Course ID
BLUEOP
Course Duration
3 days

Course Title
Bluetooth: Operation, Security, Applications, and Coexistence

Related Courses

- Bluetooth: A Comprehensive Technology Overview (BLUETOOTH, 3 days)
- Wi-Fi Technology: Principles and Operation (WIFI3, 3 days)
- IEEE 802.11 (WiFi) Wireless LAN Security (WIFISEC, 3 days)
- Wi-Fi: Technology, Applications, Design, and Deployment (WIFI-TECH, 2 days)
- Short-Range Wireless Survey: WiFi, Bluetooth, and ZigBee (SHORTRANGE, 3 days)

Aimed At

Those who are developing or implementing high-performance wireless systems will benefit from the detailed analysis of the Bluetooth specification, including range calculations, modulation and packet structures, and how Bluetooth devices find each other and establish a communication link between them. Designers will gain insight into how device authentication, encryption, and other security measures are implemented in Bluetooth, and how a Bluetooth device communicates with its host. The strengths and weaknesses of Bluetooth against other wireless network protocols, and the interference they cause to each other, will be especially useful to those who must select one or more wireless methods best suited to their specific applications.

Group Size

5-25

Prerequisites

None

Course in a Nutshell

This comprehensive three-day course introduces and analyzes Bluetooth wireless networking based on Bluetooth specification 2.1 + EDR (Enhanced Data Rate).

Participants begin by studying Bluetooth signal propagation characteristics, modulation, packet structure, data and audio processing, and error control. The role of the Bluetooth link manager in establishing a connection and implementing security and encryption measures is then discussed. Various higher layers in the Bluetooth protocol stack are examined such as packet segmentation and reassembly, service discovery, the host controller interface, and the implementation of application profiles. The Bluetooth qualification program is discussed. Finally, the ability of Bluetooth to coexist with other wireless networks in the 2.4 GHz band is analyzed.

Customize It!

Let us know your motivation for studying Bluetooth so we can customize the course to your particular requirements. The course can be tailored for audiences such as equipment or application developers, networking specialists, and less technical audiences such as management, marketing/sales, and others.

Learn How To

- Calculate the range of a Bluetooth radio over various signal paths
- Explain the Bluetooth modulation and frequency hopping processes
- Describe Bluetooth packet structure and error control options
- Describe authentication and encryption methods available with Bluetooth
- Explain how a Bluetooth device searches for other Bluetooth devices
- Describe how a piconet is established and master-slave interaction occurs
- Discuss the role of a Bluetooth profile
- Understand the Bluetooth qualification program
- Analyze Bluetooth's ability to coexist with other wireless networks

Course Outline

Day One

- Overview of the Bluetooth Specification
  - Differences between wired and wireless communications
  - Categories of information transmission
  - Overview of short range wireless networks and their promoter groups
  - Bluetooth usage models and protocol stack
- The Bluetooth Radio and Signal Propagation
  - Review of decibels
  - Link budget equation and path loss model
  - Calculating maximum range
  - Partition attenuation and primary ray tracing
  - Eavesdropping vulnerabilities
  - Bluetooth basic data rate and enhanced data rate modulation
  - Frequency hopping spread spectrum operation
  - Transmitter and receiver performance requirements
- Baseband Signaling Part 1
  - Master/slave timing
  - Addressing methods
  - Error control
  - Packet structure
  - Setting frequency hop parameters
  - Logical transport mechanisms
  - ACL, SCO, and eSCO packet construction
  - Throughput in perfect and imperfect channels

Day Two

- Baseband Signaling Part 2
  - Operational state diagram
  - Paging and inquiry processes
  - Sniff, hold, and park modes
  - Scatternet operation
- Link Management
  - Link connection and detachment
  - Link Management Protocol (LMP) packets
  - Managing sniff, hold, and park modes
  - Transmit power control and quality of service
  - Link setup using LMP packets
- Logical Link Control and Adaptation Protocol (L2CAP)
  - L2CAP functions and modes
  - Packet structure
  - Packet segmentation and reassembly
  - Protocol multiplexing and channel definitions
  - L2CAP signaling and channel setup
  - L2CAP actions and events
- Host Controller Interface
  - HCI overview and purpose
  - Command packet structure and examples
  - Event packet structure and examples
  - HCI as a high level language
  - HCI data packets
  - HCI/USB interface packet flow

Day Three

- Bluetooth Security
  - Security overview
  - Shared and public key cryptography
  - Attack methods
  - Link key generation
  - Authentication
  - Encryption
  - Security weaknesses
  - Secure simple pairing
- Applications
  - Application traffic flow
  - Service discovery protocol
  - Profile interaction

- Sample profile: Headset profile (HSP)
- Qualification and testing
- Hardware solutions
- UWB and ULP protocols

- Coexistence
  - Interference modeling
  - Bluetooth-on-Bluetooth interference
  - IEEE 802.15.2 coexistence task group
  - Coexisting with Wi-Fi: Separated nodes
  - Adaptive Frequency Hopping (AFH)
  - Coexisting with Wi-Fi: Collocated nodes
  - Antenna isolation methods
  - Active coexistence methods and performance

- Wrap-up
  - Course recap and Q/A
  - Evaluations

How You Will Learn

- A seasoned engineer-instructor well versed with Bluetooth and other short-range wireless technologies will present this course in participative lecture format.
- Along with the lecture, he will use exercises to reinforce the instruction and elucidate the important points.
- If you already know something about Bluetooth, he will build on that knowledge. He'll compare and contrast what you know with what's new, making the new concepts easier to acquire.
- If your background is less technical, we will use examples and analogies to reduce the complexity of the subject matter.
- You will receive a printed Participant Handbook which will serve as a good reference after you're back on the job.

Revised *April 20, 2008f*