802.11 Wireless LAN Fundamentals
MODULE CONTENTS

- Technologies overview
- Spread Spectrum
  - Direct Sequence Spread Spectrum (DSSS)
  - Frequency Hopping Spread Spectrum (FHSS)
- Modulation
  - DBPSK/DQPSK
  - CCK
WIRELESS DATA NETWORKS

There are many different types of wireless data communications. Each of these has its advantages and drawbacks:

- **IR**- Very high data rates, lower cost, very short distance.
- **Narrowband**- Low data rates, medium cost, license required and limited distance.
- **Spread Spectrum**- Limited to campus coverage, low power, high data rates.
- **PCS**- Low data rates, medium cost, city wide coverage.
- **WMAN**- High power, monthly fees, city wide coverage (limited cities).
- **Cellular, CDPD**- Low data rates, high packet fees, national coverage.
Radio Frequency Spread Spectrum Technology

BASICS OF RF TECHNOLOGY, MODULATION, RF INTERFERENCE & THE WLAN CLIENT ASSOCIATION PROCESS.
Module Contents

- ISM Unlicensed Frequencies
- Spread Spectrum RF Technology
- Spread Spectrum Approaches
- IEEE 802.11
- Association Processes
- Multipathing
There are three unlicensed bands, at 900MHz, 2.4GHz, and 5.7GHz. These bands are referred to as the Industrial, Medical and Scientific Frequencies. 5.2GHz is the same band that is used for the ETSI HIPERLAN specification in Europe.

A nearby neighbor of the 900MHz band is the cellular phone system. This helped the early development of the WLAN industry in the 900MHz band because of the availability of inexpensive, small RF components developed for use in that band. The 2.4GHz band has a neighbor in the PCS system that helps with component costs also.

There are no such neighbors for the 5GHz band. The WLAN industry will have to drive the development of low cost components for 5GHz products. This may mean that practical, cost effective; PCMCIA products in the 5GHz band are a long time away. The other downside to the 5GHz band is the poor range performance as compared to 2.4GHz band.
The 900MHz band is becoming overcrowded due to consumer products. It does offer longer range (for the same gain antennas) than the 2.4GHz band, but it has limitations on the maximum size of antennas that limits its overall range. At 900MHz the highest data rate that be reliably obtained is under 1Mb due to the limited frequency range.

At 2.4GHz, the lower power transmitter allows very high gain antennas, which allows long distance communication (up to 25 miles). The frequency range is also much wider than 900MHz, allowing higher data rate with a reliable range.

The 5GHz band offers more bandwidth, allowing higher data rates; however, the nature of the higher frequency limits range. Typical range for 5GHz band products indoors is about 60 feet, and outdoors is limited to about 2500 feet.

<table>
<thead>
<tr>
<th>900 MHz vs. 2.4 GHz vs. 5 GHz</th>
<th>900 MHz Band</th>
<th>2.4 GHz Band</th>
<th>5 GHz Band</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PRO</strong></td>
<td>Greater Range than 2.4 GHz Band (For in-building LAN)</td>
<td>Global Market IEEE 802.11 Higher Data Rates</td>
<td>Global Market IEEE 802.11 Higher Data Rates</td>
</tr>
<tr>
<td><strong>CON</strong></td>
<td>Maximum Data Rate 1mbps Limited Bandwidth Crowded Band</td>
<td>Less Range than 900MHz (for in-building LAN) Crowded Band</td>
<td>Much Less Range than 2.4 and 900MHz Higher Cost of RF Equipment</td>
</tr>
</tbody>
</table>
What is Spread Spectrum RF Technology

This section discusses theories and processes of using Spread Spectrum technology to send data over an RF signal.

One of the reasons Cisco Aironet Wireless has focused on the 2.4GHz band for WLAN products is that this is the only band that is available with virtually the same technical rules for use world-wide.

In most parts of the world Cisco Aironet Wireless products can be deployed without a user license (i.e., it's unlicensed). With the exception of Japan, there is over 80 MHz of available spectrum.

Each country has its own set of rules governing the installation and use of RF products. Be aware that these rules may affect which products you use and may require you to obtain a site-specific license.
What is Spread Spectrum RF Technology (cont’d)

*Spread Spectrum is a type of modulation designed to be somewhat immune to interference, difficult to detect, and hard to intercept.*

An actress, Hedy Lamarr, and a music composer, George Antheil, patented the concept of Spread Spectrum in 1942. The idea was a method for guiding a torpedo without interference from a jamming signal.

In 1986, the FCC agreed to allow the use of Spread Spectrum in the commercial market under the ISM bands.

Just as the radio in your car has AM (Amplitude Modulation) and FM (Frequency Modulation) bands, other radios use different bands and types of modulation.
Transmitting a Signal

The goal of sending data over RF is to get information across with as much data as possible, sending it as far as possible and as fast as possible. More data can be placed on a signal in one of two ways:
- More frequency used or
- Complex modulation

When transmitting a signal in data format, three questions come to mind:

- How fast - What data rate can be achieved?
- How far - How far apart can the units be that are transmitting or receiving and still get the maximum data rate?
- How many- how many users can be on the system without slowing the data rate to an unacceptable level?

Wireless 802.11 products operate as a shared medium and can be thought of much the same way as a wired 10 Mbps Ethernet segment.

These factors all relate to the ability to receive a good signal as far away as possible. Increasing the amount of data requires the use of more frequency spectrum or methods of complex modulation.
More information means more frequency spectrum is used

• As more information is placed on a radio signal, more frequency spectrum (or bandwidth) is used.

• A CB signal has very low quality audio. This requires about 3KHz of bandwidth.

• A FM radio signal provides a high quality audio, which consumes about 175KHz of bandwidth.

• A TV signal, which contains both audio and video, utilizes almost 4500K (4.5MHz) of bandwidth.

• MORE INFORMATION= MORE FREQUENCY SPECTRUM USED
Complex modulation requires better signal strength, therefore less coverage is available. High-speed modems compress the data to use the same line as an old 300-baud modem.

Years ago, a modem was able to communicate at 300 baud, today, a 56K modem gets much higher speeds over the same wire as the 300-baud modem. This increase in speed is due to the modem compressing the data into a smaller space, and using the same bandwidth of the phone line as the 300 baud modem used. One problem that may arise is that if there is noise on the phone line, the modem speed will be reduced. As the data is further compressed, it requires a stronger signal as compared to the noise level. More noise means slower speed for the data to be received correctly.

The same is true in radio. As a receiver moves farther from a transmitter the signal gets weaker, and the difference between the signal and noise decreases. At some point, the signal cannot be distinguished from the noise and loss of communication occurs.

This means the same bandwidth is available. 56K modems require a better (quieter) phone line to communicate at the higher speed. If there is noise on the line, the modem will drop down in speed to connect. More noise, less speed
802.11b uses three different types of modulation, depending upon the data rate:

- **Binary phase shift keyed (BPSK)**
- **Quadrature phase shift keying (QPSK)**
- **Complementary code keying (CCK)**

BPSK uses one phase to represent a binary 1 and another to represent a binary 0 for a total of two bits of binary data. This is utilized to transmit data at 1Mbps.

With QPSK, the carrier undergoes four changes in phase and can thus represent four binary bits of data. This is utilized to transmit data at 2 Mbps.

CCK uses a complex set of functions known as complementary codes to send more data at 11 Mbps.
OSI Reference Model:
Physical

- **Network Oper. System**
  - Network Layer
  - Guarantees delivery data
- **Drivers**
  - LLC Layer
  - send/receive data
- **LAN Controller**
  - MAC Layer
  - data into/out frame
- **MODEM**
  - Physical Layer
  - frame into/out frame
WLAN TECHNOLOGIES

- Infrared
- Narrow Band
- Spread Spectrum
  - Direct Sequence
  - Frequency Hopping
INFRARED WIRELESS TECHNOLOGY

- Low power infrared light as the carrier
- No license required
- Very restricted mobility, limited coverage
- High data rate (10 Mbps, 16 Mbps)
- Line-of-Sight Infrared
  - no objects in the path between two stations
- Diffuse Infrared
  - uses reflections to set-up wireless link
NARROW BAND WIRELESS TECHNOLOGY

- **Dedicated band (18 GHz)**
  - License required
  - ISM band (915 MHz, 2.4 GHz, 5.8 GHz)
  - unlicensed (special modulation)
  - extremely low output power i.e. limited coverage
  - high data rate (up to 10 Mbps) on short distance

- **Europe - DECT band (1.8 GHz)**
  - based on voice standard
ISM FREQUENCY ALLOCATIONS WORLDWIDE

- 915 MHz only in the Americas (region 2)
- 2.4 GHz for global availability (region 1,2,3)
SPREAD SPECTRUM WIRELESS TECHNOLOGY

- Unlicensed usage (ISM band)
- No line of sight requirement (indoor)
- High link reliability
- Built-in transmission security
- Two techniques used:
  - Direct Sequence
  - Frequency Hopping
Module Contents

• Technologies overview

• Spread Spectrum
  • Direct Sequence
  • Frequency Hopping

• Modulation
  • DBPSK/DQPSK
  • CCK
Multiple Access Methods
Multiple users share the available spectrum

**FDMA**
- Each user assigned a different frequency - like ordinary radio

**TDMA**
- Multiple users share the same frequency channel sequentially
- Time slot sequence repeats over and over

**CDMA**
- Channel is “spread” over wide frequency band
- Many users share the same frequency band at the same time
- Each user is assigned a unique “code” to identify and separate them

*also known as “Spread Spectrum”*
Spread Spectrum Technologies

DS vs. FH

• Direct Sequence
  • Each symbol is transmitted over multiple frequencies at the same time
  • Very efficient (no overhead)
  • Higher speed than FH at comparable distances
  • System capacity (multiple channels) higher than FH

• Frequency Hopping
  • Sequential use of multiple frequencies
  • Hop sequence and rate will vary
  • “End hop waste time”
• Spreading: Information signal (i.e. a “symbol”) is multiplied by a unique, high rate digital code which stretches (spreads) its bandwidth before transmission.

• Code bits are called “Chips”.

• Sequence is called “Barker Code”
Spread Spectrum Technologies
What happens during “spreading”

- Due to the multiplication of a symbol with Barker code, the “rate-of-change” increases with a factor 11
- This means that cycle rate increases from 1 MHz to 11 MHz
- In terms of spectrum this means that after RF modulation the signal is spread from 2 MHz bandwidth to 22 MHz bandwidth
At the receiver, the spread signal is multiplied again by a synchronized replica of the same code, and is “de-spread” and recovered.

The outcome of the process is the original “symbol”
When the incoming signal is de-spread, it results in either a positive (+) or a negative (-) “spike”.

These “spikes” arrive at intervals equal to the symbol time.

A positive spike represents a “1” symbol, a negative spike represents a “0” symbol.
Echoes may arrive at the receiver, fluctuations can be noticed at positions other than at the symbol time boundaries.

These fluctuations are ignored as the receiver will only interpret the spike at the synchronization points (separated from each other by the symbol time).
Module Contents

• Technologies overview

• Spread Spectrum
  • Direct Sequence
  • Frequency Hopping

• Modulation
  • DBPSK/DQPSK
  • CCK
Modulation
DBPSK (Differential Binary Phase Shift Keying)

Table 1, 1 Mb/s DBPSK Encoding Table.

<table>
<thead>
<tr>
<th>Bit Input</th>
<th>Phase Change (+jω)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>π</td>
</tr>
</tbody>
</table>
Modulation
DQPSK (Differential Quadrature Phase Shift Keying)

Dibit pattern \((d_0, d_1)\)
d0 is first in time

\[\begin{array}{|c|c|}
\hline
\text{Dibit pattern (d0,d1)} & \text{Phase Change (+jω)} \\
\hline
00 & 0 \\
01 & \pi/2 \\
11 & \pi \\
10 & 3\pi/2 (-\pi/2) \\
\hline
\end{array}\]

Table 1, 2 Mb/s DQPSK Encoding Table
CCK
Turbo 11 Mb approach

CCK = Complementary Code Keying
• IEEE 802.11 standard for high speed
• 11 and 5.5 Mbps data rates
• Outstanding high multi-path performance
• Outstanding low-SNR performance
• Seamless interoperability with existing DS
• Maintains QPSK chips at 11 MHz chip rate
• Maintains 3 frequency channels
• FCC and MKK regulations satisfied
**CCK**

**How it Works**

- Data bits are encoded to a symbol which is transmitted in the form of 8 chips.
- For Data-Rate = Medium Encoding means:
  - mapping 2 data bits to I or Q channel (in-Phase, Quaternary Phase)
  - mapping 2 data bits to one of 4 Complex Codewords
- For Data-Rate = High Encoding means:
  - mapping 2 data bits to I or Q channel (in-Phase, Quaternary Phase)
  - mapping 6 data bits to one of 64 Complex Codewords
- Codewords are complex complementary codes selected from a code set.
CCK
Operating at Medium Speed

Pick One of 4 Complex Codes *

Scrambler

MUX 1:8

1.375 MHz
8 chips clocked with 11 MHz

11 MHz

Data Rate = 4 bits/symbol * 1.375 MSps = 5.5 MBps

*= Code Set:
747B
47B7
8B7B
B8B7
see next slide
CCK
How it Works

Code Set is defined by formula:

\[
c = \{e^{j(\varphi_1 + \varphi_2 + \varphi_3 + \varphi_4)}, e^{j(\varphi_1 + \varphi_3 + \varphi_4)}, e^{j(\varphi_1 + \varphi_2 + \varphi_4)},
\]

\[
-e^{j(\varphi_1 + \varphi_4)}, e^{j(\varphi_1 + \varphi_2 + \varphi_3)}, e^{j(\varphi_1 + \varphi_3)}, -e^{j(\varphi_1 + \varphi_2)}, e^{j\varphi_1}\}
\]

Data Rate = 8 bits/symbol * 1.375 MSps = 11 Mbps
CCK
Data Rates and Symbol Rates

• Bit-rates:

  • The 11 chips Barker sequence in Standard DSSS carries one symbol clocked at 1MHz, which results in a symbol rate of 1Msymbol/sec.

  • The 8 chips sequence in CCK clocked at 1 MHz, results in a symbol rate of 1.375 Msymbol/sec (i.e. 11/8)

  • At date rate = medium, 4 data bits are mapped on one symbol, which results in 5.5 Mbps (i.e. 1.375 * 4)

  • At date rate = high, 8 data bits are mapped on one symbol, which results in 11 Mbps (i.e. 1.375 * 8)
### CCK
From DSSS BPSK to 11 Mbps CCK

<table>
<thead>
<tr>
<th>802.11 DSSS BPSK</th>
<th>802.11 DSSS QPSK</th>
<th>5.5 MBps CCK</th>
<th>11 MBps CCK</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 MBps</td>
<td>2 MBps</td>
<td>5.5 MBps CCK</td>
<td>11 MBps CCK</td>
</tr>
<tr>
<td>Barker BPSK</td>
<td>Barker QPSK</td>
<td>2 bits encoded to 4 complex code words; 2-QPSK</td>
<td>6 bits encoded to 64 complex code words; 2-QPSK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 bits used to QPSK code word</td>
<td></td>
</tr>
<tr>
<td>I, Q</td>
<td>I, Q</td>
<td>2 bits encoded to 4 complex code words; 2-QPSK</td>
<td></td>
</tr>
<tr>
<td>11 chips</td>
<td>11 chips</td>
<td>8 chips</td>
<td>8 chips</td>
</tr>
<tr>
<td>1 MSps</td>
<td>1 MSps</td>
<td>1.375 MSps</td>
<td>1.375 MSps</td>
</tr>
</tbody>
</table>

1 bit used to BPSK code word

2 bits used to QPSK code word

6 bits encoded to 64 complex code words; 2-QPSK

8 chips

1.375 MSps
Module Summary

- Technologies overview
- Spread Spectrum
  - Direct Sequence
  - Frequency Hopping
- Modulation
  - BQPSK/BQPSK
  - CCK
IEEE 802.11 MAC Functionality
Global Implementation of IEEE 802.11

- **Digital Signal Processor (Theseus)**
- **IEEE 802.11 MAC chip (Hermes)**
Global Implementation of IEEE 802.11

- Digital Signal Processor (Theseus)
- IEEE 802.11 MAC chip (Hermes)
Global Implementation of IEEE 802.11

- Protocol functions programmed in FW, so flexible.
  - For use in station and access points (additional FW loaded when operating as access point)
  - Functions can be added over time, via upgrade utilities
IEEE 802.11 Features

- Sharing Medium
- ACK protocol
- Medium reservation (RTS/CTS)
- Fragmentation
- Multi-channel roaming
- Automatic data-rate fall-back
- Cell size / Multi-rate applications
- In-cell relay
- Power Management
- Wired Equivalent Privacy (WEP)
- Wireless Distribution System (WDS)
Sharing the Medium
The Way Ethernet Works CSMA/CD

- Adapters that can detect collisions (e.g. Ethernet adapters)
  - Carrier Sensing: listen to the media to determine if it is free
  - Initiate transmission as soon as carrier drops
  - When collision is detected station defers
  - When defer timer expires: repeat carrier sensing and start transmission
Sharing the Medium
Coordinating Access Using CSMA/CA

- Wireless LAN adapters cannot detect collisions, so different coordination schemes have to be devised
- DCF (Distributed Coordination Function)
  - Implemented as CSMA/CA (Carrier Sensing Multiple Access with Collision Avoidance)
  - Contention based (using “random” back-off timers to resolve contention)
- Global systems implement DCF
Sharing the Medium
Coordinating Access Using PCF

- **PCF (Point Coordination Function)**
  - Optional additional medium access control method
  - Contention free operation with single Point Coordinator in a cell (typically residing the AP)
  - Point Coordinator controls the medium by polling stations in the BSS
- Global systems do not implement PCF but are sensitive for PCF presence
Sharing the Medium
Inter-Frame Spacing

- Inter frame spacing required for MAC protocol traffic
  - SIFS = Short interframe space
  - PIFS = PCF interframe space
  - DIFS = DCF interframe space
- Back-off timer operates in the contention window
- Back-off time is expressed in terms of number of time slots
Collisions still can occur (interference; incapability of sensing other’s carrier)
  - IEEE 802.11 defines “low-level” ACK protocol
  - Provides faster error recovery
  - Makes presence of high level error recovery less critical
- Acknowledgment are to arrive at within the SIFS
- The DCF interframe space is observed before medium is considered free for use
“Hidden Stations”

The Problem

A sends to B
C doesn’t detect that, so C might also start sending to B
Collision of messages at B: both messages lost

• Situation that occurs in larger cells (typical outdoor)
  • Loss of performance
  • Error recovery required
“Hidden Stations”

The Solution

- IEEE 802.11 defines:
  - MAC level RTS/CTS protocol (Request to Send / Clear to Send)
  - Can be switched off to reduce overhead (when no hidden nodes exist)
  - More robustness, and increased reliability
  - No interruptions when large files are transmitted
IEEE 802.11 defines:

- MAC level function to transmit large messages as smaller frames (user definable)
- Improves performance in RF polluted environments
- Can be switched off to avoid the overhead in RF clean environments

A hit in a large frame requires re-transmission of a large frame. Fragmenting reduces the frame size and the required time to re-transmit.
Multi-Channel Roaming

- Global IEEE 802.11 systems, support multi-channel roaming
  - Access points are set to a fixed frequency
  - Stations do not need to be configured for a fixed frequency
  - Stations switch frequency when roaming between access points
  - Stations “associate” dynamically to the access point with best signal, on power on
- This implies
  - Easier configuration
  - Faster installation
Multi-Channel Roaming

Channel 1

Channel 6

Channel 11

Channel 1
Automatic Rate Select

- Global PC Card, dynamically switches data-rate
  - Fall back to lower data-rate when communications quality decreases
    - out of range situations
    - Interference
  - Fall-back scheme:
    - 11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps

- This implies
  - Operating at larger distances
  - Robustness in RF polluted areas
Automatic Rate Select

- Global PC Card in AP-500, AP-1000 and AP-2000 is capable of supporting different data-rates “simultaneously”:
  - e.g. operates at “High” speed in communication to nearby station and at “Low” speed to station that is further away.
- Data rate capability is maintained in “station association table”
- Speed of IEEE Management - and Control frames use fixed speed determined as “IEEE Basic Rates”, and controlled by “Multi-cast Rate parameter”.
Cell Size / Multi Rate Applications

- Cell-size can be influenced by “Distance between APs” parameter:
  - Distance between APs = Large -> large cell
  - Distance between APs = Medium -> medium size cell
  - Distance between APs = Small -> small cell
- Cell-size influences capacity per station in the cell
  - small cell physically accommodates smaller number of stations than large cell
  - bandwidth per station in small cell greater than in large cell
- Cell size influences data-rate
  - larger distance between station and access-point may lead to lower data-rate
Cell Size / Multi Rate Applications

- Mixture of cell-sizes accommodate mixed applications:
  - Office workers:
    - High physical station density
    - High bandwidth requirement
    - Small cell operating at high data rate
    - Distance between APs is small
  - Warehouse operations (such as forklift truck):
    - Low physical station density
    - Low bandwidth requirement (transaction processing)
    - Large cell operating at low data rate
    - Distance between APs is large
Multi Rate Applications

- 1 Mbits/sec
- 11 Mbits/sec
In-Cell Relay

- IEEE 802.11, in-cell relay:
  - Single radio module when used in the AP-500, AP-1000 or AP-2000 acts as repeater between two stations
  - Provides cells that are app. twice as large as cells without an access-point
  - Communication flows via access-point so overall transmission time increases relative to pre-IEEE 802.11 (or direct station to station communication)
- This implies:
  - Larger cell size and consequently less need for access points and interconnecting infrastructure
  - Reduced performance in peer to peer communication within one cell compared to AP-less cells
**In-Cell Relay**

**In-cell relay:**
- Larger cell (diameter = $d > a$)
- Lower throughput (data travels through air twice)

**No in-cell relay:**
- Smaller cell (diameter = $a < d$)
- Higher throughput (data travels through air once)
Power Management

- IEEE 802.11, supports power management:
  - nothing to send: station in sleep mode
  - out-bound traffic stored in Access Point (out-bound = from AP to STA)
  - station wake up only for Traffic Information Map (TIM)
  - if messages: stay awake to receive them
- This implies:
  - Prolonged battery life
  - Increase usability in hand-held equipment
  - Works best in application that have limited bandwidth requirements (transaction processing)
Wired Equivalent Privacy

- Optional security functionality (factory “installed”)
- Encryption based on RC4 (1988 RSA algorithm)
- Stream cipher 64 or 128 bits key
  - User defined keys can be 40 or 104 bits long
  - 24 bits varying for each packet called the IV (Initialization vector)
- Used for data encryption
- Used for shared key station authentication
- Global’s FW inside the PC Card (implementing WEP) contains unique protection against so-called “Weak Key” attacks
  - Sniffing (key capturing) programs such as Air Snort will are ineffective in “stealing” encryption keys
Wireless Distribution System

- IEEE 802.11, WDS means
  - Multiple (7) wireless “ports” inside the access-point for wireless operations
  - 1 port can be assigned to connect Wireless Stations
  - Up to 6 ports can be used to connect wirelessly to other Access Points
  - All done by one Global PC Card in the Access Point
  - All wireless links operate on the same channel
- WDS allows:
  - Extending the existing infrastructure with wireless backbone links
  - Totally wireless system without any wired backbones, needed in locations where large areas are to be covered and wiring is not possible
Wireless Distribution System

Channel 1

Channel 6

Channel 11
IEEE 802.11 Features
Module Summary

• ACK protocol
• Medium reservation (RTS/CTS)
• Fragmentation
• Multi-channel roaming
• Automatic data-rate fall-back
• Cell size / Multi-rate applications
• In-cell relay
• Power Management
• Wired Equivalent Privacy (WEP)
• Wireless Distribution System (WDS)
IEEE 802.11 Architecture
Module Contents

• IEEE 802.11 Terminology
• IEEE 802.11 MAC Frames
• Basic processes in IEEE802.11 networks
• Configuration parameters
IEEE 802.11 Terminology

Station (STA) Architecture:

- Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, but does not provide access to a distribution system
- Most often end-stations available in terminals (work-stations, laptops etc.)
- Implemented in IEEE 802.11 PC-Card
IEEE 802.11 Terminology

Station (STA) Architecture (cont’d):

- Ethernet-like driver interface
  - supports virtually all protocol stacks
- Frame translation according to IEEE Std 802.1H
  - IEEE 802.3 frames: translated to 802.11
  - Ethernet Types 8137 (Novell IPX) and 80F3 (AARP) encapsulated via the Bridge Tunnel encapsulation scheme
  - All other Ethernet Types: encapsulated via the RFC 1042 (Standard for the Transmission of IP Datagrams over IEEE 802 Networks) encapsulation scheme
  - Maximum Data limited to 1500 octets
- Transparent bridging to Ethernet
IEEE 802.11 Terminology

**Access-Point (AP) Architecture:**

- Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, and provide access to a distribution system for associated stations
- Most often infra-structure products that connect to wired backbones
- Implemented in IEEE 802.11 PC-Card when it is inserted in an AP-500 or AP-1000
IEEE 802.11 Terminology

Access-Point (AP) Architecture (cont’d):

• Stations select an Access-Point and “associate with it

• Access-Points:
  – Support roaming
  – Provide time synchronization functions (beaconing)
  – Provide Power Management support

• Traffic typically flows through Access-Point
  – in IBSS direct Station-to-Station communication takes place
IEEE 802.11 Terminology

Basic Service Set (BSS):

- A set of stations controlled by a single “Coordination Function” (=the logical function that determines when a station can transmit or receive)
- Similar to a “cell” in pre IEEE terminology
- A BSS can have an Access-Point (both in standalone networks and in building-wide configurations), or can run without and Access-Point (in standalone networks only)
- Diameter of the cell is app. twice the coverage-distance between two wireless stations
Basic Service Set (BSS)
Independent Basic Service Set (IBSS):

- A Basic Service Set (BSS) which forms a self-contained network in which no access to a Distribution System is available
- A BSS without an Access-Point
- One of the stations in the IBSS can be configured to “initiate” the network and assume the Coordination Function
- Diameter of the cell determined by coverage distance between two wireless stations
Independent Basic Service Set (IBSS)
IEEE 802.11 Terminology

Extended Service Set (ESS):
- A set of one or more Basic Service Sets interconnected by a Distribution System (DS)
- Traffic always flows via Access-Point
- Diameter of the cell is double the coverage distance between two wireless stations

Distribution System (DS):
- A system to interconnect a set of Basic Service Sets
  - Integrated; A single Access-Point in a standalone network
  - Wired; Using cable to interconnect the Access-Points
  - Wireless; Using wireless to interconnect the Access-Points
Extended Service Set (ESS)
Single BSS (with integrated DS)
Extended Service Set (ESS)

BSS’s with Wired Distribution System (DS)
Extended Service Set (ESS)
BSS’s and Wireless Distribution System (DS)
IEEE 802.11 Terminology

Service Set Identifier (SSID):

- “Network name”
- 32 octets long
- Similar to “Domain-ID” in the pre-IEEE WaveLAN systems
- One network (ESS or IBSS) has one SSID
IEEE 802.11 Terminology

Basic Service Set Identifier (BSSID)

- “cell identifier”
- 6 octets long (MAC address format)
- Similar to NWID in pre-IEEE WaveLAN systems
- One BSS has one SSID
- Value of BSSID is the same as the MAC address of the radio in the Access-Point
Module Contents

- IEEE 802.11 Terminology
- IEEE 802.11 MAC Frames
- Basic processes in IEEE802.11 networks
- Configuration parameters
Frame Formats

MAC Header format differs per Type:

- Control Frames (several fields are omitted)
- Management Frames
- Data Frames
**Address Field Description**

<table>
<thead>
<tr>
<th>Bits: 2</th>
<th>2</th>
<th>4</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Version</td>
<td>Type</td>
<td>SubType</td>
<td>To DS</td>
<td>From DS</td>
<td>More Frag</td>
<td>Retry</td>
<td>Pwr Mgt</td>
<td>More Data</td>
<td>WEP</td>
<td>Rsvd</td>
<td></td>
</tr>
</tbody>
</table>

**Frame Control Field**

<table>
<thead>
<tr>
<th>To DS</th>
<th>From DS</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
<td>N/A</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID</td>
<td>SA</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>SA</td>
<td>DA</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>

Addr. 1 = All stations filter on this address.
Addr. 2 = Transmitter Address (TA), Identifies transmitter to address the ACK frame to.
Addr. 3 = Dependent on To and From DS bits.
Addr. 4 = Only needed to identify the original source of WDS (Wireless Distribution System) frames.
Type and subtype identify the function of the frame:

- **Type=00**  Management Frame
  - Beacon
  - (Re)Association
  - Probe
  - (De)Authentication
  - Power Management

- **Type=01**  Control Frame
  - RTS/CTS
  - ACK

- **Type=10**  Data Frame
MAC Management Frames

- Beacon
  - Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, parameters
  - Traffic Indication Map

- Probe
  - SSID, Capabilities, Supported Rates

- Probe Response
  - Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, parameters
  - same for Beacon except for TIM
MAC Management Frames (cont’d)

- Association Request
  - Capability, Listen Interval, SSID, Supported Rates

- Association Response
  - Capability, Status Code, Station ID, Supported Rates

- Re-association Request
  - Capability, Listen Interval, SSID, Supported Rates, Current AP Address

- Re-association Response
  - Capability, Status Code, Station ID, Supported Rates
MAC Management Frames (cont’d)

• Dis-association
  – Reason code

• Authentication
  – Algorithm, Sequence, Status, Challenge Text

• De-authentication
  – Reason
Module Contents

• IEEE 802.11 Terminology
• IEEE 802.11 MAC Frames
• Basic processes in IEEE802.11 networks
• Configuration parameters
Operational Processes

Association

• To establish relationship with Access-Point

• Stations scan frequency band to and select Access-Point with best communications quality
  – Active Scan (sending a “Probe request” on specific channels and assess response)
  – Passive Scan (assessing communications quality from beacon message)

• Access-Point maintains list of associate stations in MAC FW
  – Record station capability (data-rate)
  – To allow inter-BSS relay

• Station’s MAC address is also maintained in bridge learn table associated with the port it is located on
Operational Processes
Authentication

• To control access to the infrastructure via an authentication

• Stations identify themselves to other stations (or Access-Points) prior to data traffic or association

• Open System Authentication
  – Uses null authentication algorithm
  – Default

• Shared Key Authentication
  – Uses WEP privacy algorithm
  – Optional
Operational Processes
Starting an ESS

• The infrastructure network is identified by its ESSID

• All Access-Points will have been set according to this ESSID

• Wireless stations will be configured to set their desired SSID to the value of ESSID

• On power up stations will issue Probe Requests and will locate the Access-Point that they will associate with:
  – “best” Access-Point with matching ESSID
  – “best” Access-Point if the “desired SSID” has been set to “ANY”
Operational Processes
Starting an IBSS

• Station configured for IBSS operation will:
  – “look” for Beacons that contain a network name (SSID) that matches the one that is configured
  – When Beacons with matching Network Name are received and are issued by an AP, Station will associate to the AP
  – When Beacons with matching Network Name are received and are issued by another Station in IBSS mode, the station will join this IBSS
  – When no beacons are received with matching Network Name, Station will issue beacons itself.

• All Stations in an IBSS network will participate in sending beacons.
  – All stations start a random timer prior to the point in time when next Beacon is to be sent.
  – First station whose random timer expires will send the next beacon
Operational Processes
Inter-Frame Spacing

- Inter frame spacing required for MAC protocol traffic
  - SIFS = Short interframe space
  - PIFS = PCF interframe space
  - DIFS = DCF interframe space
- Back-off timer expressed in terms of number of time slots
Operational Processes
Data Frames and their ACK

- Acknowledgment are to arrive at within the SIFS
- The DCF interframe space is observed before medium is considered free for use
Operational Processes
Traffic flow - Inter-BSS

- AP-1000 or AP-500
- PC-Card
- Association table
- STA-1
- STA-2
- Bridge learn table
- STA-1: 2
- STA-2: 2
- Inter-BSS Relay
- STA-1 acknowledges packet for STA-2
- STA-2 acknowledges packet for STA-1
- STA-1 associates to BSS-A
- STA-2 associates to BSS-A
Module Contents

- IEEE 802.11 Terminology
- IEEE 802.11 MAC Frames
- Basic processes in IEEE802.11 networks
- Configuration parameters
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 /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 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 WaveLAN 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)
  - IBSS (peer-to-peer network)
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
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.
Configuration Parameters
Advanced parameters (AP-500/1000)

Medium Reservation
• To enable/disable the RTS/CTS handshake.
  – Threshold value 0-2346 (value=2347 disables Medium Reservation)

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

Multicast Rate
• To specify data-rate used for transmitting Multicast frames
Configuration Parameters
Advanced parameters (AP-500/1000)

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

**DTIM**
- Power Management related parameter to specify the timing of the delivery of multicast traffic to stations that have indicated to receive multicast messages while under power management.
  
  Example:
  - DTIM=1 means multicast traffic when it arrives at the AP is passed through after every beacon
  - DTIM=3 means multicast traffic is passed through after every 3rd beacon message
**Configuration Parameters**

**Security parameters (AP-500/1000)**

**Closed System (AP)**
- To enable rejection of association requests from stations with *Network Name* set to “ANY”

**Enable Encryption**
- To enable/disable Encryption

**Encryption keys**
- Four fields to store up to four different encryption keys

**Encryption key index**
- Index identifying which of the four keys is the active one
Configuration Parameters
For Future Implementation

Message Fragmentation (STA and AP)
• To enable/disable fragmentation of messages. When enabled user is prompted to set the fragment-size (256-2346). Default: fragmentation disabled
  • Microwave Oven (threshold = 500)
  • Medium Velocity (15 km/h) (threshold = 800)
  • High Velocity (30 km/h) (threshold = 300)

WDS Address (AP)
• MAC address of the corresponding AP in a WDS link
Module Contents

- IEEE 802.11 MAC Frames
- IEEE 802.11 Terminology
- Basic processes in IEEE802.11 networks
- Configuration parameters
System Performance
Module Contents

• Overview
• Data-rate
• Throughput
• Response times
• Capacity
• Power consumption
Performance means different things depending on application and user interest:

- **Data-rate** - Raw bit rate, comparison purposes, technology oriented
  - What is maximum speed that the technology allows?

- **Throughput** - File transfer time, real-life practice, office automation
  - How long does it take to transfer files?

- **Response times** - Transaction handling, includes more than just transfer time
  - How long does it take to complete a transaction?

- **Capacity** - Sharing bandwidth among users
  - How many stations can coexist in one cell?

- **Power consumption** - Battery operated equipment
  - How long will the battery last?
Performance expectations differ per application:

- **Transaction processing**
  - Require fast responses (same as wired LAN)
  - Characterized by short message (impose low network load)
  - Raw data-rate is of limited important (as long as network load stays low)

- **Office Automation**
  - Response times less critical
  - Medium to high network load
  - Network capacity is key aspect to keep under control
Overview

Performance expectations differ per application:

- **Multimedia**
  - Require un-interrupted execution of multimedia files (movie clips)
  - Characterized by large files
  - Raw data-rate and capacity are critical (need to be maximized)

- **CAD/CAM**
  - Characterized by large files
  - High network load
  - Need for capacity is critical (need to be maximized)
Module Contents

• Overview
• Data-rate
• Throughput
• Response times
• Capacity
• Power consumption
Data-Rate

• Data-rate (or bit-rate) expressed in Mbit/s
• Relates to the data only (not the preamble)
• Determined by technology:
  – DBPSK - 1 Mbps
  – DQPSK - 2 Mbps
  – CCK - 5.5/11 Mbps
• MAC Management frames and multicast frames are transmitted at lower data-rate to be able to reach stations with different speed capabilities
  – Multi-cast traffic can be configured to high speed (in the AP), in combination with the cell-size (=distance between APs).
Data Rate
Auto Fallback

Auto Rate Select
  – Start at highest possible data-rate (= 11 Mbps)
  – Fall-back to next lower data-rate
    • when 2 subsequent transmissions fail (ACKs missed)
  – Upgrade to next higher data-rate
    • after 10 successful transmissions (ACKs)
    • after 10 seconds
    • try next higher data-rate
      – if fails, go back to “Low”
      – if successful, go to normal rate
  – AP follows STA
Module Contents

- Overview
- Data-rate
- Throughput
- Response times
- Capacity
- Power consumption
Throughput

- Typically expressed in Kbytes/sec
- Throughput lower than bit-rate due to
  - IEEE 802.11 Management & Control frames xmit at lower data rate
  - Contention window (required to avoid collisions)
  - Inter-frame spacing in the media
  - Sources of interference
  - Network Operating System overhead (protocol stacks)
  - Other users that share the media
- Throughput as perceived by users differ also due to
  - Path between station and access point (need for re-transmissions)
    - Distance
    - Environment (walls, sources of interference)
  - File size
  - Additional security solutions such as WEP and VPN tunnels
Throughput
Impact of IEEE 802.11 MAC

802.11 frame structure
Throughput

Impact of IEEE 802.11 MAC

### IEEE 802.11b, 802.11a and 802.3 Frame Structure and Overhead Related Parameters

<table>
<thead>
<tr>
<th></th>
<th>802.11b</th>
<th>802.11a</th>
<th>802.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit rates</td>
<td>1, 2, 5.5, 11 Mbit/s</td>
<td>6, 9, 12, 18, 24, 36, 48, 54 Mbit/s</td>
<td>10, 100 Mbit/s (1000 Mbit/s is not shown)</td>
</tr>
<tr>
<td>DIFS</td>
<td>50 μs</td>
<td>25 μs</td>
<td>IFS 9.6 μs, 0.96 μs</td>
</tr>
<tr>
<td>Slot time</td>
<td>20 μs</td>
<td>6 μs</td>
<td>51.2 μs, 5.12 μs</td>
</tr>
<tr>
<td>Preamble and PHY header</td>
<td>192 μs</td>
<td>10, 7, 6, 5, 4, 3, 3 μs</td>
<td>6.4 μs, 0.64 μs</td>
</tr>
<tr>
<td>MAC overhead</td>
<td>34 byte</td>
<td>34 byte</td>
<td>18 byte</td>
</tr>
<tr>
<td>Payload data</td>
<td>46 – 1500 byte (0 – 2312 byte without 802.3 infrastructure)</td>
<td>46 – 1500 byte (0 – 2312 byte without 802.3 infrastructure)</td>
<td>46 – 1500 byte</td>
</tr>
<tr>
<td>Short IFS</td>
<td>10 μs</td>
<td>13 μs</td>
<td>N.A.</td>
</tr>
<tr>
<td>Preamble and PHY header</td>
<td>192 μs</td>
<td>10, 7, 6, 5, 4, 3, 3 μs</td>
<td>N.A.</td>
</tr>
<tr>
<td>MAC overhead per ACK</td>
<td>14 byte</td>
<td>14 byte</td>
<td>N.A.</td>
</tr>
</tbody>
</table>
Throughput
Depends on Configuration

<table>
<thead>
<tr>
<th>Data rate (11 Mbps)</th>
<th>11 Mbps</th>
<th>5.5 Mbps</th>
<th>2 Mbps</th>
<th>1 Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBSS (station to station)</td>
<td>5.04</td>
<td>3.44</td>
<td>1.59</td>
<td>0.87</td>
</tr>
<tr>
<td>Single BSS (station to station via WP)</td>
<td>2.85</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESS (wireless station to wired station)</td>
<td>4.66</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Throughput in Single BSS lower than IBSS or ESS as result of intra-cell relay function (traffic travels twice through the medium, invoking defers as part of CSMA/CA)

All values are in Mbps

Source: Testing at WCND using WhatsUpGold throughput test (packet size = 8192 Bytes)
Throughput Depends on Protocol Stacks

Measurements using WaveLAN at 2 Mbit/sec

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Measured Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETBEUI</td>
<td>180 Kbytes/sec</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>144 Kbytes/sec</td>
</tr>
<tr>
<td>IPX/SPX</td>
<td>155 Kbytes/sec</td>
</tr>
</tbody>
</table>

Source: Testing at WCND
## Throughput

Depends on number of stations in cell

### Measurements using WaveLAN at 2 Mbit/sec

<table>
<thead>
<tr>
<th>Number of stations</th>
<th>Measured Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>177 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td>1.42 Mbit/sec</td>
</tr>
<tr>
<td>3</td>
<td>177 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td>1.42 Mbit/sec</td>
</tr>
<tr>
<td>4</td>
<td>167 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td>1.34 Mbit/sec</td>
</tr>
<tr>
<td>5</td>
<td>166 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td>1.33 Mbit/sec</td>
</tr>
<tr>
<td>6</td>
<td>160 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td>1.28 Mbit/sec</td>
</tr>
<tr>
<td>7</td>
<td>159 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td>1.27 Mbit/sec</td>
</tr>
</tbody>
</table>

Source: Testing at WCND  
File size: 10 Kbytes  
Protocol: IPX/SPX
Throughput
Depends on File Size

Measurements using WaveLAN at 2 Mbit/sec

<table>
<thead>
<tr>
<th>File size</th>
<th>Measured Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 Kbytes</td>
<td>236 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td>1.88 Mbit/sec</td>
</tr>
<tr>
<td>500 Kbytes</td>
<td>184 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td>1.47 Mbit/sec</td>
</tr>
<tr>
<td>1 Mbytes</td>
<td>181 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td>1.44 Mbit/sec</td>
</tr>
</tbody>
</table>

Source: Canterbury Christ Church College
Number of stations: 1
Protocol: TCP/IP
Throughput
Depends on Path Between Station and AP

Ground floor

1st floor

Source: Canterbury Christ Church College
## Throughput

Depends on Path Between Station and AP

Measurements using WaveLAN at 2 Mbit/sec

<table>
<thead>
<tr>
<th>Position</th>
<th>Measured Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>206 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>204 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>200 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>202 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>202 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>202 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>200 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>163 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>182 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>200 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>201 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>199 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>200 Kbytes/sec</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Canterbury Christ Church College
Number of stations: 1
File size(s): 100 Kbytes, 500 Kbytes, 1 Mbytes (measurements are averages)
Protocol: TCP/IP
Module Contents

• Overview
• Data-rate
• Throughput
• **Response times**
• Capacity
• Power consumption
Response Times

- Typically expressed in seconds
- Key aspect in transaction processing
- Network load is small (short messages)
- Depends less on factors that determine throughput
  - Network Operating System overhead (protocol stacks)
  - Other users that share the media
  - Inter-frame spacing in the media
  - path between station and access point (need for re-transmissions)
- But more on server application
  - Time it takes to turn around of the transaction-request
Response Times

<table>
<thead>
<tr>
<th></th>
<th>4 Kbytes</th>
<th>50 Kbytes</th>
<th>350 Kbytes</th>
<th>800 Kbytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>WaveLAN</td>
<td>0.14</td>
<td>0.53</td>
<td>3.70</td>
<td>10.4</td>
</tr>
<tr>
<td>Token Ring</td>
<td>0.14</td>
<td>0.54</td>
<td>3.60</td>
<td>8.60</td>
</tr>
<tr>
<td>Ethernet</td>
<td>0.11</td>
<td>0.30</td>
<td>1.80</td>
<td>5.11</td>
</tr>
</tbody>
</table>
Module Contents

- Overview
- Data-rate
- Throughput
- Response times
- Capacity
- Power consumption
Number of stations per “radio-cell” depends on

- Bandwidth requirements per station
  - user profile

- Available bandwidth per cell
  - net capacity per cell depending on protocol and path: 1.1 - 1.8 Mbit/sec (for a 2 Mbit/sec data rate)
  - maximum data-rate (11 Mbit/sec maximum)

- Dimension (coverage) of the cell

- Number of co-located cells
  - can be increased by using additional channels
Capacity
Bandwidth Requirements

Differ per application:

- Transaction processing
  - < 8 Kbit/sec

- Office Automation
  - < 64 Kbit/sec (depending on user profile)

- Multimedia
  - 100-800 Kbit/sec

- CAD/CAM
  - >1.5 Mbit/sec
Capacity
Office Automation User Profiles

- Single cell
- Raw cell capacity: 2 Mbit/sec
- User profiles:
  - Light user
    - 16 Kbit/sec
  - Medium user
    - 32 Kbit/sec
  - Heavy user
    - 64 Kbit/sec

**Simultaneous Office Automation Users**

- Light User (2 KBps) - 80
- Medium User (4 KBps) - 40
- Heavy User (8 KBps) - 20
Capacity
Dimension of the Cell

• Cell size scaling

• Changes carrier detect and defer thresholds
  – Carrier Detect threshold - indication for station to accept/reject signal
  – Defer threshold - indication to station to defer for transmission from other station in the cell

• Expressed in terms of “Distance between APs”
  – Large
  – Medium
  – Small

• Cell size to match application:
  – small cell for high band width high capacity
  – Large cell for low bandwidth low capacity
## Capacity

### Dimension of the Cell

<table>
<thead>
<tr>
<th>“Distance between AP” parameter setting</th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cell diameter (open office)</td>
<td>~ 60 meter</td>
<td>~ 90 meter</td>
<td>&gt; 100 meter</td>
</tr>
<tr>
<td>Carrier detect threshold</td>
<td>- 85 dBm</td>
<td>- 90 dBm</td>
<td>- 95 dBm</td>
</tr>
<tr>
<td>Defer threshold</td>
<td>- 75 dBm</td>
<td>- 85 dBm</td>
<td>- 95 dBm</td>
</tr>
<tr>
<td>Cost impact</td>
<td>Highest</td>
<td>Less</td>
<td>Lowest</td>
</tr>
</tbody>
</table>
Capacity
Multi-channel Networks

- 802.11b radios operate in 2.4 GHz ISM band 2400-2483.5 MHz, but require a frequency band of app. 22 MHz
Capacity
Multi-channel Networks

Regulatory domain defines allowed channel set:

<table>
<thead>
<tr>
<th>Channel ID</th>
<th>FCC</th>
<th>ETSI</th>
<th>France</th>
<th>Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2412</td>
<td>2412</td>
<td>-</td>
<td>2412</td>
</tr>
<tr>
<td>2</td>
<td>2417</td>
<td>2417</td>
<td>-</td>
<td>2417</td>
</tr>
<tr>
<td>3</td>
<td>2422</td>
<td>2422</td>
<td>-</td>
<td>2422</td>
</tr>
<tr>
<td>4</td>
<td>2427</td>
<td>2427</td>
<td>-</td>
<td>2427</td>
</tr>
<tr>
<td>5</td>
<td>2432</td>
<td>2432</td>
<td>-</td>
<td>2432</td>
</tr>
<tr>
<td>6</td>
<td>2437</td>
<td>2437</td>
<td>-</td>
<td>2437</td>
</tr>
<tr>
<td>7</td>
<td>2442</td>
<td>2442</td>
<td>-</td>
<td>2442</td>
</tr>
<tr>
<td>8</td>
<td>2447</td>
<td>2447</td>
<td>-</td>
<td>2447</td>
</tr>
<tr>
<td>9</td>
<td>2452</td>
<td>2452</td>
<td>-</td>
<td>2452</td>
</tr>
<tr>
<td>10</td>
<td>2457</td>
<td>2457</td>
<td>2457</td>
<td>2457</td>
</tr>
<tr>
<td>11</td>
<td>2462</td>
<td>2462</td>
<td>2462</td>
<td>2462</td>
</tr>
<tr>
<td>12</td>
<td>-</td>
<td>2467</td>
<td>2467</td>
<td>2467</td>
</tr>
<tr>
<td>13</td>
<td>-</td>
<td>2472</td>
<td>2472</td>
<td>2472</td>
</tr>
<tr>
<td>14</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2484</td>
</tr>
</tbody>
</table>
# Capacity

## Multi-channel Networks - ETS

<table>
<thead>
<tr>
<th>Channel number</th>
<th>Top of channel</th>
<th>Center frequency</th>
<th>Bottom of channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2412</td>
<td>2423</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2411</td>
<td>2422</td>
<td>2433</td>
</tr>
<tr>
<td>3</td>
<td>2416</td>
<td>2427</td>
<td>2438</td>
</tr>
<tr>
<td>4</td>
<td>2421</td>
<td>2432</td>
<td>2443</td>
</tr>
<tr>
<td>5</td>
<td>2426</td>
<td>2437</td>
<td>2448</td>
</tr>
<tr>
<td>6</td>
<td>2431</td>
<td>2442</td>
<td>2453</td>
</tr>
<tr>
<td>7</td>
<td>2436</td>
<td>2447</td>
<td>2458</td>
</tr>
<tr>
<td>8</td>
<td>2441</td>
<td>2452</td>
<td>2463</td>
</tr>
<tr>
<td>9</td>
<td>2446</td>
<td>2457</td>
<td>2468</td>
</tr>
<tr>
<td>10</td>
<td>2451</td>
<td>2462</td>
<td>2473</td>
</tr>
<tr>
<td>11</td>
<td>2456</td>
<td>2467</td>
<td>2478</td>
</tr>
<tr>
<td>12</td>
<td>2461</td>
<td>2472</td>
<td>2483</td>
</tr>
<tr>
<td>13</td>
<td>2467</td>
<td>2478</td>
<td>2484 MHz</td>
</tr>
</tbody>
</table>

ISM Band: 2400 MHz to 2484 MHz
Capacity
Multi-channel Networks - FCC

Channel number
Top of channel
Center frequency
Bottom of channel

2400 MHz ↔ ISM Band → 2484 MHz

<table>
<thead>
<tr>
<th>Channel</th>
<th>Top of channel</th>
<th>Center frequency</th>
<th>Bottom of channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2412</td>
<td>2423</td>
<td>2401, 2423</td>
</tr>
<tr>
<td>2</td>
<td>2417</td>
<td>2428</td>
<td>2406, 2428</td>
</tr>
<tr>
<td>3</td>
<td>2422</td>
<td>2433</td>
<td>2411, 2433</td>
</tr>
<tr>
<td>4</td>
<td>2427</td>
<td>2438</td>
<td>2416, 2438</td>
</tr>
<tr>
<td>5</td>
<td>2432</td>
<td>2443</td>
<td>2421, 2443</td>
</tr>
<tr>
<td>6</td>
<td>2437</td>
<td>2448</td>
<td>2426, 2448</td>
</tr>
<tr>
<td>7</td>
<td>2442</td>
<td>2453</td>
<td>2431, 2453</td>
</tr>
<tr>
<td>8</td>
<td>2447</td>
<td>2458</td>
<td>2436, 2458</td>
</tr>
<tr>
<td>9</td>
<td>2452</td>
<td>2463</td>
<td>2441, 2463</td>
</tr>
<tr>
<td>10</td>
<td>2457</td>
<td>2468</td>
<td>2446, 2468</td>
</tr>
</tbody>
</table>
Capacity
Multi-channel Networks

• Multiple channels within 2.4 GHz band, can be used based on regulatory domain

  – ETS (most of Europe, Australia, ..): 1 .. 3 channels
  
  – North America: 1 .. 3 channels
  
  – World: 1 .. 3 channels
  
  – Japan: 1 .. 3 channels
  
  – France: single channel
Capacity
Multi-channel Networks

- Network Capacity can be increased by using different channels (by co-locating or stacking cells):
  - Multiple APs covering the same area but using different frequencies.
  - Can lead to capacity increase of factor 3-4 depending on proper AP placement, and allowable channels.

- Warning:
  - Use multiple channels only when there is a need for additional capacity.
  - If extra capacity is not needed, select one channel for the complete network and choose the channel that has least interference.
Capacity
Multi-channel Networks

- Three APs (identified by a colored star) cover a rectangular area (e.g. Classroom)
  - AP-1 set to channel 1
  - AP-2 set to channel 6
  - AP-3 set to channel 11
- 25 stations in the classroom (represented by colored dots) associate to one of the APs
Using two PC Cards in one AP-1000 requires:
- One PC Card to be connected to a range extender
- Two channel systems (versus three channel systems shown earlier)

Note: a ✓ symbol indicates a channel combination that can be used.
**Capacity**

Multi-channel Networks - Near-far Behavior

- Impact of physically nearby station that operates in different channel
- Seen as interference - no defer
- Minimum distances need to be observed to allow good operation

<table>
<thead>
<tr>
<th>Station-A’s channel</th>
<th>Station-B’s channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel 1</td>
<td>Channel 3</td>
</tr>
<tr>
<td>Channel 4</td>
<td>Channel 5</td>
</tr>
<tr>
<td>Channel 6</td>
<td>Channel 7</td>
</tr>
<tr>
<td>Distance d3</td>
<td>5-10 meter</td>
</tr>
<tr>
<td></td>
<td>1-4 meter</td>
</tr>
<tr>
<td></td>
<td>1-2.5 meter</td>
</tr>
<tr>
<td></td>
<td>1-2 meter</td>
</tr>
<tr>
<td></td>
<td>1-1.5 meter</td>
</tr>
</tbody>
</table>

\[ d1 = d2 = 20 \text{ meter} \]
Module Contents

- Overview
- Data-rate
- Throughput
- Response times
- Capacity
- Power consumption
Power Consumption

Power consumption can be reduced by Standard 802.11 Power Save Mode:

• Improves battery life

• Impacts throughput

• Not recommended for all applications
Power Consumption
How Power Management Works

- Station under Power Management can be in two states:
  - Awake
  - Doze (sleep)

- Traffic to be transmitted to the station is buffered by the Access-Point, when station is in doze state

- Station wakes for (nth) Beacon and examines TIM (TIM = Traffic Indication Map), which is inside Beacon

- When traffic is present station polls the Access-Point for each buffered frame

- When station needs to transmit it wakes up for transmission, and goes back to sleep immediately
Power Consumption
How Power Management Works

- Station can be configured to receive multi-cast messages

- Access-Point will buffer multi-cast traffic and send it following a DTIM (=Delivery Traffic Information Message) inside the Beacon

- DTIM interval can be configured at the Access-Point in terms of # of beacons between subsequent DTIM messages:
  - e.g every nth beacon (where n is user configuration parameter)
Power Consumption
How Power Management Works

TIM-Interval
TX operation
PS Station
PS-Poll
TX operation

Time-axis
AP activity
Broadcast
TIM
TIM
DTIM
TIM
TIM
DTIM

Broadcast

TIM-Interval
DTIM interval

Sparco Technologies
Power Consumption
Impact of Power Management

• Improves battery life

• Reduced amount of power consumed by the network card
  – Overall battery life improvement more significant when network card’s power consumption represent large portion of total
  – Overall battery life improvement insignificant when platform station consumes substantial amount of power for non-network elements

• Impacts throughput
  – Transmission of large files will suffer from reduced performance
  – Transaction oriented processing will not perceive performance impact
Power Consumption
Impact of Power Management

- Platform that consumes more power for other elements
  - Disk
  - Screen
  - Memory

50% reduction in PC Card’s power consumption
10% reduction in overall system power consumption
Power Consumption
Impact of Power Management

- Platform that is designed for low power
  - no back-light on screen
  - no rotating media
  - low power processor

Basic platform elements (20%)
PC Card (80%)

50 % reduction in PC Card’s power consumption
40 % reduction in overall system power consumption
### Power Consumption

**Impact of Power Management**

- Throughput measurements on notebook computer
- Large file (7.01 Mbytes) transmission

<table>
<thead>
<tr>
<th></th>
<th>Network disk to Notebook</th>
<th>Notebook to network disk</th>
<th>Average Battery life</th>
</tr>
</thead>
<tbody>
<tr>
<td>With Power Management</td>
<td>213 sec</td>
<td>422 sec</td>
<td>128 minutes</td>
</tr>
<tr>
<td>Without Power Management</td>
<td>62 sec</td>
<td>89 sec</td>
<td>102 minutes</td>
</tr>
</tbody>
</table>
Power Consumption

Applicability of Power Management

- Hand-held data terminals (scanners)
- PDAs under Windows/CE
- Sub-Notebook
- Notebook (light load on network)
- Notebook (medium load on network)
- Notebook (heavy load on network)
Roaming
Module Contents

- Scan
- Sweep
- Association
- Authentication
- Roaming
Scan

- Access-Point and Station need to be established on same frequency in order to communicate

- Access-Points operate on a fixed frequency (selected from an allowed set of channels)

- Stations dynamically “tune” the radio to the channel of the Access-Point

- Process is called Scanning
IEEE 802.11 defines two methods:

- **Passive Scanning**
  - Station switches to a given channel and listens for incoming beacons from Access-Point

- **Active Scanning**
  - Station switches to a given channel and issues a “Probe Request”
  - Access-Point replies with a “Probe Response”
Module Contents

- Scan
- **Sweep**
- Association
- Authentication
- Roaming
Sweep

• A series of scans on different channels is called a “Sweep”

• A Sweep uses a “channel-list” that contains the channels to scan

• There are two type of sweeps:
  
  – “Full Sweep”
    • All channels in the “channel-list” are scanned
  
  – “Short Sweep”
    • A sub-set of the “channel-list” is used to perform the scan
Sweep

“Short Sweep” will speed up the roaming process

• Subset of channel lists contains
  – Active channels
    • Channels that have been found to be used before since the station has been switched on
  – Most likely channels
    • Channels that have likely channel separation from active channels (more than two channels away from active one)
    • Example: If channel 5 is active, channel 2 and 8 are likely. *Channel 3, 4, 6 and 7 are unlikely as they are too close to channel 5 and will not be scanned*
Module Contents

• Scan
• Sweep
• Association
• Authentication
• Roaming
Association

Station that needs connection to a network initiates “Initial Association” sequence:

- Execute a full sweep
- Select AP with best communications quality, that matches the value for “network name” (= SSID).
  - If “network name” set to “ANY” and Access-Point is not set to “closed”
- Station send “Association Request”
- AP enters the Station in its Association Table (and assigns an “Association Code” to it)
Association

Association table

<table>
<thead>
<tr>
<th>Bridge learn table</th>
<th>STA-1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>STA-2</td>
<td>2</td>
</tr>
</tbody>
</table>

ORiNOCO PC-Card

Association table

<table>
<thead>
<tr>
<th>STA-1</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>STA-2</th>
</tr>
</thead>
</table>

Inter-BSS Relay

STA-1

Associate

STA-2

Associate
Module Contents

• Scan
• Sweep
• Association
• Authentication
• Roaming
Authentication

- Stations authenticate at each Access-Point once before their first association to the Access-Point.

- A roaming station may need to re-authenticate at the Access-Point that it is roaming to, even though it has been authenticated by the Access Point it roams away from. In future implementations of IAPP, this will pass authentication information as part of the hand-over protocol.
Authentication

- Authentication schemes (will be explained in module on security):
  - IEEE 802.11 defined:
    - Open System Authentication
    - Shared Key Authentication (based on WEP)
  - RADIUS Based MAC authentication
    - Based on MAC address of PC Card registered in centrally kept Access Control list
Module Contents

- Scan
- Sweep
- Association
- Authentication
- Roaming
Roaming Communications Quality

• Key indicator of to assess path between Station and Access-Point
• Determined by:
  – SNR (Signal to Noise Ratio) on path with current Access-Point:
    • Running Average Signal Level from Beacon receptions
    • Running Average Noise Level from all receptions in current channel
  – Result of Sweep (when Searching):
    • SNR of Probe Responses
Roaming Communications Quality

- Station monitors the *communications quality (CQ)* of the link to “its” Access-Point

- When station moves away from Access-Point the CQ drops decreases

- When CQ drops below a set threshold value the Station enters Cell-Search state
Roaming
Cell Search State

Station ...

- Informs current AP to buffer traffic during Sweep (PM buffering)
- Blocks its own transmissions during Sweep
- Scans Multiple Channels
  - limited to Active (or Likely-to-be-Active) Channels
  - learns during sweeps
    - 3 channels on each side of an Active channel are considered “Not Likely”
- Uses Active Scanning (Probe Requests)
- Takes 5 .. 50 ms per Channel (depending on activity)
Roaming
Switching to new Access-Point

- Switching based on “delta-SNR”:
  - SNR of Probe Responses compared to SNR current Access-Point

- When CQ drops below “Cell Search Threshold” new Access-Point should already been identified

- Station also enters “cell-search” when it misses 4 or more Beacons in a row:
  - Busy cell
  - Form of load balancing
Roaming
Out of Range Condition

• When no Access-Point present acceptable to station:
  – Station will stay associated
  – Station will fall back to lower bit-rate
  – Eventually loss of association

• Out of Range Threshold is Carrier Detect Threshold (influenced by AP Density parameter)

• Station will scan all channels in full sweep every 10 seconds (versus short sweep in Cell Search Mode)
Roaming Hand-over

Station …

– First retrieves buffered frames from current Access-Point
– Then re-associates with new Access-Point

Access Point …

– Uses Inter Access Point Protocol (IAPP)
  • over the Distribution System that connects the APs
  • to inform old Access-Point of the event and allow it to change the association table
  • to update filter tables in intermediate bridges
  • IAPP uses UDP/IP, so works over routers, but ..... 

  *roaming over routers* requires Mobile IP
– Old Access-Point dumps (remaining) buffered frames for STA
Roaming and IAPP

IAPP protocol elements:

- WMP (WaveLAN Management Protocol) Station Announce
  - one-directional protocol to signal a re-association of a mobile station

- Announce Protocol
  - Protocol used by an AP to identify itself to other APs and to obtain information on other APs in the same area

- Hand-over Protocol
  - bi-directional message exchange between AP’s when initiated when a mobile station re-associates
At hand-over, a message is sent from new AP to old AP, using the MAC address of the mobile station as Source Address.

Causes bridges and switches in between the two APs to learn that the mobile station has changed location and these bridges will update their tables accordingly.

Some switches may act differently and reflect the movement of the mobile station as an address violation.
1. At startup AP transmits a so-called "Announce request" (IP Multicast Destination Address) using defined UDP/IP group addressing.

2. APs that are part of the same network and are already operational will respond with a so-called "Announce response", containing:
   - IP address of the replying AP
   - BSSID of the replying AP
3. The new AP uses the data in the reply to build a BSSID-to-IP conversion table to relate the BSSID, (used by the roaming station to identify its "old" AP) to the IP address of the "old" AP

   Future implementations will carry information, such as
   • the name of the AP, to be used to identify APs in the "Site Monitor" display
   • authorization information regarding the mobile station in case a centrally based Authentication scheme is used.
4. After an appropriate time interval, when all responses are received, the "new" AP will issue an "Announce response" to indicate its operational status.
   - The "new" AP will (as will all APs) re-issue the "Announce response" to keep informing all participating APs about any changes in the status.
IEEE 802.11

1. Re-association Request
2. Re-association Response

IEEE 802.11 Hand-over Protocol

New AP

3. Handover Request
4. Handover Response

IAPP

Old AP

Mobile station

Re-association Response
1. When the mobile station moves away from its "old" AP, it issues a **Re-associate Request** to a "new" AP,

2. The "new" AP will return a **Re-association Response** when it accepts the roaming station. The AP service for the mobile station starts at this point in time

3. The "new" AP sends a **Hand-over Request** to the old AP (via the Distribution System). IP address of old AP is determined based on BSSID carried in the Re-association Request

4. When the **Hand-over Response** received, the hand-over is considered to be completed.
Mobility and Existing Networks
Roaming over Routers

- Mobility has more impact, since MAC level learning is not sufficient
  - Station changes NETWORK ADDRESS because Sub-net changes
- Moving STAs translates to continuously changing network topology
- Two provisions are required:
  - hand-over messages need to be IP messages
  - “Mobile” IP must be in place
- Mobile IP is not a single standard and still in progress
  - various Internet Drafts
Mobility and Existing Networks

Routed LANs

Routed LANs / Mobile IP

- Home Agent
- Server
- Foreign Agent
- AP
- Router
- STA=
  Mobile Node
Mobility and Existing Networks

Routed LANs

**Routed LANs / Mobile IP**

- Station registers at Foreign Agent
- Foreign Agent informs Home Agent
- Traffic **TO** station flows via Home Agent and Foreign Agent
  - several “encapsulation” techniques are defined
  - optimization via “REDIRECT” warning to Correspondent Node (Server)
- Traffic **FROM** station is routed directly
Module Contents

- Scan
- Sweep
- Association
- Authentication
- Roaming
RF Interference
Module Contents

- The ISM Band
- Sources of interference
- Methods to coexist
The ISM Band

- Dedicated band made available for radio LANs
- Industrial, Scientific and Medical band: 2400 - 2483.5 MHz
- Set aside under ETSI (EMEA), FCC (USA), MKK (Japan)
- Each country endorses band (local type approval)
- Regulatory body can help out in case of “Illegal users”
The ISM Band 2400 - 2483.5 MHz
ISM Band Mix

- Microwave Ovens & other Industrial, Scientific equipment
- 1 Watt leakage
- Wireless LANs, WANs all ISM bands @ 100 mWatt
- Government & Military radio links
Module Contents

• The ISM Band

• Sources of interference

• Methods to coexist
Sources of Interference

- Microwave ovens
- Other wireless systems
- Electrical devices
- Passive systems
Sources of Interference
Microwave oven

Data from NTIA Report 94-303-1 US department of Commerce
Sources of Interference
Microwave Oven - Example of Spectrum Used

Data from NTIA Report 94-303-1 US department of Commerce
Sources of Interference
Microwave Oven - Operational Distances

Errorless Performance:

$d_1 = 2.1 \times d_2$ Worst Oven
$d_1 = 0.6 \times d_2$ Average Oven
$d_1 = 0.35 \times d_2$ Best Case Oven
Sources of Interference
Time Domain Emission of Microwave Oven

- Microwave oven uses on/off cycle
- Off cycle could be used to get wireless transmissions through
- Depending on the power cycle (50 or 60 Hz), the “off time” equals to 10 or 8.3 msec
- Transmitting a max size packet (1500 bytes) takes app.:
  - 12.5 msec @1 Mbps
  - 6.2 msec @2 Mbps
  - 2.3 msec @5.5 Mbps
  - 1.1 msec @11 Mbps

Data from NTIA Report 94-303-1 US department of Commerce
Sources of Interference
Microwave Oven Robustness

- Under normal operational settings, the Proxim PC Card will fall back in speed after two successive lost ACKs (which can happen as result of interference)
- If the Microwave Oven is the source of the interference, it would mean that the situation gets worse (lower speed means less chance to hit the off-cycle)
- Selecting “Microwave Oven Robustness” avoids falling back in speed too quickly and never drops to 1 Mbps

Example of Proxim PC Card
Sources of Interference

Other Wireless Systems

• Other ISM systems
  – Wireless LANs (FH and DS) typically use low power if adhere to regulations

• Other (unknown users)
  – Office buildings with more than company
  – May need coordination between IT staffs of companies that are interfering

• Non-ISM systems
  – High powered devices
  – May need arbitration from regulatory authorities
Sources of Interference

Electrical Devices

• Indoor:
  – Elevator motors
  – Overhead cranes with heavy spiking electric motors
  – Welding equipment

• Outdoor elements
  – Power lines
  – Electrical railroad track
  – Power stations
Sources of Interference

Passive Systems

Passive systems

• Indoor
  – walls that contain metal
  – cabinets
  – metal desks

• Outdoor
  – Structures, buildings etc
  – Moving objects: aircraft, cranes, vehicles
Module Contents

- The ISM Band
- Sources of interference
- Methods to coexist
Methods to Coexist
Access Point and Station Deployment

• Proper site survey to identify potential sources of interference

• Proper positions of the Radio systems as far away from potential sources of interference

• Deploy additional (redundant systems) Radios

• Advise mobile users to stay clear from sources of interference, when roaming
Methods to Coexist

Channel Choice

• Based on site analysis choose channels away from frequency used by source of interference

• “Tune around source of interference”
Methods to Coexist

Environmental Control

- Shield the source of interference
- Change the source of interference (re-tuning to be out of the band)
- Shield the Radio systems to be less effected by source of interference
Methods to Coexist
Coexistence of FH and DS

- FH and DS systems experience each other’s traffic as noise
- Generally DS systems suffer more from FH systems than vice versa
  - FH systems “hop” around DS systems
  - DS systems establish on a given channel (can only tune around a static source of interference; FH system represent a moving source of interference)
- Interference can be significant depending on
  - respective locations (near/far situations)
  - respective output power levels
  - amount of traffic generated on the FH system
  - the dwell time of the hopper (fast hoppers create less impact that slow ones)
  - Number of co-located FH “channels”
Methods to Coexist
Coexistence of FH and DS

Co-existence of Radios
- Per 1.6 second, 11 noise spikes can be expected, that may interfere with the channel, based on following parameters:
  - dwell time is 20 msec
  - hop sequence uses 80 frequencies
  - width of the frequency channel is 11 MHz
  - there is data traffic between the stations
- Spike is narrow (1 MHz)
- Spike lasts for 20 msec
Methods to Coexist
Coexistence of FH and DS - Test Set-up

Test set-up

Access Point

Cross-over cable

Server

Bridge Master

Notebook

Bridge Slave

Hub

Station (1)

Station (2)

14 meter

1 meter

3 meter

2 meter
Module Summary

• The ISM Band

• Sources of interference

• Methods to coexist