Course ID
BLUETOOTH5
Course Duration
5 days

Course Title

Bluetooth: An In-depth Five Day Course

Related Courses

- Bluetooth: A Comprehensive Technology Overview (BLUETOOTH, 3 days)
- Bluetooth: Operation, Security, Applications, and Coexistence (BLUEOP, 3 days)
- Short-Range Wireless Survey: WiFi, Bluetooth, and ZigBee (SHORTRANGE, 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)

Aimed At

Professionals who are developing or implementing high-performance wireless systems will benefit from the detailed analysis of the Bluetooth BR, EDR, LE, and 802.11 AMP specifications, including range calculations, modulation and packet structures, and how Bluetooth devices find each other and establish a communication link among 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 five-day course undertakes a comprehensive description and analysis of Bluetooth wireless networking based on Bluetooth specification 4.0, which includes the alternate MAC/PHY (AMP) and low energy (LE) integration. Included are the Bluetooth basic rate (BR) and enhanced data rate (EDR) systems along with both LE and IEEE 802.11 AMP communication methods.

We will begin by studying Bluetooth signal propagation characteristics, modulation, packet structure, data and audio processing, and error control. Performance comparisons among BR, EDR, LE, and 802.11 AMP communication methods are made. 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 reason for studying Bluetooth so we can customize the course to your group’s needs. 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 channel access methods
- 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
- Explain how the link is managed and how user date is transported
- Understand the differences between BR, EDR, 802.11 AMP, and LE protocols
- Show how Bluetooth authentication and encryption operate
- 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

- Introduction
    - ◦ Differences between wired and wireless communications
    - ◦ Categories of information transmission
    - ◦ Overview of short range wireless networks
    - ◦ Bluetooth usage models and protocol stack
- 2.4 GHz Signal Propagation and Range Estimation
    - ◦ Review of decibels
    - ◦ Link budget equation and path loss model
    - ◦ Calculating maximum range
    - ◦ Partition attenuation and primary ray tracing
    - ◦ Eavesdropping vulnerabilities
    - ◦ Multipath characteristics and mitigation
- The Bluetooth Radio (BR/EDR and LE)
    - ◦ Frequency hopping spread spectrum operation
    - ◦ Bluetooth basic rate and enhanced data rate modulation

- ◦ Low energy technology modulation
- ◦ Channel set for BR/EDR and LE signals
- ◦ Required radio performance
- ◦ Performance analysis of a typical Bluetooth radio

Day Two

- The Bluetooth Radio (802.11 AMP)
  - ◦ Quadrature amplitude modulation
  - ◦ Orthogonal frequency division multiplexing operation
  - ◦ Direct sequence spread spectrum operation
  - ◦ Channel set for IEEE 802.11 signals
  - ◦ Operation of the IEEE 802.11a/b/g AMP radio
- Baseband Signaling Part 1 (BR/EDR)
  - ◦ Master/slave timing
  - ◦ Error control
  - ◦ Addressing methods
  - ◦ Packet structure
  - ◦ Setting frequency hop parameters
  - ◦ Logical transport mechanisms
  - ◦ Bluetooth audio
  - ◦ Throughput in perfect and imperfect channels
- Baseband Signaling Part 2 (BR/EDR)
  - ◦ Operational state diagram
  - ◦ Paging and inquiry processes
  - ◦ Sniff, hold, and park modes
  - ◦ Scatternet operation

Day Three

- Baseband Signaling Part 3 (LE)
  - ◦ Operational state diagram
  - ◦ Addressing
  - ◦ Packet structure
  - ◦ Operation of the advertising, initiating, and connecting devices
  - ◦ Data channel selection and packet exchange
  - ◦ Data channel control
- Baseband Signaling Part 4 (802.11 AMP)
  - ◦ Distributed coordination function and timing
  - ◦ 802.11 frame structure
  - ◦ Management, control, and data frames
  - ◦ 802.11 throughput
  - ◦ Operational state diagram

  - Service access points
  - Bluetooth 802.11 AMP protocol adaptation layer

- 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

Day Four

- Logical Link Control and Adaptation Protocol (L2CAP)
  - L2CAP overview and purpose
  - Packet segmentation and reassembly
  - Protocol multiplexing and channel definitions
  - L2CAP signaling and channel setup
- Host Controller Interface
  - HCI overview and purpose
  - Command packet structure
  - Command groups and examples
  - Event packet structure
  - Event groups and examples
  - HCI/USB interface
- Bluetooth Security
  - Security overview
  - Link key generation and initialization
  - Combination key derivation
  - Authentication
  - Encryption
  - Filtering device access
  - LE security mechanism
  - Overview of 802.11 robust security network (RSN)

Day Five

- Applications
  - Profile overview
  - Service discovery protocol
  - Generic access profile (GAP)
  - Headset profile (HSP)
  - Qualification and testing
  - Development tools
  - Hardware solutions

- Coexistence
  - Interference modeling
  - Bluetooth-on-Bluetooth interference
  - Coexisting with Wi-Fi: separated nodes
  - Coexisting with Wi-Fi: collocated nodes
  - Examples and throughput analysis
- Wrap-up
  - Course recap and Q/A
  - Evaluations

How You Will Learn

- A seasoned presenter well versed with Bluetooth and other short-range and wireless technologies will present this course in participative lecture format.
- Along with the lecture, we will use exercises to enrich the instruction and clarify the important points.
- If you already know something about Bluetooth, we will build on that knowledge base. We'll compare and contrast what you know with what's new, making the new ideas easier to learn.
- If your background is less technical, we will use examples and analogies to simplify the complex subject matter.
- You will receive a printed Participant Handbook which will help you remember and retain what you learned in class and apply it on your job.

Revised *March 18, 2010f*