

THE SECOND IEEE WORKSHOP ON Wireless Local Area Networks

IEEE 802.11 Wireless LAN

draft Standard

Keith B. Amundsen
Wireless Solutions
508-470-9483

keith_b_amundsen@raytheon.com

October 24, 1996

Worcester Polytechnic Institute

Introduction

- **IEEE 802.11 Draft 5.0 is a draft standard for Wireless Local Area Network (WLAN) communication.**
- **This tutorial is intended to describe the relationship between 802.11 and other LANs, and to describe some of the details of its operation.**
- **It is assumed that the audience is familiar with serial data communications, the use of LANs and has some knowledge of radios.**

Agenda

- **Glossary of 802.11 Wireless Terms**
- **Overview**
- **802.11 Media Access Control (MAC)**
- **Frequency Hopping and Direct Sequence Spread Spectrum Techniques**
- **802.11 Physical Layer (PHY)**
- **Security**
- **Performance**
- **Inter Access Point Protocol**
- **Implementation Support**
- **Raytheon Implementation**

Glossary of 802.11 Wireless Terms

- **Station (STA):** A computer or device with a wireless network interface.
- **Access Point (AP):** Device used to bridge the wireless-wired boundary, or to increase distance as a wireless packet repeater.
- **Ad Hoc Network:** A temporary one made up of stations in mutual range.
- **Infrastructure Network:** One with one or more Access Points.
- **Channel:** A radio frequency band, or Infrared, used for shared communication.
- **Basic Service Set (BSS):** A set of stations communicating wirelessly on the same channel in the same area, Ad Hoc or Infrastructure.
- **Extended Service Set (ESS):** A set BSSs and wired LANs with Access Points that appear as a single logical BSS.

Glossary of 802.11 Wireless Terms, cont.

- **BSSID & ESSID:** Data fields identifying a stations BSS & ESS.
- **Clear Channel Assessment (CCA):** A station function used to determine when it is OK to transmit.
- **Association:** A function that maps a station to an Access Point.
- **MAC Service Data Unit (MSDU):** Data Frame passed between user & MAC.
- **MAC Protocol Data Unit (MPDU):** Data Frame passed between MAC & PHY.
- **PLCP Packet (PLCP_PDU):** Data Packet passed from PHY to PHY over the Wireless Medium.

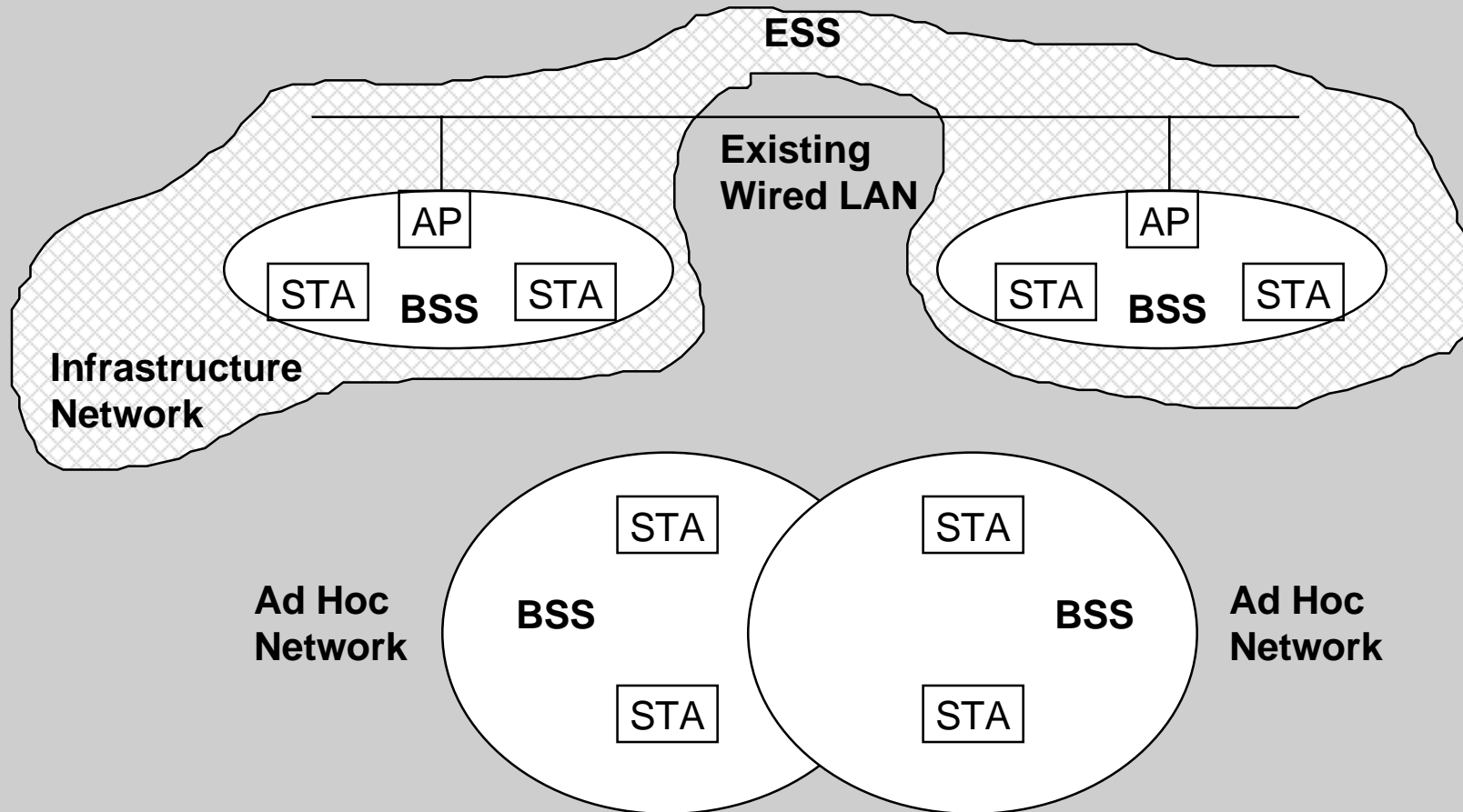
Overview, IEEE 802, and 802.11 Working Group

- **IEEE Project 802 charter:**
 - **Local & Metropolitan Area Networks**
 - **1Mb/s to 100Mb/s and higher**
 - **2 lower layers of 7 Layer OSI Reference Model**
- **IEEE 802.11 Working Group scope:**
 - **Wireless connectivity for fixed, portable and moving stations within a limited area**
 - **Appear to higher layers (LLC) the same as existing 802 standards**
 - **Transparent support of mobility (mobility across router ports is being address by a higher layer committee)**

Overview, IEEE 802.11 Committee

- **Committee formed in 1990**
 - **Wide attendance**
- **Multiple Physical Layers**
 - **Frequency Hopping Spread Spectrum**
 - **Direct Sequence Spread Spectrum**
 - **Infrared**
- **2.4GHz Industrial, Scientific & Medical shared unlicensed band**
 - **2.4 to 2.4835GHz with FCC transmitted power limits**
- **2Mb/s & 1Mb/s data transfer**
- **50 to 200 feet radius wireless coverage**
- **Draft 5.0 Letter Ballot passed and forwarded to Sponsor Ballot**
 - **Published Standard anticipated 1997**
- **Next 802.11 - November 11-14, Vancouver, BC**
 - **Chairman - Victor Hayes, v.hayes@ieee.org**

Overview, 802.11 Architecture



Overview, Wired vs. Wireless LANs

- **802.3 (Ethernet) uses CSMA/CD, Carrier Sense Multiple Access with 100% Collision Detect for reliable data transfer**
- **802.11 has CSMA/CA (Collision Avoidance)**
 - Large differences in signal strengths
 - Collisions can only be inferred afterward
 - Transmitters fail to get a response
 - Receivers see corrupted data through a CRC error

802.11 Media Access Control

- **Carrier Sense: Listen before talking**
- **Handshaking to infer collisions**
 - DATA-ACK packets
- **Collision Avoidance**
 - RTS-CTS-DATA-ACK to request the medium
 - Duration information in each packet
 - Random Backoff after collision is determined
 - Net Allocation Vector (NAV) to reserve bandwidth
 - Hidden Nodes use CTS duration information

802.11 Media Access Control, cont.

- **Fragmentation**
 - **Bit Error Rate (BER) goes up with distance and decreases the probability of successfully transmitting long frames**
 - **MSDUs given to MAC can be broken up into smaller MPDUs given to PHY, each with a sequence number for reassembly**
 - **Can increase range by allowing operation at higher BER**
 - **Lessens the impact of collisions**
 - **Trade overhead for overhead of RTS-CTS**
 - **Less impact from Hidden Nodes**

802.11 Media Access Control, cont

- **Beacons used convey network parameters such as hop sequence**
- **Probe Requests and Responses used to join a network**
- **Power Savings Mode**
 - **Frames stored at Access Point or Stations for sleeping Stations**
 - **Traffic Indication Map (TIM) in Frames alerts awaking Stations**

Frequency Hopping and Direct Sequence Spread Spectrum Techniques

- **Spread Spectrum used to avoid interference from licensed and other non-licensed users, and from noise, e.g., microwave ovens**
- **Frequency Hopping (FHSS)**
 - **Using one of 78 hop sequences, hop to a new 1MHz channel (out of the total of 79 channels) at least every 400milliseconds**
 - **Requires hop acquisition and synchronization**
 - **Hops away from interference**
- **Direct Sequence (DSSS)**
 - **Using one of 11 overlapping channels, multiply the data by an 11-bit number to spread the 1M-symbol/sec data over 11MHz**
 - **Requires RF linearity over 11MHz**
 - **Spreading yields processing gain at receiver**
 - **Less immune to interference**

802.11 Physical Layer

- **Preamble Sync, 16-bit Start Frame Delimiter, PLCP Header including 16-bit Header CRC, MPDU, 32-bit CRC**
- **FHSS**
 - **2 & 4GFSK**
 - **Data Whitening for Bias Suppression**
 - **32/33 bit stuffing and block inversion**
 - **7-bit LFSR scrambler**
 - **80-bit Preamble Sync pattern**
 - **32-bit Header**
- **DSSS**
 - **DBPSK & DQPSK**
 - **Data Scrambling using 8-bit LFSR**
 - **128-bit Preamble Sync pattern**
 - **48-bit Header**

802.11 Physical Layer, cont.

- **Antenna Diversity**
 - **Multipath fading a signal can inhibit reception**
 - **Multiple antennas can significantly minimize**
 - **Spacial Separation of Orthogonality**
 - **Choose Antenna during Preamble Sync pattern**
 - **Presence of Preamble Sync pattern**
 - **Presence of energy**
 - **RSSI - Received Signal Strength Indication**
 - **Combination of both**
- **Clear Channel Assessment**
 - **Require reliable indication that channel is in use to defer transmission**
 - **Use same mechanisms as for Antenna Diversity**
 - **Use NAV information**

Security

- **Authentication: A function that determines whether a Station is allowed to participate in network communication**
 - **Open System (null authentication) & Shared Key**
 - **WEP - Wired Equivalent Privacy**
 - **Encryption of data**
- **ESSID offers casual separation of traffic**

Performance, Theoretical Maximum Throughput

- Throughput numbers in Mbits/sec:
 - Assumes 100ms beacon interval, RTS, CTS used, no collision
 - Slide courtesy of Matt Fischer, AMD

	1 Mbit/sec		2 Mbit/sec	
MSDU size (bytes)	DS	FH (400ms hop time)	DS	FH (400ms hop time)
128	0.364	0.364	0.517	0.474
512	0.694	0.679	1.163	1.088
512 (frag size = 128)	0.503	0.512	0.781	0.759
2304	0.906	0.860	1.720	1.624

Inter Access Point Protocol

- **Not covered in draft standard**
- **Aironet & Lucent presented to 802.11 in July**
 - **Desired for secure environments**
 - **Desired for wireless infrastructure Distribution Systems that have no wired backbone**
- **Full discussion at 802.11 in November**

Implementation Support

- **Advanced Micro Devices Am79C930 PCnet™-Mobile Controller**
- **OKI Semiconductor MSM7712 Wireless LAN Controller**
- **Raytheon GaAs RF MMICs**

AMD Am79C930 PCnet™-Mobile

- **MAC Soft -> 80188 based architecture**
- **IEEE 802.11 MAC Firmware provided by AMD**
- **PHY independent**
 - **Programmable interface supports all PHY types**
- **Device Driver software available**
 - **NDIS3, NDIS2, ODI**
- **144 pin TQFP package**
- **PCMCIA & ISA Plug & Play interfaces**
- **5 & 3 volt functionality**
- **1 & 2 Mbit/sec data rates, with dynamic rate switching capability**
- **Evaluation software & HW available**
- **Cyrus Namazi: 408 749 3415**

OKI MSM7712 Wireless LAN Controller

- **Support for IEEE 802.11 draft standards**
- **Suitable for low-cost stations and access points**
- **PCMCIA compliant (v2.1) interface supporting 16-bit transfers**
- **On-chip radio modem for high-throughput data transfers**
- **Interface to radio providing antenna select, power control, and synthesizer programming**
- **Processor interface support for 80C86, 80C186, V33 & V53A**
- **Multi-port memory control for local simplified shared memory**
- **EEPROM interface to download configuration data and provide non-volatile card parameter storage**
- **Low-power mode for low power battery applications**
- **5V external and 3.3V core operation**
- **144-pin LQFP suitable for PCMCIA Type II cards**
- **Scott Gardner: 408-737-6357**

Raytheon GaAs RF MMICs

- **RMCS2410-10**
 - **2.4GHz Upconverter / Downconverter**
 - **28-pin flat pack**

- **RMMS2410-10**
 - **2.4GHz Power Amplifier**
 - **2.4GHz Low Noise Amplifier**
 - **28-pin flat pack**

Raytheon Implementation

- **PC Card (Station)**
 - **Custom ASIC**
 - **MAC**
 - **PCMCIA Interface**
 - **Radio Modem**
 - **Microprocessor**
 - **Memory**
 - **Dual Antenna**
- **Access Point**
 - **Microprocessor**
 - **Ethernet Interface**
 - **PCMCIA Interface**
 - **Memory**