzers
  - Wireless Intrusion Detection Systems (WIDS)
    - Intrusion detection
    - Intrusion prevention
    - Implementation

- Survey of available WIDS products

WiFi Training in Depth: Technology, Security, Deployment Part 11: Wi-Fi Deployment and Optimization

- **Operating Frequencies and Signal Spectrum**
  - Frequency hopping
- **Key Performance Indicators (KPI)**
  - Range
  - Data rate and throughput
  - Latency
  - Security
  - Others
- **Project Planning**
  - Requirements
  - Site Survey
  - Coverage vs. Capacity
  - AP Installation
  - Network Traffic Analysis
- **Co-existence**
  - Interference characteristics
  - General coexistence strategies
  - Wi-Fi coexisting with other Wi-Fi networks
  - Wi-Fi coexisting with other wireless systems
  - Wi-Fi and Bluetooth
    - Wi-Fi effect on Bluetooth
    - Bluetooth effect on Wi-Fi
    - Techniques for improving coexistence
    - Coexistence between collocated devices
  - Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC)
  - Methods to improve coexistence
- **Infrastructure consideration**
  - WLAN controllers and switches
  - Load balancing and other considerations

WiFi Training in Depth: Technology, Security, Deployment Part 12: How WiFi Fits in with LTE, and 5G

- **Seamless Roaming**
  - Roaming between 3GPP and Wi-Fi
- **LTE vs Wi-Fi**
  - Scenarios where Wi-Fi is best
  - Scenarios where LTE is best
- **LTE-WiFi Aggregation (LWA)**
- **WiFi vs. Unlicensed LTE (LAA/eLAA/MulteFire)**

  - Listen Before Talk (LBT)
- **WiFi and Spectrum Sharing**
- **WiFi in 5G**

WiFi Training in Depth: Technology, Security, Deployment
Part 13: WiFi in Relationship with M2M, IoT, and 5G Wireless

  - M2M: What it is, applications, technologies
  - IoT: What it is, applications, technologies
  - 5G LTE: LTE-A evolution to 5G, features related to M2M and IoT
  - How WiFi fits in with M2M, IoT, and 5G

Course Wrap-up: Recap, Discussion, Course Evaluation

Website: www.eogogics.com **or** www.gogics.com
E-mail: info@eogogics.com
Tel. +1 (703) 345-4375
USA 1 (888) 364-6442