KUNGL TEKNISKA HÖGSKOLAN

Institutionen för mikroelektronik och informationsteknik

# 2G1330 Mobile and Wireless Network Architectures

## WLAN

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Last modified: 2002.03.18:00:11

# Lecture 9 &10

- Wireless Local Area Networks (WLANs)

IEEE 802.11 Medium Access Control (MAC) protocol uses Carrier sense multiple access (CSMA) with collision avoidance (CA) medium access scheme.

Several variants:

| | |
|---|---|
| **IEEE 802.11b** | 1, 2, 5.5 and 11 Mbps - DS-SS<br>Wireless Ethernet Compatibility Alliance certifies its members' equipment as conforming to the 802.11b standard. Compliant hardware is stamped **Wi-Fi (Wireless Fidelity)** compatible; operates in 2.4GHz band |
| **IEEE 802.11g** | enable data transmission speeds of up to 54 Mbps, with backwards compatibility to 802.11b infrastructure; operates in 2.4GHz band |
| **IEEE 802.11a** | using OFDM (Orthogonal Frequency Division Multiplexing) achieves upto 54 Mbps - currently **not** approved for use in Sweden; operates in 5 GHz band |
| **IEEE 802.11h** | designed to adapt 802.11a to the european HiperLAN/2 requirements; operates in 5 GHz band |

# Two possible network configurations

**Independent configuration** Mobile stations communicate directly to each other with no access point (base station) support, i.e., peer-to-peer (**ad hoc**) networking

**Infrastructure configuration** Mobile stations communicate only via access points (APs)

# Terms

**Basic Service Set (BSS) -** a group of stations that are under the direct control of a single coordination function (PCF or DCF)

**Independent BSS (IBSS) -** also known as an adhoc network, defined as a BSS which exist without an access point (AP)

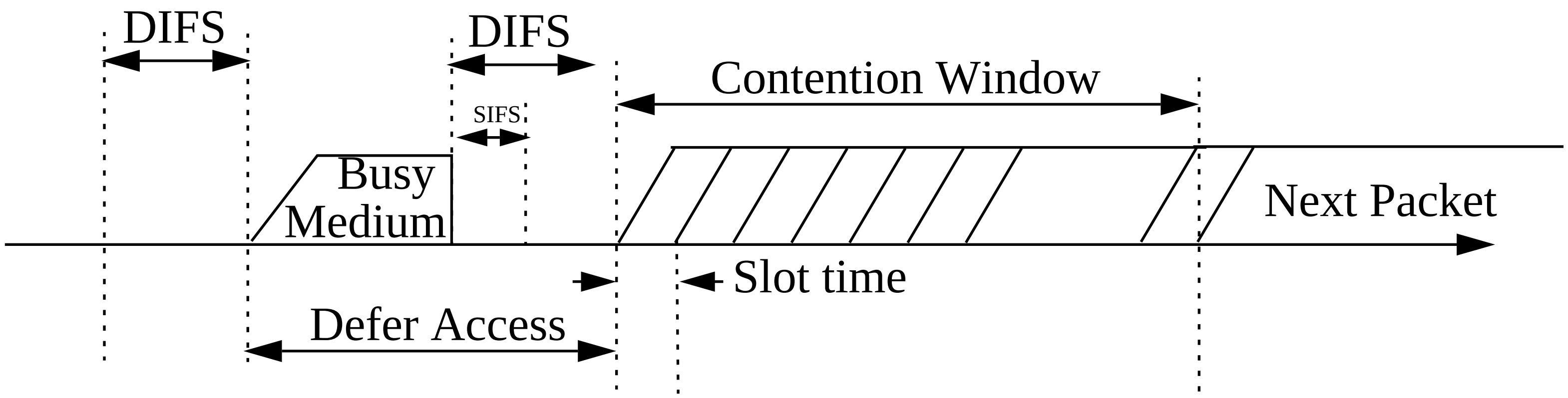
**Infrastructure network -** a network of wireless stations along with APs, which enables stations in one BSS to communicate with stations in another BSS

**Distribution System (DS) -** a backbone network between the two or more access points

**Extended Service Set (ESS)** a series of overlapping BSSs (each with its own AP) connected together by means of a Distribution System (DS)

**Hidden node -** a node is said to be hidden when its transmissions cannot be heard by some other node in the network (although it can be heard be one or more other nodes)

# IEEE 802.11 Basic Access Method



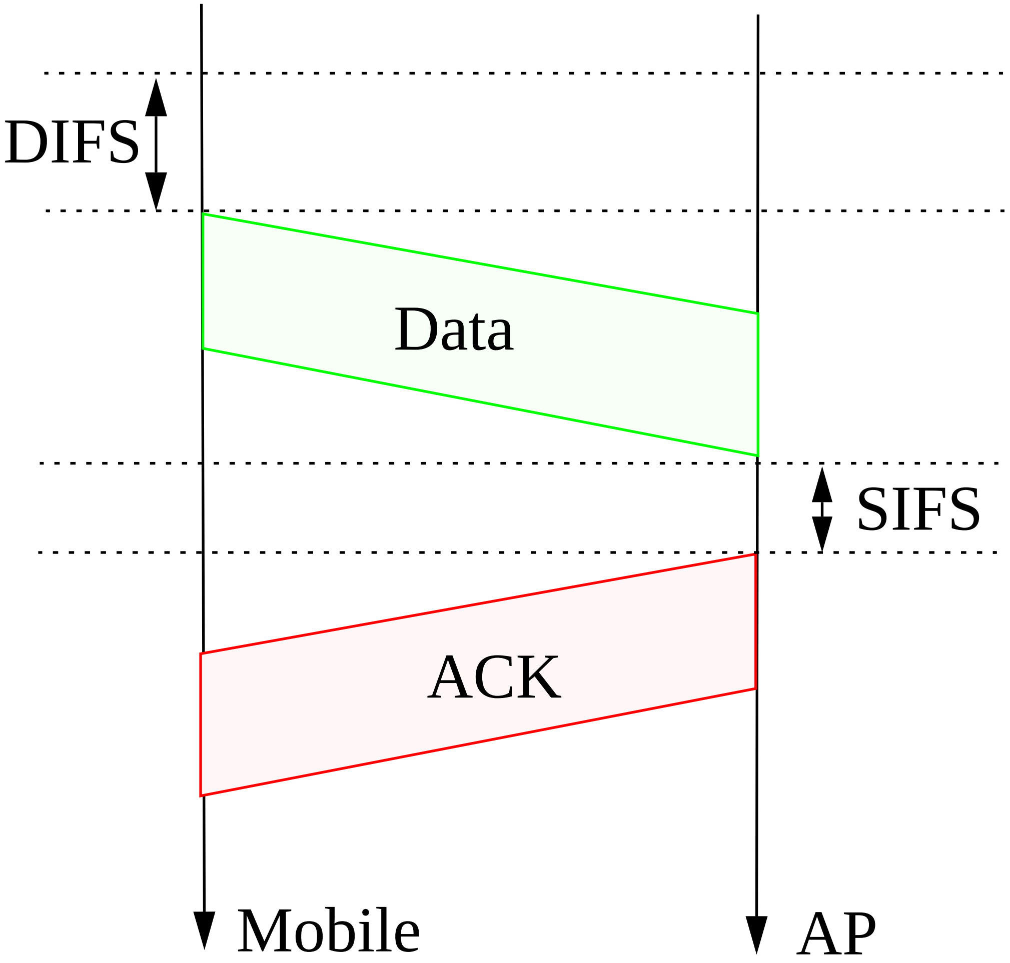
| | |
|---|---|
| IFS | Inter Frame spacing - during this time the medium is idle |
| SIFS | Short IFS - transmission after SIFS is reserved for ACKs, Clear To Send frame, or to send a fragmented MAC protocol data unit (MPDU) |
| DIFS | if after DCF-IFS (DIFS) a station finds the media free it can transmit a pending packet;<br>otherwise it sets a backoff timer after selecting a random backoff value (BV) {selected from a uniform distribution over [0 .. CW-1], where CW is the width of the contention window in slots}<br>if medium become busy before time goes off, then the value is frozen until the next DIFS interval, where upon it continues the count down<br>CW is doubled after collisions and reset to $CW_{min}$ after a successful transmission |
| EIFS | Extended IFS - used when the receiver can’t correct the received packet |

# Distribution Coordinating Function (DCF)

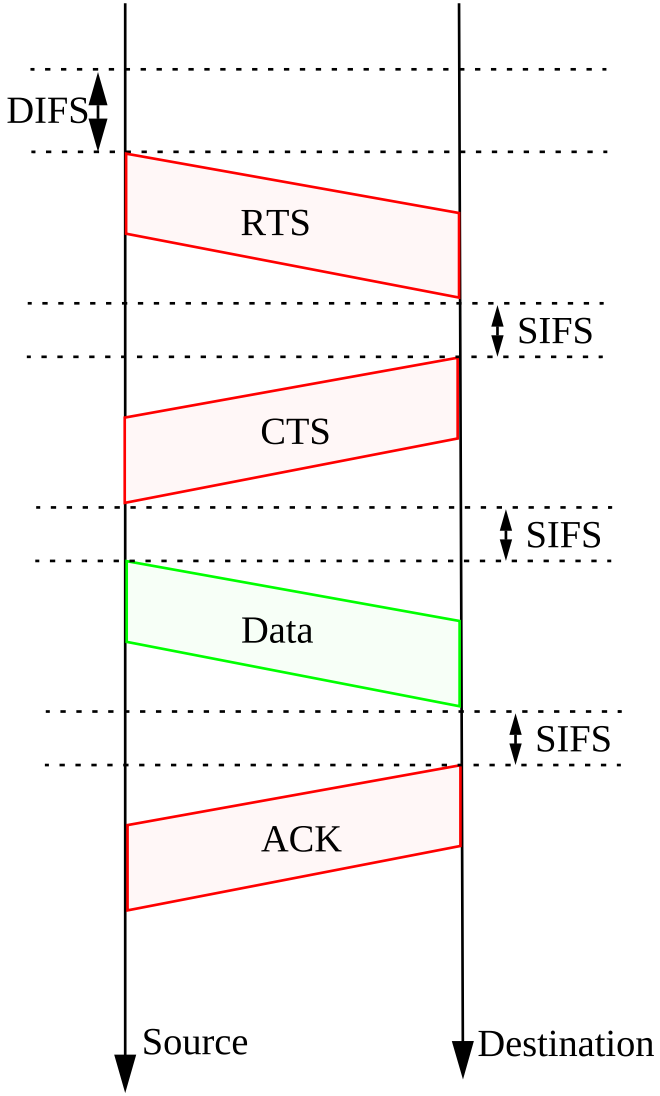
Distribution Coordinating Function (DCF) is based on carrier sense multiple access with collision avoidance (CSMA/CA)

Receivers send an ACK if they successfully receive a packet, otherwise the transmitter resends.

# CSMA/CA with ACK in infrastructure network



# IEEE 802.11 RTS/CTS mechanism



# IEEE 802.11 Frame Format

| | |
|---|---|
| Frame Control | 2 bytes |
| Duration/ID | 2 bytes |
| Address 1 | 6 bytes |
| Address 2 | 6 bytes |
| Address 3 | 6 bytes |
| Sequence Control | 2 bytes |
| Address 4 | 6 bytes |
| Frame Body | 0 .. 2312 bytes |
| CRC | 4 bytes |

# IEEE 802.11 Frame Control

<table>
<tr><td>B0</td><td>B1</td><td>B2</td><td>B3</td><td>B4</td><td>B5</td><td>B6</td><td>B7</td><td>B8</td><td>B9</td><td>B10</td><td>B11</td><td>B12</td><td>B13</td><td>B14</td><td>B15</td></tr>
<tr><td colspan="2">Protocol Version</td><td colspan="2">Type</td><td colspan="4">Subtype</td><td>To DS</td><td>From DS</td><td>More Frag</td><td>Retry</td><td>PwrMgt</td><td>More data</td><td>WEP</td><td>RSVD</td></tr>
<tr><td colspan="2">2</td><td colspan="2">2</td><td colspan="4">4</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
</table>

| | |
|---|---|
| Protocol Version | currently 00, other values reserved |
| To DS/From DS | 1 for communcation between two APs |
| More Fragments | 1 if another fragment follows |
| Retry | 1 if packet is a retransmission |
| Power Management | 1 if station is in sleep mode |
| More date | 1 if there are more packets to the terminal in power-save mode |
| WEP | 1 if data bits are encrypted |

# Startup, then Join a network

- Turn on & discovery phase
  - determine AP or other stations exist
  - get SSID and other parameters
- Negotiate for connection
  - Authentication & Association

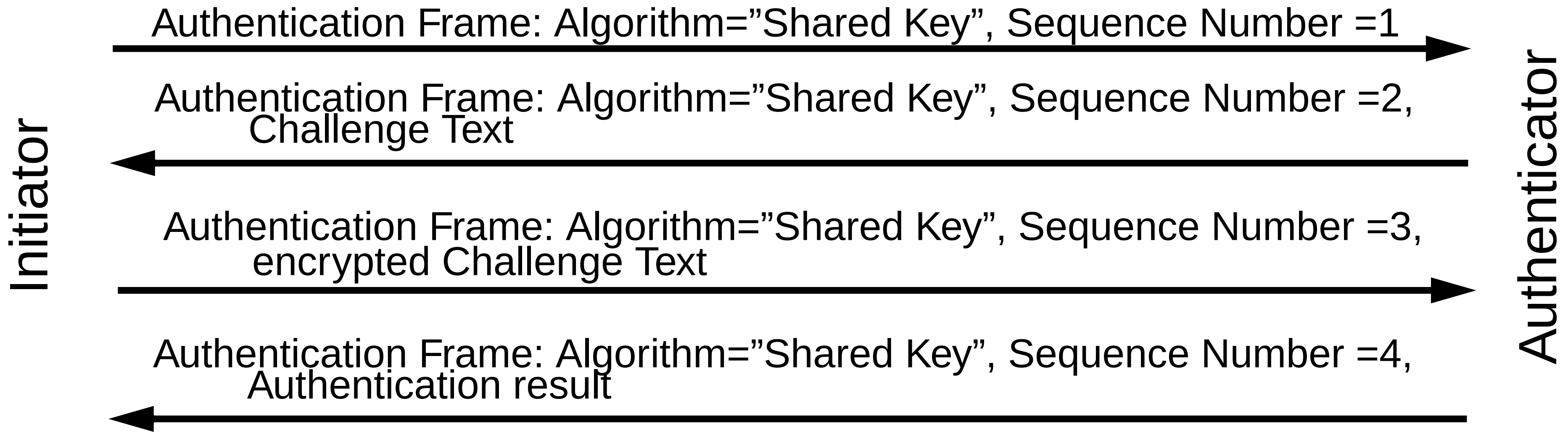
# Discovery Phase

Enter scanning mode: Passive / Active scanning mode

- Passive
  - Listen for a Beacon for ChannelTime period
  - From Beacon get the SSID & parameters
- Active
  - Transmit a probe frame (including the SSID that you wish to join)
  - Wait for a period for responds by AP or other stations

# Authentication

- Open system authentication
  - **Default** mode
  - Flow:
    - send: Authentication Frame: Algorithm=”Open”, Sequence Number =1
    - response: Authentication Frame: Algorithm=”Open”, Sequence Number =2, result=accept/reject
- Shared key authentication
  - Somewhat higher degree of security
  - Need to implement WEP
  - Flow:



Authentication Frame: Algorithm=”Shared Key”, Sequence Number =1

Authentication Frame: Algorithm=”Shared Key”, Sequence Number =2, Challenge Text

Authentication Frame: Algorithm=”Shared Key”, Sequence Number =3, encrypted Challenge Text

Authentication Frame: Algorithm=”Shared Key”, Sequence Number =4, Authentication result

# Wire Equivalent Privacy (WEP)

IEEE 802.11 featured **Wire Equivalent Privacy (WEP)** - this proved to be rather insecure; there are efforts to fix it - but meanwhile or in any case one can use VPNs.

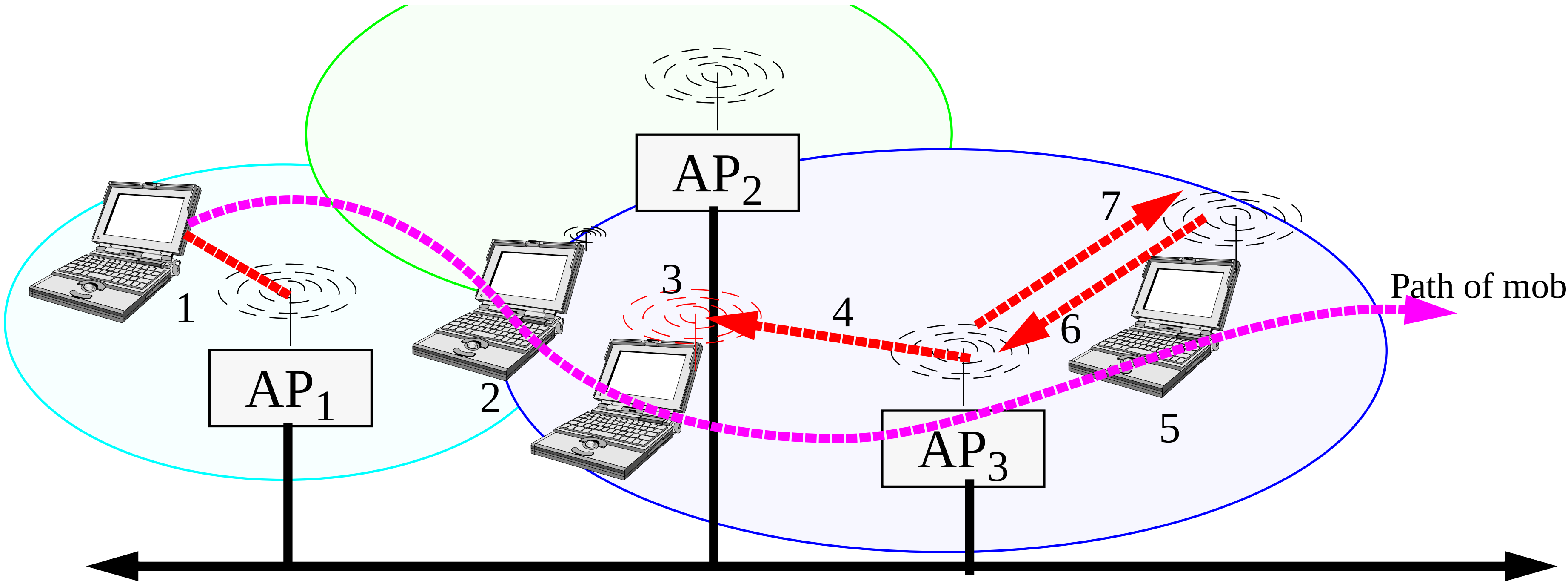
WEP use for data encryption & shared key authentication

- Encryption of data through RSA RC4 algorithm
- 40-bit secret key + 24-bits Initialization Vector (IV)
- IV in frame in clear text
- Integrity Check Value (ICV) included in frame
- When WEP is enabled, Shared Key Authentication is enabled

Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”, AT&T Labs Technical Report TD-4ZCPZZ, Revision 2, August 21, 2001 *http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf*

see also *http://www.cs.umd.edu/~waa/wireless.html*

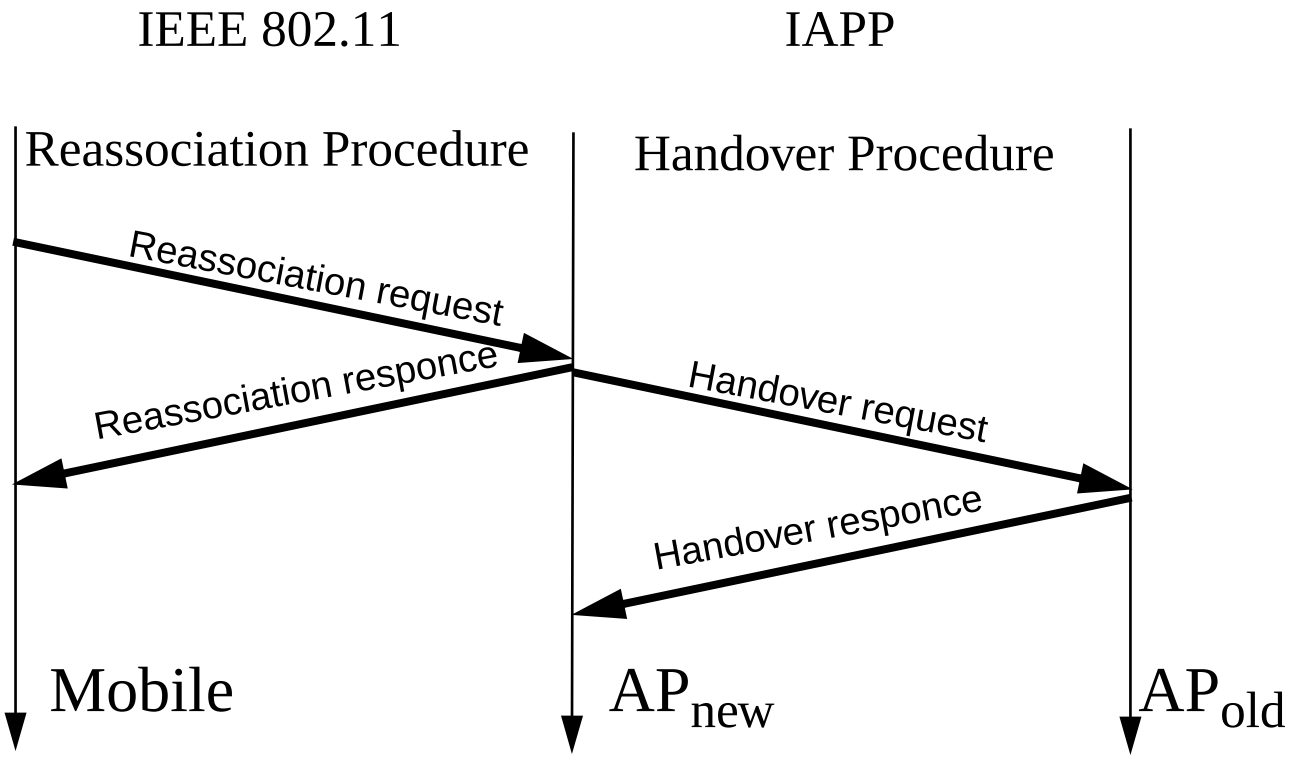
# Handoff



1. Mobile starts with a strong signal from AP$_1$
2. The signal from AP$_1$ is now weaker, so mobile starts to look around for a better AP
3. Mobile sends a Probe Request
4. AP$_3$ send probe response
5. Mobile chooses AP$_3$ as the best AP
6. Mobile sends Reassociation request
7. AP3 sends a Reassociation Response

# Inter-Access Point Protocol (IAPP)

Project 802.11f: IAPP Inter Access Point Protocol



# Fast Handoff

- 802.11 being used in PDAs, WLAN phones, lots of new devices (especially for multimedia)
  - Multimedia applications sensitive to connectivity loss (when the loss of data exceeds that which the playout buffers can cover up)
  - TCP sensitive to multiple losses
    - Loss of an entire window causes connection to go into slow-start
- basic handoff is fast and simple, but insecure
  - Authentication occurs prior to reassociation so pre-authentication is possible
  - Management frames are not authenticated, thus no cryptographic operations in critical path
  - If APs involved in the handover use the same WEP key, no inter-AP communication is required
- Unfortunately 802.1x complicates 802.11 handoff
  - now STAs have dynamic per-session keys
  - authentication occurs **after** reassociation, not before
  - If re-authentication is required, then STAs need to complete authentication before recovering connectivity
  - Authentication and key management methods requiring public key operations (e.g. EAP-TLS) -- this can take several seconds to complete
  - Using a TLS continuation can decrease the number of round-trips (from 3.5 to 2.5)
  - if authentication server is far away, then disconnection time can be large

for further information see [8]

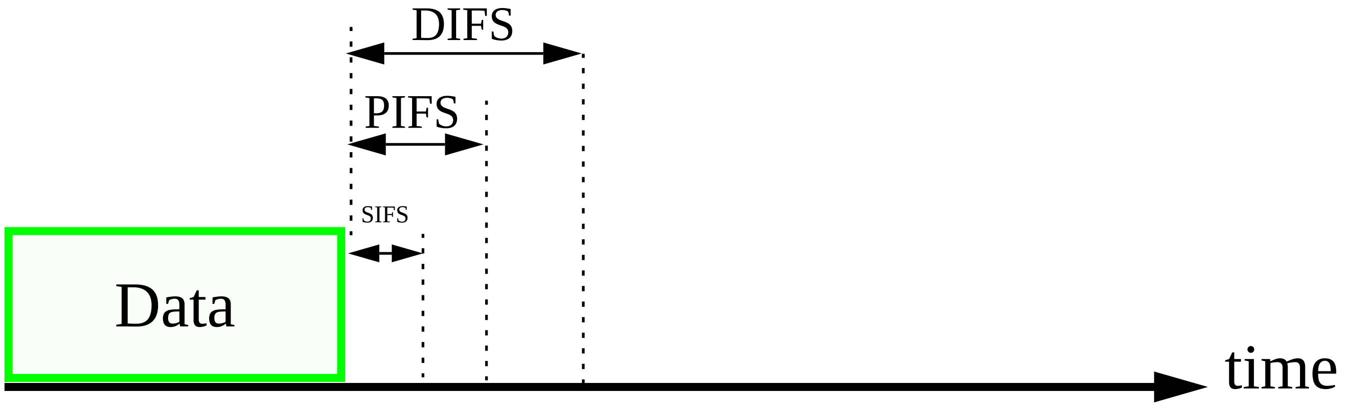
# Point Coordination Function (PCF)

Point Coordination Function (PCF) an optional extension to DCF that provides a time division duplexing capability to accommodate time bounded, connection-oriented services.

AP polls each station:

- enabling the polled station to transmit without contending for the medium
- Contention free period repetition interval (consisting of contention free period (CFP) and contention period (CP) is initiated by the AP through a Beacon frame.
  - If AP finds the medium idle, it waits for a PCF inter frame spacing (PIFS) period of time and then transmits a beacon frame with a polling frame following SIFS seconds after it
  - when a station receives the poll from the AP, the medium is reserved for the duration of its transfer (upto the length of CFP),when the data transfer complete (or the reserved time is up), the AP waits for PIFS seconds and polls another station - it continues until the CP interval is up - then the system operates in DCF mode.
- note: AP can transmit data along with the polling frame

# Spacing



# Timing and Power Management

Synchronization (to within 4 µs plus propagation delay) of all clocks within a BSS maintained by periodic transmission of beacons containing time stamp info. AP (in infrastructure mode) is the timing master and generates all timing beacons.

Power saving modes:

awake STAs (aka mobiles) are fully powered and can receive packets at **any** time.

doze

- unable to transmit or receive data, but uses little power
- STA must inform the AP it is entering the doze mode, then AP does not sent packets simply buffers them
- Unicast:
  - When AP has packets queued for STAs in doze state, a traffic indication map (TIM) is broadcast as part of the timing beacon
  - STAs in the doze mode power up receivers to listen for beacons, if identified by the TIM, they return to awake mode and transmit a PS-Poll message so the AP knows that they are ready to receive data
- Broadcast/multicast:
  - buffered broadcast/multicast packets queued in the AP are indicated in a delivery traffic indication message (DTIM) that is broadcast periodically to awaken all STAs and alert them to a forthcoming broadcast/multicast message; the message is then sent **without** the AP **waiting** for PS-Poll msgs.

# AAA

IEEE 802.1x -port-based network access control for authentication, authorization, and security[7]

See also Juan Caballero Bayerri and Daniel Malmkvist, “Experimental Study of a Network Access Server for a public WLAN access network”, M.S. Thesis, KTH/IMIT, Jan. 2002 [6].

## IEEE Extensible Authentication Protocol

An authentication protocol which supports multiple authentication mechanisms, runs directly over the link layer without requiring IP and therefore includes its own support for in-order delivery and re-transmission. Originally developed for use with PPP: Larry J. Blunk and John R. Vollbrecht, “PPP Extensible Authentication Protocol (EAP) standard”, RFC 2284

# Roaming

Roaming is dependent on the underlying networks providing you service and if they are to charge -- knowing who to charge and how much to charge.

Unlike macrocellular systems where you generally only face roaming when making large scale movements (between countries or major regions of a country), in WLAN systems the intersystem movement may occur with little of no movement!

## Clearinghouse

Clearinghouse to perform settlements between the various operators, see for example Excilan (*http://www.excilan.com*).

## Interconnect Provider

Telia’s Golden Gate and its Interconnect Provider Role, Nyckelgård, Sören, Telia Golden Gate - Technical Overview, available January 23, 2002 at *http://www.telia.se/filer/cmc_upload/0/000/030/185/ResearchGoldenGateTec1Overv2.doc* and

Martin Altinkaya and Saman Ahmedi, “SIP in an Interconnector and Service Provider Role”, M.S. Thesis, KTH/IMIT, Dec. 2001.

Since IEEE 802.11 specifies only upto the interface to the 802.2 link layer all mobility management is outside the scope of the standard.

# Proxies

Numerous proxy based proposals exist to “improve” performance across wireless links - especially targeted to TCP (most have problems keeping TCP/IP’s **end-to-end** semantics)

See:

Luis Muñoz, Marta Garcia, Johnny Choque, Ramón Agüero, and Petri Mähönen, “Optimizing Internet Flows over IEEE 802.11b Wireless Local Area Networks: A Performance-Enhancing Proxy Based on Forward Error Control”, IEEE Communications Magazine, December 2001, pp. 60-67.

# HiperLAN2

Developed by the European Telecommunications Standard Institute (ETSI) Broadband Radio Access Networks (BRAN)

- Dedicated spectrum (in Europe) at 5 GHz
- uses Orthogonal Frequency Division Multiplexing (OFDM) with 52 subchannels, 48 subchannels for data, and 4 subchannels for pilot symbols
- TDMA/TDD frames with fixed duration of 2ms
- Maximum gross data rate of 54 Mb/s
- MAC protocol was designed to support multimedia services

For more information see HiperLAN2 Global Forum *http://www.hiperlan2.com/*

and ETSI standards documents at: *http://www.etsi.org/frameset/home.htm?/technicalactiv/Hiperlan/hiperlan2.htm*

# 802.11a and 802.11h

IEEE 802.11a and ETSI’s HiperLAN2 standards have nearly identical physical layers, but are very different at the MAC level

IEEE 802.11h adds **Transmit Power Control (TPC)** to limit a device from emitting more radio signal than needed, and **Dynamic Frequency Selection (DFS)**, which lets the device listen to what is happening in the airspace before picking a channel

- TPC and DFS were introduced to satisfy European requirements
- 802.11h is to be sold under the name Wi-Fi5 (to build on the Wi-Fi branding)

# Multihop

MeshNetworks Inc. (*www.meshnetworks.com*) MeshLAN Multi-Hopping software:

- designed for use with Wi-Fi hardware
- extending useful range by adding multi-hopping peer-to-peer capabilities to off-the-shelf 802.11 cards

# QDMA (quad-division multiple access)

MeshNetworks' proprietary radio technology developed (by ITT Industries (`www.itt.com`)) for and currently used by the military.

- IP from end to end
- supports high-speed mobile broadband access
- infrastructure-free, i.e., ad hoc peer-to-peer networking

Claims they can deliver up to 6 Mbps to each user in a QDMA wireless network.

Products have built-in GPS (Global Positioning System) capabilities and QoS for IP voice and video.

First implemented in 2.4GHz as prototype routers, relays, and PDA-size client devices; now developing equipment for MMDS (2.5GHz) licensed operators.

They have FCC experimental license to build a (US) nationwide 4,000-node test network.

# All IP networks

Numerous efforts have shifted from simply using IP (rather than ATM) in the backbone and have been moving to an all IP network (i.e., IP directly to/from MS and in the infrastructure).

- Airvana Inc. (www.airvananet.com): all-IP architecture for radio access network equipment for 3G using CDMA2000 1x Evolution-Data Only (1xEV-DO) wireless technology, data rates up to 2.4 Megabits per second (Mbps) under ideal circumstances, with average sustained rates expected to be 300 to 600 kbps

Some view "4G" as the Fourth Generation **IP-based** wireless network.

**Eliminates** SS7 (Signaling System 7) telecommunications protocol

Flarion `http://www.flarion.com/` RadioRouter™ base stations used to build all-IP network

…

# Space Data Corporation

Space Data Corporation *http://www.spacedata.net/* to provide low data rate wireless (messaging and later voice) service to rural and surburban US (about 90% of the land mass, but only 20% of the population); Piggyback their repeaters on US National Weather Service biodegradable latex weather balloons “SkySites”.

Each balloon goes up to about 100,000 feet ~ 30km and stays there for ~1.5 days; baloons are launched from 70 sites twice each day; the repeater has power for 16 hours (12 for operation and the rest as a reserve). They expect to use 50,000 balloons per year, each repeater costs US$300

Their business model does not depend on any recovery of balloons (although they are adding GPS to theirs)

- US National Weather Service gets 18% of their back - they put a mailing address and promise to pay the postage on their payloads
- lots of knowledge of winds from 60 years of weather balloons

Space Data has a license for 1.4 MHz of bandwidth nationwide (license US$4.2M)

# Wireless Internet Service Providers (WISPs)

- Location specific WISP - exploiting high value sites (airports, hotels, coffee shops, … )
  - example: Surf ‘n Sip, MobileStar, and Wirelessbolaget
  - Advantages: often have “exclusive” offering
  - Disadvantages: users may also want access in other locations -- hence roaming agreements will be important
- Single site or campus WISP - a subset of the location specific WISP category (e.g., university or corporate campus, a single conference center/exhibition hall)
  - example: KTH and SU’s IT-University campus, CMU’s campus, …
  - Advantages: they know the site very well, generally they have “exclusive” offering, users are trapped - so they will have to pay and pay and pay or it is part of the tele/datacom offering
  - Disadvantages: for some sites the users are only there for a short period (hours to days), very high turn over in users (so low administrative costs are very important); in university and corporate campus settings very high demands/expectations

- Mobile carrier WISP - mobile (WWAN) operator also offering WLAN
    - examples: Telia HomeRun (Sweden), Sonera wGate (Finland), and VoiceStream (Germany / US) {due to their acquisition of MobileStar in the US - what happens if they bring this technology back to Europe?}
    - Advantages: they know where their users spend time (from their existing traffic and location data) so they can easily build out hotspots; retain customers with whom they already have a billing relationship
    - Disadvantages: offering WLAN might reduce their income (as they might have been able to charge (a lot) for the traffic via the WWAN in these same spots)
- ISP WISP - existing ISP that extends their network via WLAN access points
    - example: Sweden’s PowerNet
    - Advantages: pretty straight forward extension of their existing network, by shipping dual xDSL/cable/… + AP devices[1]; retain customers with whom they already have a billing relationship
    - Disadvantages: offering WLAN might reduce their income since neighbors can share rather than installing their own service
- WISP - a pure wireless internet service provider
    - example: Sweden: Wirelessbolaget, DefaultCity, U.S.: Wayport
    - Advantages: this is their business
    - Disadvantages: this is their business but they depend on an ISP for back haul

[1] Actiontec Electronics

- Operator Neutral WISP - an Internet eXchange (IX) to which several independent ISPs (or WISPs) are connected
  - example: StockholmOpen.net
  - Advantages: enable multiple operators
  - Disadvantages:
- Franchising WISP -
  - example:
  - Advantages: they simply sell the idea, starter kit, supply backup support, …
  - Disadvantages: dependant on getting a cut from the franchise
- Virtual WISP - no actual network, … - but rather they simply rent/buy capacity for their users; thus their major role is to support and bill users
  - example: Boingo
  - Advantages: very low to near zero costs for infrastructure
  - Disadvantages: they must provide either high service level and/or low prices to retain their customers
- Community/Grassroots WISP - altruistic providers
  - example: NYC Wireless
  - Advantages: people making their WLAN available to others “because it is the right thing to do”
  - Disadvantages: Support way or many not exist

Herslow, Navarro, and Scholander classify the WISPs based on whether they are “for fee” or for “free” and coverage area: hotspot vs. wide area.

# MIT’s AI Lab: Project Oxygen

> “Enabling people "to do more by doing less," that is, to accomplish more with less work.
>
> Bringing abundant computation and communication, as pervasive and free as air, naturally into people’s lives.”
>
> -- *http://oxygen.lcs.mit.edu/*

Utilzing self-configuring network with devices embedded in desks, walls, homes, … to create intelligent spaces

Handheld devices to support speech interfaces and reconfiguration for various protocols.

This is one of several projects trying to exploit ubiquitous/pervasive computing nad communication.

# Intelligent/Smart Spaces

Knowing what is around you is very useful for configuring devices and offering services, there are several proposals for how to do this:

- SUN's Jini
- Microsoft's Univeral Plug-and-Play

For further information see Theo Kanter's dissertation "Adaptive Personal Mobile Communication -- Service Architecture and Protocols":
*http://ps.verkstad.net/Thesis/Final/theoDissertation.pdf*

and also his defense slides:

*http://ps.verkstad.net/Thesis/Defense/theoDefense.pdf*

# Further reading

## WISPs

[1] Louise Herslow, Carl-Johan Navarro, and Joakim Scholander, “Exploring the WISP Industry - Analysing Strategies for Wireless Internet Service Providers”, Masters thesis, Institute of Economic Research, Lund University, Sweden, January 2002.

*http://www.scholander.com*

[2] David Alvén and Reza Farhang, “Does it take a WISP to manage a wisp of hotspots? - Analysis of the WLAN market from a WISP perspective”, Masters Thesis, Department of Microelectronics and Information Technology, Royal Institute of Technology, Sweden, February 2002. *http://www.e.kth.se/~e96_rfh/wisp_analysis.pdf*

## IEEE 802.11

[3] *http://standards.ieee.org/getieee802/*

[4] *http://www.80211-planet.com/*

[5] Rusty O. Baldwin, Nathaniel J. Davis IV, Scott F. Midkiff, and Richard A. Raines, “Packetized Voice Transmission using RT-MAC, a Wireless Real-time Mediaum Access Control Protocol, Mobile Computing and Communicaitons Review, V. 5, N. 3, July 2001, pp. 11-25.

## AAA

[6] Juan Caballero Bayerri and Daniel Malmkvist, *Experimental Study of a Network Access Server for a public WLAN access network*, M.S. Thesis, KTH/IMIT, Jan. 2002. *http://www.e.kth.se/~e97_dma/FinalReport.pdf*

[7] IEEE 802.1x Port Based Network Access Control *http://www.ieee802.org/1/pages/802.1x.html*

[8] Tim Moore and Bernard Aboba “Authenticated Fast Handoff”, IEEE 802.11 Task group i, November 2001, doc. IEEE 802.11 submission *http://www.drizzle.com/~aboba/IEEE/11-01-TBD-I-Authenticated-FastHandoff.ppt*