Wi-Fi Hardware

Abdus Salam ICTP, February 2004

School on
Digital Radio Communications for Research and Training in Developing Countries

Ermanno Pietrosemoli
Latin American Networking School
(Fundación EsLaRed) – ULA
Mérida Venezuela www.eslared.org.ve

Wi-Fi Technology Overview
Agenda

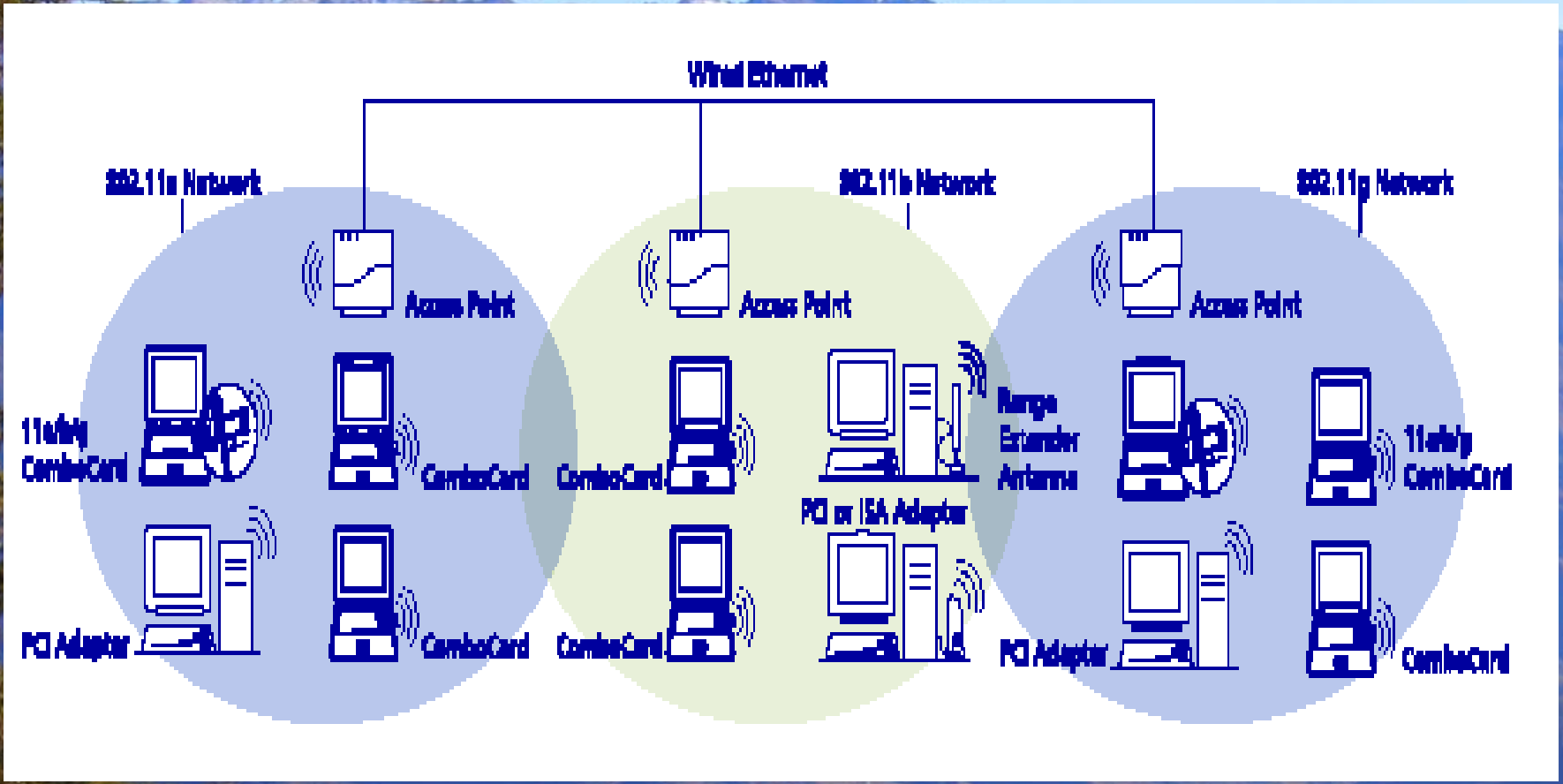
- Review
- 802.11 HW choices
- HW configuration
- Addenda to the Standards
- Software Tools

IEEE 802.11 Wireless LAN Standard

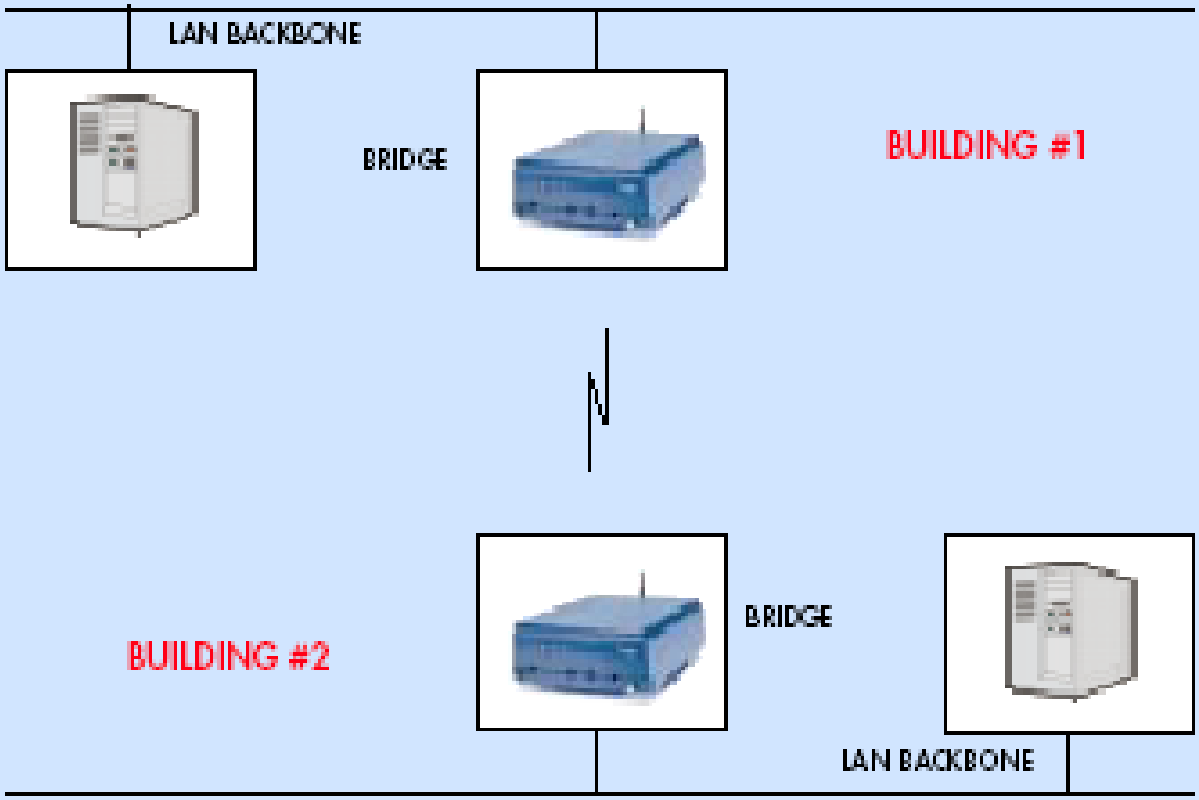
MAC Layer Basic Access Protocol Requirements.....

- Single MAC that supports multiple PHYs for both Ad-Hoc and Infrastructure Networks
- Supports Distributed Coordination Function (DCF) for efficient medium sharing without overlap restrictions.
  - **Uses CSMA with Collision Avoidance derivative (CSMA/CA)**
  - Based on *Carrier Sense* function in PHY called *Clear Channel Assessment* (CCA).
- Uses of RTS / CTS to provide a *Virtual Carrier Sense* function to protect against *Hidden Nodes*.
- Includes fragmentation to cope with different PHY characteristics.
- Supports Point Coordination Function (PCF) used for Time Bounded Services
- Supports Privacy and Access Control
  - WEP RC4 encryption alogorithm, by RSA Data Security
    - Uses a 64-bit key (40-bit seed, 24-bit Initialization vector)

General Layout



WIRELESS BRIDGING

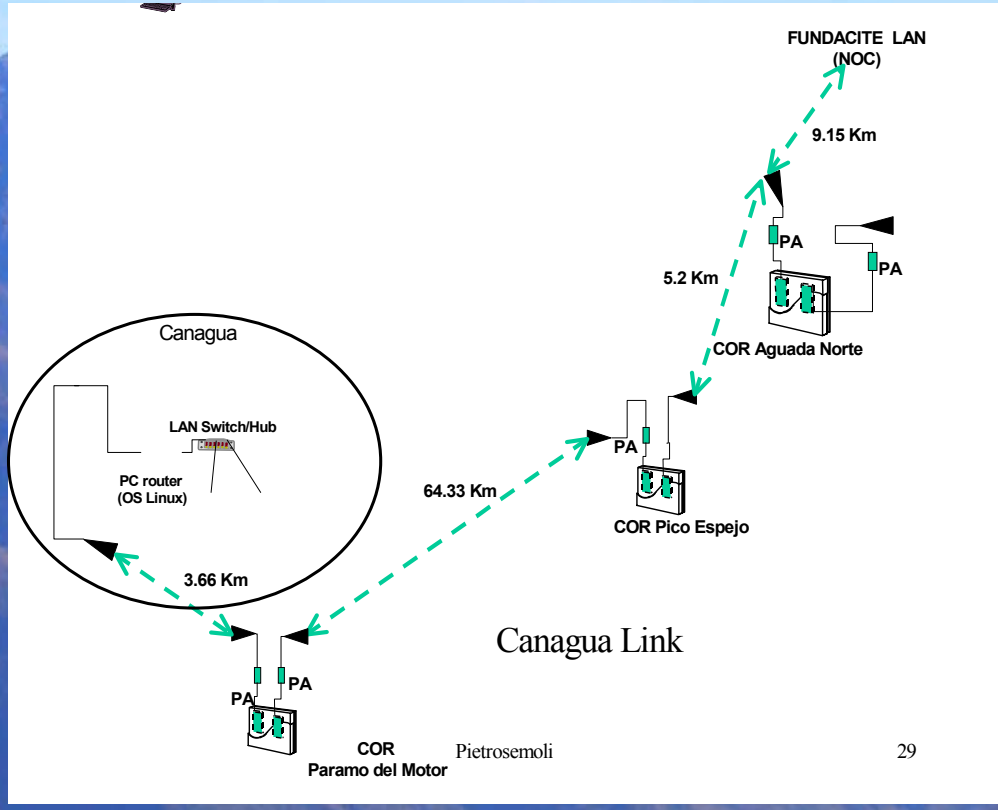


POINT-TO-POINT WIRELESS BRIDGE

What it's available

Commercial Products:

- Access points
- Residential Gateways
- Enterprises Gateways
- Bridges

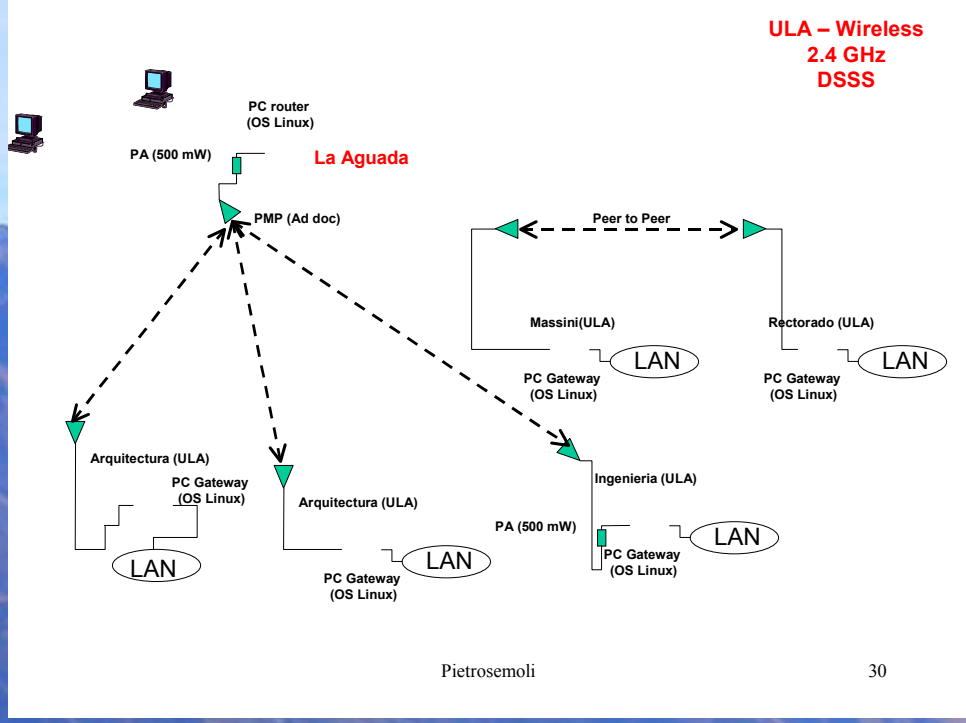


- COR Central Outdoor Router
- ROR Remote Outdoor Router

What it's available

DIY:

Linux Box with wireless card



- Maximum flexibility: Bridge, Router, Firewall, Nat, DHCP
- Potential cost saving if recycling PCs
- Reliability concern
- Drivers Available for most cards
- Standalone low power PCs available
- Easy implementation of Mesh topology
- Complexity of install and maintenance

Hardware List

- Antenna
- Antenna Cable and Connectors
- Lightning Arrestor
- Pigtail
- Wireless Card + bus adapter
- Access Point?
- Amplifier?

Wireless LAN Client Devices

The term "client devices" will, for purposes of this discussion, cover several wireless LAN devices that an access point recognizes as a client on a network. These devices include:

- PCMCIA & Compact Flash Cards
- Ethernet & Serial Converters
- USB Adapters
- PCI & ISA Adapters

Client Devices

A sample Ethernet and serial converter

Client Devices

Wireless Flash Combo (128MB)

Portable Wireless 802.11b USB Storage Device
Dimension: 93 x 30 x 15 mm (L x W x H
Weight: 30 g $110 www.soyousa.com

http://www.netgear.com/

- 802.11b / 2.4GHz
- 802.11g / 2.4GHz
- 108Mbps

DWL-AB520

- 802.11a and 802.11b Compatible
- Dual-Band Access for Network Investment Protection
- Supports Advanced Encryption Security (AES)

ATHEROS DRIVEN™

Wi Fi™
The Standard for Wireless Fidelity.

AirPro Wireless Network

Multimode 2.4/5GHz Wireless

PCI Adapter

11a/b
802.11a & 802.11b

SPECIFICATIONS

Standards
- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.1x

Local Bus Architecture
- PCI 2.2 Compliant
- PCI 32-bit Interface

OS Supported
- Windows 98SE
- Windows Me
- Windows 2000
- Windows XP

Frequency Range

802.11a
- 5.150 - 5.350GHz & 5.725 - 5.825GHz (U.S. & Canada)

802.11b
- 2400 - 2.497GHz

Data Rates

802.11a
- 6, 9, 12, 18, 24, 36, 48, 54 Mbps

802.11b
- 1, 2, 5.5, 11 Mbps

Encryption
- Advanced Encryption Security (AES)
- 64/128/152-bit WEP (Wired Equivalent Privacy)

Radio & Modulation Technology

802.11a
- OFDM (Orthogonal Frequency Division Multiplexing)

802.11b
- DSSS (Direct Sequence Spread Spectrum)

Media Access Control
- CSMA/CA with ACK

Antenna Type
- Omni-Directional Dipole Antenna with 2 ~ 4dBi Gain

Transmit Power
- 802.11a - 13-14 dBm (54Mbps)
- 802.11b - 18 dBm (11Mbps)

Receiver Sensitivity
- 802.11a - 66 dBm (54Mbps)
- 802.11b - 84 dBm (11Mbps)

Operating Voltage
- 3.3VDC ± -10%

Environmental Requirements
- Operating Temperature 32˚ to 131˚F (0˚ to 55˚C)
- Non-Operating Humidity 5% to 95% Non-Condensing
- Operating Humidity 10% to 90% Non-Condensing
- Storage Temperature -4˚ to 167˚F (-20˚ to 75˚C)

Emissions Compliance
- FCC Part 15b

Physical Dimensions
- L = 6.6 Inches (168 mm)
- W = 4.2 Inches (107 mm)
- H = .16 Inches (4 mm)

Warranty
- Three Years

http://www.hyperlinktech.com

http://www.proxim.com/products/wifi/

- 

Configuration and Management

There are two steps to installing wireless LAN client devices:

1. Install the drivers
2. Install manufacturer's wireless utilities

Configuration Parameters

Avaya Wireless PC-Card used in client station and AP-1000 or AP-500

- "Behaves" differently based on the parent unit
  - When inserted in AP-1000 or AP-500, AP firmware is downloaded into the PC-Card (Note: this is Avaya Wireless/MAC FW, not "Bridge FW")
  - When inserted in client station, STA firmware is active (default FW)
- Requires different configuration parameter sets to support the different behavior
- Configuration can be performed by:
  - Setting parameters at installation
  - Changing parameters in property settings
  - Using Avaya Wireless AP Manager (for APs)

Configuration Parameters
Basic parameters (Station)

Network Name (SSID)

- ASCII string to identify the network that the station wants to connect to (similar to Domain-ID in WLAN pre-IEEE)

Station Name (SSID)

- ASCII string to provide a user friendly station identification, when used in diagnostic purposes (in Windows systems: equal to “computer name”)

Type of Operation

- To identify the kind of network that the station will be part of
  - Network centered around APs (or RG-1000)

Configuration Parameters
Advanced parameters (Station)

MAC Address

- Physical address of the card:
  - Universal; factory installed (default)
  - Local; user-defined (6 Hexadecimal characters)

Distance between APs

- To specify the coverage of a “cell” in terms of the distance between the Access-Points
  - Large
  - Medium
  - Small

Configuration Parameters
Advanced parameters (Station)

Microwave Oven Robustness

- Check box to enable/disable data-rate fallback delay-mechanism to allow improved performance in presence of microwave ovens

RTS/CTS Medium Reservation

- Check box to enable/disable the RTS/CTS handshake.

Card Power Management

- Check box to enable/disable Power Management

Configuration Parameters
Encryption parameters (Station)

Enable Encryption

- To enable/disable Encryption

Encryption keys

- Four fields to store up to four different encryption keys
- Entries take up to 5 ASCII or 10 hexa-decimal values (when using 64 WEP)

Encryption key index

- Index identifying which of the four keys is the active one

Configuration Parameters
Basic parameters (AP-500/1000)

Network Name (SSID)

- ASCII string to identify the network that the Access-Point is part of (similar to Domain-ID in WaveLAN pre-IEEE). Only available in “Access Point” mode.

Frequency (channel)

- To indicate the frequency channel that the AP-500/1000 will use for its “cell”. The channel is selected from the set that is allowed in the regulatory domain.

Addenda to the basic 802.11 protocol

- 802.11 a, b, g
  enhanced speed and multipath performance
- 802.11 e Quality of Service
- 802.11 d Additional regulatory domains
- 802.11 h Spectrum Managed 802.11a
- 802.11 I Security
- 802.1 x Authentication

Task Group H: Spectrum Managed 802.11a

802.11 radios transmit and without getting appropriate feedback, halt and retransmit.

802.11h overlays 802.11a to solve both interference and overuse problems, as well as improve coexistence with other specs that might reside on the same band. The h spec requires devices to check whether given frequencies are in use before transmitting (Dynamic Frequency Selection or DFS), as well as only transmitting at the minimum necessary power level (Transmit Power Control or TPC).

Task Group H: Spectrum Managed 802.11a

These additions were formulated specifically to meet requirements for using the 5 GHz band in the European Union, which has been promoting its own specification called HiperLAN2

There's a chance for spillover of h into other standards like b and g, of course, to improve their responsiveness

Task Group E: Quality of Service

- Every packet has an equal chance of getting through in 802.11b. Task Group E wants to change that, allowing for what's known as "quality of service" or QoS, to guarantee that some packets have more priority than others. This is a fairly tricky task, involving coordination between client radios, access points, and system administrators.
- QoS is needed for consistent voice-quality calls using VOIP (voice over IP) and for streaming multimedia.

Task Group 802.1x

Is developing a method of authenticating users through a back-end system in a secure fashion. Some weaknesses in the approach have already been discovered, unfortunately, as there is a lot of room for man-in-the-middle style interception

Wireless LAN Analysis- tools

- AiroPeek *from WildPackets*
- Grasshopper *from BV Systems*
- Mobile Manager *from Wavelink*
- Sniffer Wireless *from Network Associates*
- NetStumbler
- AirSnort *via the SourceForge*
  - AirSnort has been designed to break WEP encryption keys.
  - It operates by passively monitoring transmissions, and when enough “interesting” packets have been gathered, usually over a 24 hour period, it can then calculate the WEP key.

.

Questions?