WLAN

802.11a-z

In this chapter we discuss basic communication issues, such as synchronization, coding, scrambling, modulation, and so on.

Wireless Products

- WLAN is *integrated*
  - E. g. Intel Centrino chipsets
- Increasing data rates
  - Towards Fast Ethernet speeds and more
- Today strong native security solutions available
  - IPsec/TLS grade
- VoIP support
  - QoS solutions available
- Ongoing penetration in consumer market
  - TV/Radio-links, Wireless HiFi, various gadgets, …

The first widespread commercial use of the 802.11b standard for networking was made by Apple Computer under the trademark AirPort. On the non-Apple market, Linksys could be considered the current leader.

A Very First Introduction (1)

- Basic standards:
  - 802.11a, 802.11b, 802.11g, 802.11n
- Frequencies used
  - ISM 2.4 GHz (mostly used; 3-4 usable channels)
  - ISM 5 GHz (more channels; depends on country)
- Strange terms
  - The client station is often called the "STA"
    - This convention is NOT used in this chapters; we prefer the universal term "client"
  - Outdoor Device Unit (ODU)
    - Can be used outdoors (weatherproof)
- Access Points (APs) manage traffic from, to, and between clients
  - The radio cell is a shared collision network
  - EVERY traffic must go over the AP – there is no direct inter-client traffic possible (clients would refuse that)

A Very First Introduction (2)

- The wireless network name (cell name) is called Service Set Identifier (SSID)
  - Basic-SSID (SSID for a single cell)
  - Extended-SSID (same SSID spans over multiple cells)
- Typical security used:
  - WiFi Protected Access (WPA)
- Typical QoS used:
  - WiFi Multi Media (WMM)
- Typical distances possible
  - Strongly depends on antennas
  - 20-50 meters indoor
  - Up to 15 km outdoor (much more possible with some efforts)
- Typical cell throughput possible
  - 802.11b => 5-6 Mbit/s
  - 802.11a|g => up to 22|25 Mbit/s
  - 802.11n => probably 300-400 Mbit/s (will be ratified end 2006)

Evolution of the 802.11 Standards

- 1980s: Early developments - 215, 344, 860 kbit/s @ 900 MHz
- 1997: 802.1y aka 802.11
  - 1 or 2 Mbit/s, FHSS or DSSS
  - 902-928 MHz, problems with EU & Asia
- 1999: 802.11b
  - 1, 2, 5.5, 11 Mbit/s, only DSSS
  - ISM 2,4000-2,4835 GHz, nearly world-wide available
  - USA: 11 channels, Europe 13, Japan 14
  - 3 non-overlapping (1,6,11 with 22 MHz per channel)
- 1999: 802.11a (*shipped* in 2001)
  - 6,9,12,18,24,36,48,54 Mbit/s, OFDM
  - 5.150-5.350 GHz, 8-12(-24) non-overlapping channels
  - 20 MHz per channel
- 2003: 802.11g
  - 1,2,5.5,11,12,18,24,36,48,54, DSSS and OFDM
  - ISM 2,4 GHz => same channels as 802.11b
- 2004: 802.11i (Security)
  - AES-CCM + 802.1x (TKIP/MIC only as migrating solution)
- 2006: 802.11n
  - Up to 600 Mbit/s via MIMO-OFDM
  - Optimized MAC for higher throughput

Germany: "From 13 November 2002, frequencies in the bands 5150 MHz - 5350 MHz and 5470 MHz - 5725 MHz may be used for Wireless Local Area Networks free of charge. The Regulatory Authority for Telecommunications and Posts (RegTP) published a general assignment of these frequencies in its Official Gazette of 13 November 2002."

802.11 begann in dem 902-928 MHz Frequenzbereich. Jedoch wurde, soweit ich weiß, kein Standard jemals für diesen Bereich fertiggestellt. 900 Mhz Band ist nämlich nur in Amerika (Nord und Süd), sowie in Australien frei. Europa, Asien, Afrika ist dieser Bereich nicht frei. Deshalb hat sich auch ziemlich schnell die Entwicklung in das 2,4 Ghz Band verschoben (dieses ist absulut überall linzenz frei).

Infrared (900 nm), diffuse light versus directional light. Widely used in mobile phones, Laptops. IrDA 2000 Standard. Transfer rate only 4 Mbit/s (directional). Easy screening.

IEEE WLAN Standards Overview

802.11a – 5 GHz- Ratified in 1999 (shipping 2001)
802.11b – 11Mbit/s 2.4GHz, ratified in 1999
802.11c – MAC-layer bridging (802.1d)
802.11d – Additional regulatory domains (world mode)
802.11e – Quality of Service
802.11f – Inter-Access Point Protocol (IAPP)
802.11g – Higher Datarate (>20MBit/s, actually 54 MBit/s) 2.4GHz
802.11h – 54 Mbit/s at 5GHz using DFS and TPC (Europe)
802.11i – Authentication and security
802.11j – Japan regulatory conformance
802.11k – Radio Resource Management (Signal Quality, 2004)
802.11m – Various 802.11 improvements (bugfixes)
802.11n – Beyond 100 Mbit/s, longer distances (2004)
802.11p – Wireless Access for the Vehicular Environment (WAVE)
802.11r – Fast roaming
802.11s – Mesh networks
802.11T – Wireless Performance Prediction (WPP), test methods and metrics
802.11u – Interoperability with non-802 networks (e.g. cellular)
802.11v – WLAN Management

802.11a can communicate at a maximum rate of 72Mbps but due to FCC frequency restrictions, it is currently limited to 54Mbps. If these regulations change, a simple firmware upgrade will update your equipment.

There are two consortiums for 802.11n: WWiSE and TGnSYNC.

802.11p (WAVE) is meant for "vehicular environments" such as ambulances and passenger cars.

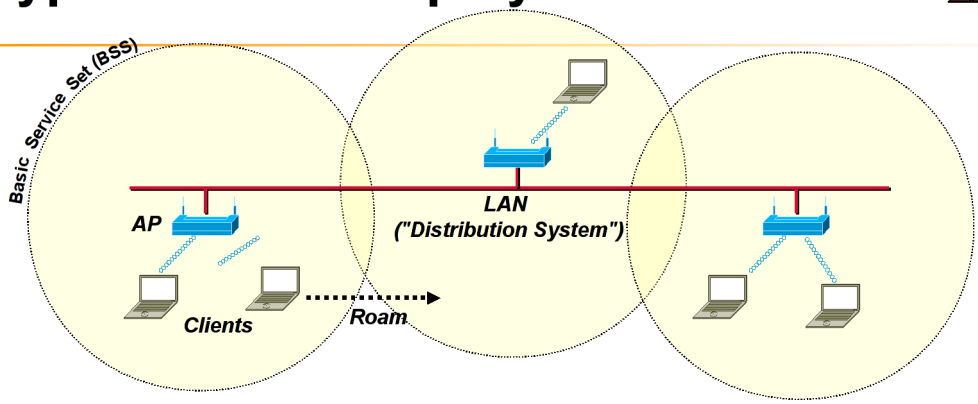
For 802.11n news, see
http://grouper.ieee.org/groups/802/11/Reports/tgn_update.htm

Wireless Fidelity Alliance

- Wi-Fi Alliance (1999)
  - Certifies interoperability of IEEE 802.11 products and promotes them as the global, wireless LAN standard across all market segments
  - Formely known as Wireless Ethernet Compatibility Alliance (WECA)
- Certified substandards
  - 802.11i => Wi-Fi Protected Access (WPA)
  - 802.11e => Wireless Multimedia (WMM)

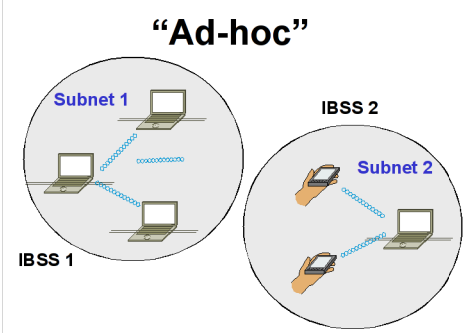
www.wi-fi.com

Typical WLAN Deployment

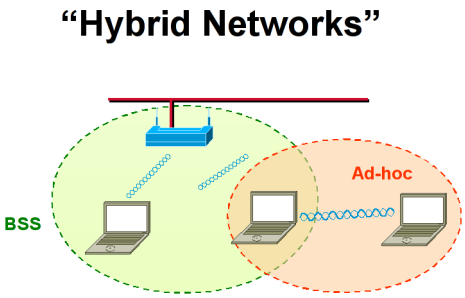


- "Extended Service Set (ESS)"
  - Multiple radio cells (aka Basic Service Sets (BSS)) are interconnected by an Ethernet Switch ("Distribution System")
- Routed connections to other networks possible
- Every wireless traffic runs over an AP !!!
  - No direct communication between clients possible (clients would refuse that)
- AP provides security and QoS features
  - As well as client-to-VLAN membership etc

Other WLAN Network Types



- No infrastructure or AP available
  - End users communicate directly with each other
    - => Smaller total coverage
  - Also send beacons to sync their communication
- End devices can be more complex if mesh-routing required
  - Important current issue!
- Typically no security concepts
  - Therefore not recommended



- Rarely supported
- Critical security problem
  - Member of BSS who also allows IBSS could potentially provide unwanted access to wired network
  - Admin has no full access control anymore

(C) Herbert Haas 2010/02/15 9

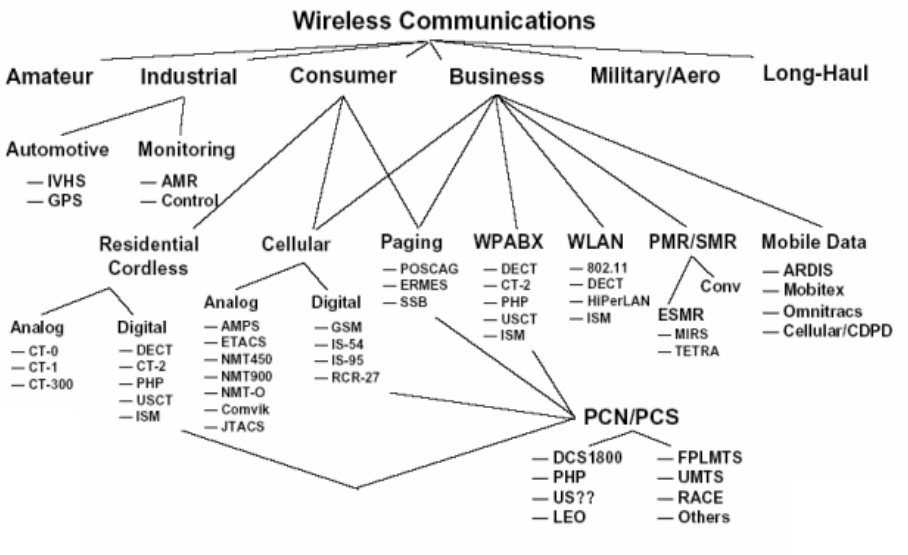
Ad hoc networks or Independent Basic Service Set (IBSS): Stations communicate peer-to-peer. Infrastructure Mode uses Access Points (AP). AP bridges wireless and wired networks. Stations communicate via AP only, Shared device - like hub! All station clocks within a BSS are synchronized by periodic transmission of time stamped beacons.

In the infrastructure mode, the AP serves as the timing master and generates all timing beacons. Synchronization is maintained to within 4 microseconds plus propagation delay. Timing beacons also play an important role in power management. There are two power saving modes defined: awake and doze. In the awake mode, stations are fully powered and can receive packets at any time. Nodes must inform the AP before entering doze. In this mode, nodes must "wake up" periodically to listen for beacons which indicate that AP has queued messages.

Some Acronyms:

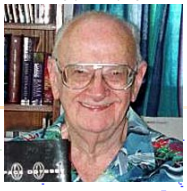
AP	…Access Point
BS	…Base Station (=AP)
BSS	…Basic Service Set (1 AP)
IBSS	…Independent Basic Service Set
ESS	…Extended Service Set (multiple APs)
QBSS	…QoS BSS (802.11e)
DS	…Distribution System
SSID	…Service Set Identifier

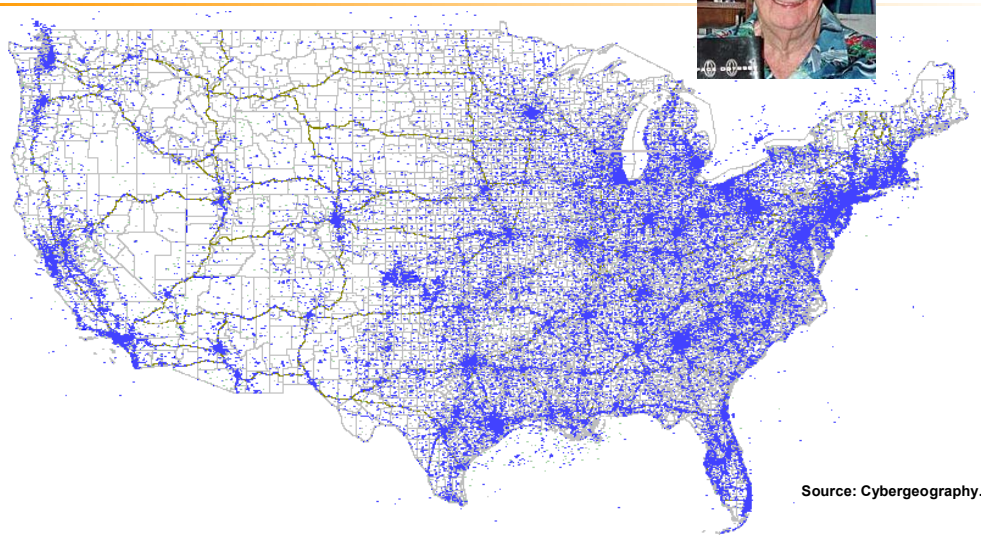
Wireless Overview



"I've suggested, half seriously, that the next step is direct mental input – the 'brain cap,' which you put on your head and then the impressions, sights, everything, go directly into the brain. I'm afraid this may turn us all into permanent 'couch potatoes' because we then need not travel anywhere. We can experience anything, learn anything...just lying on the couch."

Arthur C. Clarke





Source: Cybergeography.org

A simple dot map of commercial wireless antennas in the USA (Note: This was even in 2002!)

This juvenescent guy above is… Arthur C. Clarke, right. Author of "2001 – A Space Odyssey" (and lots of other good science fiction novels), first promoter of the geostationary orbit, and much else. Lives in Sri Lanka.