

Nomadic Communications Labs



Alessandro Villani
avillani@science.unitn.it



Configuration of CISCO AP 1200 Series

AP 1200: Features

□ This AP supports:

- Multiple SSID (up to 16). For each one it is possible to choose:
 - If transmitting in broadcast the SSID (guests mode)
 - The method of authentication
 - The maximum number of customers
 - VLAN: a VLAN for each SSID
- Authentication Methods:
 - MAC Address
 - 802.1x
 - WPA

AP 1200: Initial Configuration

- Configuration using serial port
 - 9600 baud
 - 8 data bits
 - Parity none
 - stop bit 1
 - flow control no

AP 1200: Initial Configuration

□ “Standard” CISCO commands:

- enable
- *Password* → Cisco
- `configure [terminal]`
- `ip default-gateway 192.168.10.1`
- `interface BVI 1`
- `ip address 192.168.10.40 255.255.255.0`
- exit
- Ctrl-z
- `copy running-config startup-config`
- reload

AP 1200: Initial Configuration

- To display the initial configuration:
 - Enable
 - Password: Cisco
 - `show running-config`

AP 1200: WEB Interface

- After the first configuration via CLI:

| |
|----------------------|
| HOME |
| EXPRESS SET-UP |
| SECURITY |
| NETWORK MAP + |
| ASSOCIATION + |
| NETWORK INTERFACES + |
| SECURITY + |
| SERVICES + |
| WIRELESS SERVICES + |
| SYSTEM SOFTWARE + |
| EVENT LOG + |

Hostname CISCO1200-NetworkLab

Express Set-Up

| | |
|--------------------------------|---|
| Host Name: | <input type="text" value="CISCO1200-NetworkLab"/> |
| MAC Address: | 000d.2967.cef5 |
| Configuration Server Protocol: | <input type="radio"/> DHCP <input checked="" type="radio"/> Static IP |
| IP Address: | <input type="text" value="192.168.10.40"/> |
| IP Subnet Mask: | <input type="text" value="255.255.255.0"/> |
| Default Gateway: | <input type="text" value="192.168.10.1"/> |
| SNMP Community: | <input type="text" value="defaultCommunity"/> |
| | <input checked="" type="radio"/> Read-Only <input type="radio"/> Read-Write |

Radio0-802.11B

| | |
|-----------------------------|--|
| Role in Radio Network: | <input checked="" type="radio"/> Access Point Root <input type="radio"/> Repeater Non-Root |
| Optimize Radio Network for: | <input checked="" type="radio"/> Throughput <input type="radio"/> Range <input type="radio"/> Custom |
| Aironet Extensions: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |

AP 1200: Firmware Update

- The Firmware is downloadable from the CISCO WEB Site:
 - <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243>
 - You have to register at least as guest user
 - The current version is: c1200-k9w7-tar.123-8.JEC2.tar
 - The AP firmware can be updated via tftp or via http

AP 1200: Wireless Configuration

- Role in a Wireless Network:
 - Root/Repeater
- Power:
 - You can limit the power of the AP radio
 - It is also possible to limit the power (in transmission) of the client stations (CISCO extensions)

AP 1200: Wireless Configuration

□ Speed:

- Basic (Require in WEB Interface): unicast and multicast traffic, used from the highest to the lowest. At least one rate must be set to basic. Note that if the client doesn't support a Basic rate, it can not associate to the AP
- Enabled: Unicast traffic only
- Disabled: This speed is not usable

AP 1200: Wireless Configuration

□ Configuration of the basic parameters

Hostname CISCO1200-NetworkLab CISCO1200-NetworkLab uptime is 3

Network Interfaces: Radio0-802.11B Settings

Enable Radio: Enable Disable

Current Status (Software/Hardware): Enabled ↑ Up ↑

Role in Radio Network: Access Point Root (Fallback to Radio Island)
(Fallback mode upon loss of Ethernet connection)
 Access Point Root (Fallback to Radio Shutdown)
 Access Point Root (Fallback to Repeater)
 Repeater Non-Root

Data Rates: Best Range Best Throughput

| | | | |
|------------|--|------------------------------|-------------------------------|
| 1.0Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |
| 2.0Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |
| 5.5Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |
| 11.0Mb/sec | <input checked="" type="radio"/> Require | <input type="radio"/> Enable | <input type="radio"/> Disable |

Transmitter Power (mW): 1 5 20 30 50 Max [Power Translation Table \(mW/dBm\)](#)

Limit Client Power (mW): 1 5 20 30 50 Max

Default Radio Channel: Least Congested Frequency Channel 10 2457 MHz

Least Congested Channel Search: (Use Only Selected Channels)

- Channel 1 - 2412 MHz
- Channel 2 - 2417 MHz
- Channel 3 - 2422 MHz
- Channel 4 - 2427 MHz
- Channel 5 - 2432 MHz
- Channel 6 - 2437 MHz
- Channel 7 - 2442 MHz
- Channel 8 - 2447 MHz
- Channel 9 - 2452 MHz
- Channel 10 - 2457 MHz

AP 1200: Wireless Configuration

□ World Mode:

- Clients can receive “national” information about setting. Legacy for CISCO compatibility, 802.11d new standards

□ Antenna:

- Diversity: both antennas are used and the one that receives the best signal is chosen

□ Encapsulation:

- To manage the non 802.3 packages, these have to be encapsulated. Interoperability with others: RFC1042; 802.1H optimized for CISCO

AP 1200: Wireless Configuration

□ RTS:

- Choose low values if not all of the stations are within sensing range of each other

□ Fragmentation:

- Choose low values if the area is disturbed or with low transmission quality

□ CISCO Extension:

- Used to support special features

AP 1200: Wireless Configuration

□ Configuration of the basic parameters

| | | | |
|---|---|--|--|
| World Mode Multi-Domain Operation: | <input type="radio"/> Disable | <input type="radio"/> Legacy | <input checked="" type="radio"/> Dot11d |
| Country Code: | <input type="text" value="Italy"/> <input checked="" type="checkbox"/> Indoor <input checked="" type="checkbox"/> Outdoor | | |
| Radio Preamble | <input checked="" type="radio"/> Short | <input type="radio"/> Long | |
| Receive Antenna: | <input checked="" type="radio"/> Diversity | <input type="radio"/> Left (Secondary) | <input type="radio"/> Right (Primary) |
| Transmit Antenna: | <input checked="" type="radio"/> Diversity | <input type="radio"/> Left (Secondary) | <input type="radio"/> Right (Primary) |
| External Antenna Configuration: | <input type="radio"/> Enable | <input checked="" type="radio"/> Disable | |
| | Antenna Gain(dB): <input type="text" value="DISABLED"/> (-128 - 128) | | |
| Aironet Extensions: | <input checked="" type="radio"/> Enable | <input type="radio"/> Disable | |
| Ethernet Encapsulation Transform: | <input checked="" type="radio"/> RFC1042 | <input type="radio"/> 802.1H | |
| Reliable Multicast to WGB: | <input checked="" type="radio"/> Disable | <input type="radio"/> Enable | |
| Public Secure Packet Forwarding: | <input type="radio"/> Enable | <input checked="" type="radio"/> Disable | |
| Beacon Period: | <input type="text" value="100"/> (20-4000 Kusec) | Data Beacon Rate (DTIM): | <input type="text" value="2"/> (1-100) |
| Max. Data Retries: | <input type="text" value="64"/> (1-128) | RTS Max. Retries: | <input type="text" value="64"/> (1-128) |
| Fragmentation Threshold: | <input type="text" value="2346"/> (256-2346) | RTS Threshold: | <input type="text" value="2312"/> (0-2347) |
| Repeater Parent AP Timeout: | <input type="text" value="0"/> (0-65535 sec) | | |
| Repeater Parent AP MAC 1 (optional): | <input type="text"/> (HHHH.HHHH.HHHH) | | |
| Repeater Parent AP MAC 2 (optional): | <input type="text"/> (HHHH.HHHH.HHHH) | | |
| Repeater Parent AP MAC 3 (optional): | <input type="text"/> (HHHH.HHHH.HHHH) | | |
| Repeater Parent AP MAC 4 (optional): | <input type="text"/> (HHHH.HHHH.HHHH) | | |

AP 1200: Wireless Configuration

□ Channel Selection:

- It is possible to make the AP choose the channel automatically
- It is possible to set it manually
- It is possible to do a survey to determine the state of the channels in the area

The screenshot displays the configuration page for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point". The navigation menu on the left includes: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, IP Address, FastEthernet, Radio0-802.11B, Radio1-not installed, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area shows the "RADIO0-802.11B STATUS" tab selected. Below the navigation, there are tabs for "RADIO0-802.11B STATUS", "DETAILED STATUS", "SETTINGS", and "CARRIER BUSY TEST". The "CARRIER BUSY TEST" tab is active, showing a "Carrier Busy Test" section with a "Start" button. Below this is a "Carrier Busy Test Output" table with the following data:

| Frequency | Carrier Busy % |
|-----------|----------------|
| 2412 | 2 |
| 2417 | 2 |
| 2422 | 1 |
| 2427 | 0 |
| 2432 | 0 |
| 2437 | 0 |
| 2442 | 0 |
| 2447 | 0 |
| 2452 | 0 |
| 2457 | 0 |
| 2462 | 1 |
| 2467 | 1 |
| 2472 | 1 |

AP 1200: SSID and Authentication

□ SSID:

- You have to define an SSID. Default "tsunami"
- Guest SSID: is the SSID advertised

□ Authentications:

- Open: all the devices are allowed to authenticate with the AP
- Shared: there is an exchange of a message plain or encrypted. Unsafe
- EAP: the safest mode

□ Authentication based on MAC:

- Open authentication → "With MAC Authentication"

AP 1200: SSID and Authentication

□ Definition of Cryptography

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point". The hostname is "CISCO1200-NetworkLab" and the uptime is "2 days, 49 minutes". The page is divided into several sections:

- Security: Encryption Manager**
 - Set Encryption Mode and Keys for VLAN:** A dropdown menu is set to "3". A link "Define VLANs" is visible.
 - Encryption Modes**
 - None
 - WEP Encryption** (Mandatory) - Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC), Enable Per Packet Keying (PPK)
 - Cipher (WEP 128 bit)
 - Encryption Keys**

| | Transmit Key | Encryption Key (Hexadecimal) | Key Size |
|-------------------|----------------------------------|------------------------------|----------|
| Encryption Key 1: | <input checked="" type="radio"/> | ***** | 128 bit |
| Encryption Key 2: | <input type="radio"/> | | 128 bit |
| Encryption Key 3: | <input type="radio"/> | | 128 bit |
| Encryption Key 4: | <input type="radio"/> | | 128 bit |
 - Global Properties**
 - Broadcast Key Rotation Interval:** Disable Rotation, Enable Rotation with Interval: [DISABLED] (10-10000000 sec)
 - WPA Group Key Update:** Enable Group Key Update On Membership Termination, Enable Group Key Update On Member's Capability Change


At the bottom right, there are buttons for "Apply" and "Cancel".

AP 1200: Configuration via CLI

□ All the configurations via HTTP are possible via CLI

■ show running-config

```
interface Dot11Radio0
  no ip address
  no ip route-cache
  !
  encryption vlan 3 key 1 size 128bit 7 501B2057424875554B78965D207B
  transmit-key
  encryption vlan 3 mode wep mandatory
  !
  ssid CREATE-NET-TEST
    vlan 4
    authentication open mac-address mac_methods
    accounting acct_methods
    mobility network-id 4
    information-element ssid advertisement
  !
  ssid WILMA-LAB
    vlan 3
    authentication open mac-address mac_methods
    accounting acct_methods
    mobility network-id 3
    information-element ssid advertisement
  !
  ssid WILMA-LAB-TEST
    vlan 5
    authentication open mac-address mac_methods
    accounting acct_methods
    guest-mode
    mobility network-id 5
```



Configuration of LinkSys AP WAP54G

WAP54G: Firmware Update

- The Firmware is downloadable from the LinkSys WEB Site:
 - <http://www.linksysbycisco.com/US/en/support/WAP54G>
 - The AP firmware can be updated via http

WAP54G: WEB Interface

- We can configure it via WEB interface:

The screenshot displays the Linksys WAP54G web interface. The top header includes the Linksys logo, "A Division of Cisco Systems, Inc.", and the firmware version "v2.08, May 13, 2004, ETSI". The main navigation bar shows "Setup" as the active tab, with sub-tabs for "Status", "Advanced", and "Help". Below this, there are links for "Basic Setup", "Password", "AP Mode", and "Log".

The interface is divided into sections for configuration:

- Firmware Version:** v2.08, May 13, 2004, ETSI
- AP Name:** Linksys WAP54G
- LAN Section:**
 - Configuration Type:** Static IP Address
 - IP Address:** 192 . 168 . 10 . 15 (This is the IP address, Subnet Mask and Default)
 - Subnet Mask:** 255 . 255 . 255 . 0 (Gateway of the Access Point as it is seen by)
 - Gateway:** 192 . 168 . 10 . 1 (your local network.)
- Wireless Section:**
 - Mode:** Mixed
 - SSID:** NCL (SSID Broadcast: Enable)
 - Channel:** 1 (Regulatory Domain: Europe)
 - Wireless Security:** Enable Disable (Edit Security Settings)

At the bottom, there are buttons for "Save Settings", "Cancel Changes", and "Help". The Cisco Systems logo is visible in the bottom right corner.

WAP54G: WEB Interface

- From the main page you can change the B/G/mixed mode:

The screenshot displays the Linksys WAP54G web interface. The top navigation bar includes the Linksys logo, "A Division of Cisco Systems, Inc.", and "Firmware Version: 2.08". The main header shows "Wireless-G Access Point" and "WAP54G". The left sidebar has a "Setup" menu with sub-items: "Basic Setup", "Password", "AP Mode", and "Log". The "AP Mode" sub-item is selected.

The main content area is divided into sections: "Firmware Version" (v2.08, May 13, 2004, ETSI), "AP Name" (Linksys WAP54G), "LAN" configuration (Static IP Address, IP Address: 192.168.10.15, Subnet Mask: 255.255.255.0, Gateway: 192.168.10.1), and "Wireless" configuration. The "Wireless" section shows the MAC Address (00:0F:66:11:D2:C3) and the "Mode" dropdown menu, which is highlighted with a red circle. The "Mode" dropdown is currently set to "Mixed" and shows options for "Mixed", "G-Only", and "B-Only". Other settings include "SSID Broadcast" (Enable) and "Wireless Security" (Disable).

At the bottom of the page, there are buttons for "Save Settings", "Cancel Changes", and "Help". The Cisco Systems logo is visible in the bottom right corner.

WAP54G: WEB Interface

- In the Advanced page, Advanced Wireless tab, you can modify a lot of parameters:

The screenshot displays the Linksys WAP54G web interface. The top navigation bar includes the Linksys logo, "A Division of Cisco Systems, Inc.", and the firmware version "2.08". The main navigation area shows "Advanced" as the selected page, with sub-tabs for "Setup", "Status", "Advanced", and "Help". The "Advanced" sub-tab is further divided into "Filters", "Advanced Wireless", and "SNMP".

The "Advanced Wireless" configuration page lists the following parameters:

| Parameter | Value | Default | Range |
|-------------------------|-----------|-----------|------------|
| Authentication Type | Auto | Auto | |
| Transmission Rates | Auto | Auto | |
| CTS Protection Mode | Disable | Disable | |
| Basic Rates | Default | Default | |
| Antenna Selection | Diversity | Diversity | |
| Frame Burst | Off | off | |
| Beacon Interval | 100 | 100 | 20~1000 |
| RTS Threshold | 2346 | 2346 | 256 - 2346 |
| Fragmentation Threshold | 2346 | 2346 | 256 - 2346 |
| DTIM Interval | 3 | 3 | 1 - 255 |

At the bottom of the page, there are buttons for "Save Settings", "Cancel Changes", and "Help". The Cisco Systems logo is visible in the bottom right corner.

WAP54G: WEB Interface

- For this AP you can change:
 - The Fragmentation Threshold
 - The Transmitting speed
 - The RTS Threshold
 - The mode (B/G/Mixed)



WireShark (Previously ethereal)

WireShark

- ❑ WireShark is a network packet analyzer completely open source
- ❑ Available at the address:
<http://www.wireshark.org/>
- ❑ It can decode a lot of protocols, including:
 - IEEE 802.11 wireless LAN
 - Radius
 - 802.1x Authentication

WireShark: filtering when capturing

- A “capture filter” has the form of a series of primitive expressions connected by connections (**and/or**) and possibly preceded by a **not**:

[not] **primitive** [and|or [not]
primitive ...]

- For examples:

tcp port 23 and host 193.205.194.23

tcp port 23 and not host 193.205.194.23

WireShark: filtering when capturing

- ❑ **Some of the most used primitives:**
- ❑ **[src|dst] host <host>**
 - This primitive allows to filter on the basis of the IP address or the name of the host
- ❑ **ether [src|dst] host <ehost>**
 - This primitive allows to filter on the basis of the ethernet address of the host
- ❑ **[src|dst] net <net> [{mask <mask>}|{len <len>}]**
 - This primitive allows to filter on the basis of the network addresses
- ❑ **[tcp|udp] [src|dst] port <port>**
 - This primitive allows to filter on the basis of the TCP and UDP port numbers
- ❑ **ip|ether proto <protocol>**
 - This primitive allows to filter on the basis of the protocols specified at Ethernet or IP level



Promiscuous Mode and Monitor Mode

Promiscuous Mode

- ❑ To make *sniffing* on a network device it is required that the filter based on the MAC address in the destination field applied to the incoming packets is deactivated:
promiscuous mode
- ❑ In most cases the control is not hardcoded and therefore it is possible to disabled it acting on the driver

Monitor Mode

- ❑ For many 802.11 wireless cards, besides the *Promiscuous Mode*, it is possible to use another mode: the *Monitor Mode*
- ❑ This mode allows to make sniffing in a completely passive way: we can see all what is on the wireless channel without having to join to the WLAN (it is not possible to transmit, but the card can be used more efficiently for listening)
- ❑ The possibility of using a card in Monitor Mode depends on the driver

Monitor Mode

- A (not complete) list of cards, with the corresponding linux driver which support the Monitor Mode, is available at the address:

<http://www.kismetwireless.net/documentation.shtml>



802.11 Frames

802.11 Frame

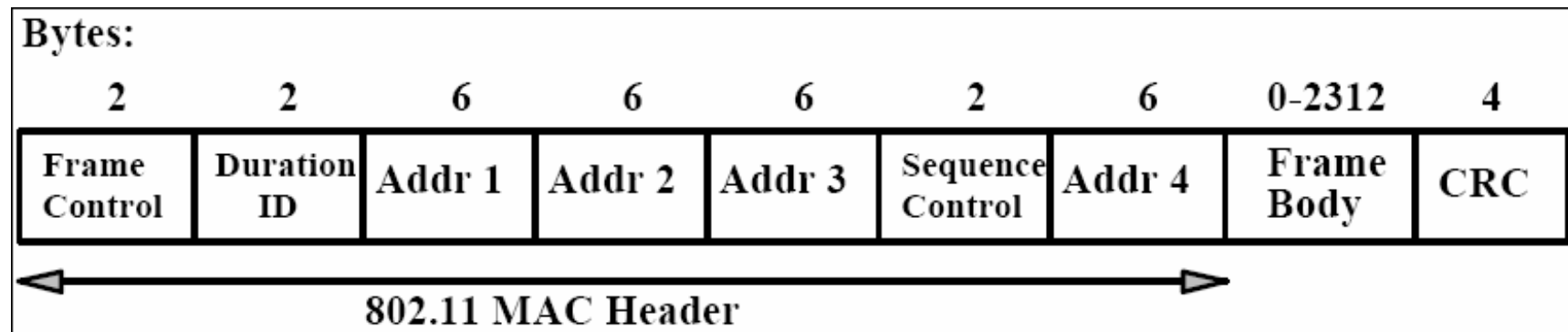
- ❑ The Monitor Mode (plus applications like WireShark or Kismet) allows us to analyze the frames of a 802.11 communication
- ❑ 802.11 defines several types of frame which stations (NIC and AP) use to communicate among them and to manage and check the wireless link

802.11 Frame

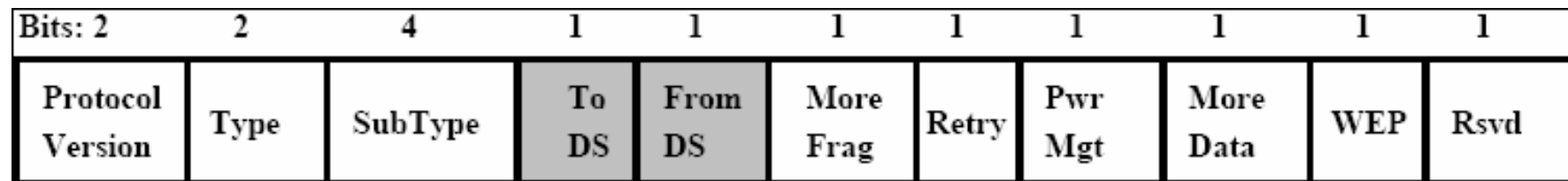
- ❑ Each frame has a control field that defines the version of the 802.11 protocol, the type of frame, and several flags like if WEP is active, if the management power is active, ...
- ❑ Every frame contains MAC addresses of the source and destination station, a frame number, the frame body and a frame check (for error control)

802.11 Frame

□ Frame format:



□ The Frame Control Field is:



Frame Control Field

802.11 Frame: Management

□ Management Frame

| Type Value | Type Description | Subtype Value | Subtype Description |
|------------|------------------|---------------|------------------------|
| 00 | Management | 0000 | Association Request |
| 00 | Management | 0001 | Association Response |
| 00 | Management | 0010 | Reassociation Request |
| 00 | Management | 0011 | Reassociation Response |
| 00 | Management | 0100 | Probe Request |
| 00 | Management | 0101 | Probe Response |
| 00 | Management | 0110-0111 | Reserved |
| 00 | Management | 1000 | Beacon |
| 00 | Management | 1001 | ATIM |
| 00 | Management | 1010 | Disassociation |
| 00 | Management | 1011 | Authentication |
| 00 | Management | 1100 | Deauthentication |
| 00 | Management | 1110-1111 | Reserved |

802.11 Frame: Control

□ Control Frame

| Type Value | Type Description | Subtype Value | Subtype Description |
|------------|------------------|---------------|---------------------|
| 01 | Control | 0000-1001 | Reserved |
| 01 | Control | 1010 | PS-Poll |
| 01 | Control | 1011 | RTS |
| 01 | Control | 1100 | CTS |
| 01 | Control | 1101 | ACK |
| 01 | Control | 1101 | CF End |
| 01 | Control | 1111 | CF End + CF-ACK |

802.11 Frame: Data

□ Data Frame

| Type Value | Type Description | Subtype Value | Subtype Description |
|------------|------------------|---------------|----------------------------|
| 10 | Data | 0000 | Data |
| 10 | Data | 0001 | Data + CF-Ack |
| 10 | Data | 0010 | Data + CF-Poll |
| 10 | Data | 0011 | Data + CF-ACK + CF-Poll |
| 10 | Data | 0100 | Null Function (no data) |
| 10 | Data | 0101 | CF-Ack (no data) |
| 10 | Data | 0110 | CF-Poll (no data) |
| 10 | Data | 0111 | CF-Ack + CF-Poll (no data) |
| 10 | Data | 1000-1111 | Reserved |

802.11 Frame: Management

- **Management Frames:** they allow to establish and keep the communications. For instance:
 - **Authentication Frame:** NIC begins the authentication process sending to the AP an *authentication frame* containing its identity:
 - Open system: NIC sends an authentication frame, and AP answers with an authentication frame containing the indication of success or failure
 - Shared key: NIC initially sends an authentication frame, and AP answers with an authentication frame containing a challenge. NIC must send an encrypted version of challenge (using the WEP key) in an authentication frame

802.11 Frame: Management

- **Deauthentication frame**
- **Association request frame:** Allows the AP to allocate resources for the NIC.
A NIC begins the association process sending an *association request frame* to an AP. This frame holds information about NIC (for instance the data rates supported) and the SSID of the WLAN it is associating
- **Association response frame:** An AP sends a *association response frame* containing a notification of acceptance or rejection of the NIC request of association. If AP accepts the NIC, the frame includes information like the association ID and the supported rates

802.11 Frame: Management

- **Beacon frame:** The AP periodically sends a *beacon frame* to announce his presence and send information, like timestamp, SSID, and other parameters regarding the AP itself
- **Probe request frame:** A station sends a *probe request frame* when it needs to obtain information from another station
- **Probe response frame:** A station will answer with a *probe response frame*, containing information like the supported speeds, after it has received a *probe request frame*

802.11 Frame: Control

- **Control Frames:** used in the delivery of frames data among the stations. For instance:
 - **Request to Send (RTS) frame**
 - **Clear to Send (CTS) frame**
 - **Acknowledgement (ACK) frame:** after the arrive of a data frame, the receiving station will use a error checking process and will send an *ACK frame* to the transmitting station if there are not mistakes. If the transmitting station does not receive an ACK after a certain time it will resend the data frame

802.11 Frame: Data

- **Data Frames:** The data frame contains inside the frame body the packets from the highest levels, as web pages, control information for the printers, ...,

802.11 Frame: Frame Control Field

□ **ToDS:**

- This bit is set to 1 when the frame goes to the AP for the forwarding to the DS (*Distribution System*)
- The bit is set to 0 in all other cases

□ **FromDS:**

- This bit is set to 1 when the frame is received from the DS
- The bit is set to 0 in all other cases, i.e., for frames that do not leave the BSS

802.11 Frame: Frame Control Field

□ **More Fragments:**

- This bit is to 1 when there are more fragments belonging to the same data packet following the current frame

□ **Retry:**

- This bit means that this frame is the retransmission of a frame previously transmitted. It is used by the receiving station to be aware of retransmission due to ACK loss

□ **Power Management:**

- This bit shows the Power Management behavior of the station after the transmission of this frame

802.11 Frame: Frame Control Field

□ **More Data:**

- This bit is used for the Power Management to specify that there are still frames for the station in the buffer. The station can decide to use the information to continue the polling or to switch in Active Mode.

□ **WEP:**

- This bit means that the frame body is encrypted with WEP

□ **Order:**

- This bit means that the frame is sent using a *Strictly-Ordered service class*

802.11 Frame: Frame Control Field

□ **Duration/ID:**

- This field has two meanings according to the type of frame :
 - In a Power-Save Poll message it corresponds to the Station ID
 - In all the other frames this is the duration used for the calculation of NAV

□ **Sequence Control:**

- This field is used to represent the order of various fragments belonging to the same packet and identify duplicate frames.
It consists of two subfields: *Fragment Number* and *Sequence Number*

Frame 802.11: Frame Control Field

□ **Address Fields:**

- A frame can contain up to 4 addresses based on the value of ToDS and FromDS bits:
 - **Address-1** it is always the receiver address.
If ToDS is set to 1 then it is the address of AP, otherwise it is the address of the final station
 - **Address-2** it is always the transmitter address.
If FromDS is set to 1 then it is the address of AP, otherwise it is the address of the final station
 - **Address-3** If FromDS is set to 1, Address-3 is the original source address, if ToDS is set to 1 then Address 3 is the destination address, otherwise it is the address of the AP in IBSS
 - **Address-4** is used when a Wireless Distribution System is used and the frame is transmitted by an AP to another

802.11 Frame: MAC Header

□ Address Fields:

| To DS | From DS | Address 1 | Address 2 | Address 3 | Address 4 |
|-------|---------|-----------|-----------|-----------|-----------|
| 0 | 0 | DA | SA | BSSID | N/A |
| 0 | 1 | DA | BSSID | SA | N/A |
| 1 | 0 | BSSID | SA | DA | N/A |
| 1 | 1 | RA | TA | DA | SA |

- **SA = Source MAC Address**
- **DA = Destination MAC Address**
- **TA = Transmitter MAC Address**
- **RA = Receiver MAC Address**
- **BSSID = AP MAC Address or Random MAC in Ad-Hoc**

802.11 Frame: Frame Format

- **CRC:** it is a field of 32-bits for the error checking, Cyclic Redundancy Check (CRC)



Beacon and Probe Frame

Beacon Frame – Part 1

```
Frame 1 (98 bytes on wire, 98 bytes captured)
  Arrival Time: Apr  7, 2005 23:30:17.202927000
  Time delta from previous packet: 0.000000000 seconds
  Time since reference or first frame: 0.000000000 seconds
  Frame Number: 1
  Packet Length: 98 bytes
  Capture Length: 98 bytes
  Protocols in frame: wlan
IEEE 802.11
  Type/Subtype: Beacon frame (8)
  Frame Control: 0x0080 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 8
    Flags: 0x0
      DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
From DS: 0) (0x00)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = Order flag: Not strictly ordered
  Duration: 0
  Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
  Source address: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  BSS Id: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  Fragment number: 0
  Sequence number: 1394
```

Beacon Frame – Parte 2

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Timestamp: 0x0000000007AC11AC

Beacon Interval: 0.102400 [Seconds]

Capability Information: 0x0021

....1 = ESS capabilities: Transmitter is an AP

....0. = IBSS status: Transmitter belongs to a BSS

.... 00.. = CFP participation capabilities: No point coordinator

at AP (0x0000)

....0 = Privacy: AP/STA cannot support WEP

....1. = Short Preamble: Short preamble allowed

....0.. = PBCC: PBCC modulation not allowed

.... 0... = Channel Agility: Channel agility not in use

.... .0.. = Short Slot Time: Short slot time not in use

..0. = DSSS-OFDM: DSSS-OFDM modulation not allowed

Tagged parameters (62 bytes)

Tag Number: 0 (SSID parameter set)

Tag length: 5

Tag interpretation: WILMA

Tag Number: 1 (Supported Rates)

Tag length: 4

Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) [Mbit/sec]

Beacon Frame – Part 3

Tag Number: 3 (DS Parameter set)

Tag length: 1

Tag interpretation: Current Channel: 13

Tag Number: 5 ((TIM) Traffic Indication Map)

TIM length: 4

DTIM count: 1

DTIM period: 2

Bitmap Control: 0x00 (mcast:0, bitmap offset 0)

Tag Number: 7 (Country Information)

Tag length: 6

Tag interpretation: Country Code: EU, Unknown (0x00) Environment, Start Channel: 1, Channels: 13, Max TX Power: 50 dBm

Tag Number: 133 (Cisco Unknown 1 + Device Name)

Tag length: 30

Tag interpretation: Unknown + Name: Cisco 350 - VVM

Probe Request – Part 1

```
Frame 2 (37 bytes on wire, 37 bytes captured)
  Arrival Time: Apr  7, 2005 23:30:17.272964000
  Time delta from previous packet: 0.070037000 seconds
  Time since reference or first frame: 0.070037000 seconds
  Frame Number: 2
  Packet Length: 37 bytes
  Capture Length: 37 bytes
  Protocols in frame: wlan
IEEE 802.11
  Type/Subtype: Probe Request (4)
  Frame Control: 0x0040 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 4
    Flags: 0x0
      DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
From DS: 0) (0x00)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = Order flag: Not strictly ordered
  Duration: 0
  Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
  Source address: 00:0b:cd:8d:30:3b (172.31.194.10)
  BSS Id: ff:ff:ff:ff:ff:ff (Broadcast)
  Fragment number: 0
  Sequence number: 2
```


Probe Request – Part 2

IEEE 802.11 wireless LAN management frame

Tagged parameters (13 bytes)

Tag Number: 0 (SSID parameter set)

Tag length: 5

Tag interpretation: WILMA

Tag Number: 1 (Supported Rates)

Tag length: 4

Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 [Mbit/sec]

Probe Response – Part 1

```
Frame 4 (84 bytes on wire, 84 bytes captured)
  Arrival Time: Apr  7, 2005 23:30:17.281343000
  Time delta from previous packet: 0.001169000 seconds
  Time since reference or first frame: 0.078416000 seconds
  Frame Number: 4
  Packet Length: 84 bytes
  Capture Length: 84 bytes
  Protocols in frame: wlan
IEEE 802.11
  Type/Subtype: Probe Response (5)
  Frame Control: 0x0050 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 5
    Flags: 0x0
      DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
From DS: 0) (0x00)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = Order flag: Not strictly ordered
  Duration: 314
  Destination address: 00:0b:cd:8d:30:3b (172.31.194.10)
  Source address: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  BSS Id: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  Fragment number: 0
  Sequence number: 1397
```

Probe Response – Part 2

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Timestamp: 0x0000000007AD44C3

Beacon Interval: 0.102400 [Seconds]

Capability Information: 0x0021

.... ..1 = ESS capabilities: Transmitter is an AP

.... ..0. = IBSS status: Transmitter belongs to a BSS

.... ..00.. = CFP participation capabilities: No point coordinator

at AP (0x0000)

.... ..0 = Privacy: AP/STA cannot support WEP

.... ..1. = Short Preamble: Short preamble allowed

.... ..0.. = PBCC: PBCC modulation not allowed

.... ..0... = Channel Agility: Channel agility not in use

.... ..0.. = Short Slot Time: Short slot time not in use

..0. = DSSS-OFDM: DSSS-OFDM modulation not allowed

Tagged parameters (48 bytes)

Tag Number: 0 (SSID parameter set)

Tag length: 5

Tag interpretation: WILMA

Tag Number: 1 (Supported Rates)

Tag length: 4

Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) [Mbit/sec]

Tag Number: 3 (DS Parameter set)

Tag length: 1

Tag interpretation: Current Channel: 13

Tag Number: 133 (Cisco Unknown 1 + Device Name)

Tag length: 30

Tag interpretation: Unknown + Name: Cisco 350 - VVM



Authentication

Authentication Request – Part 1

```
Frame 10 (30 bytes on wire, 30 bytes captured)
  Arrival Time: Apr  7, 2005 23:30:17.510590000
  Time delta from previous packet: 0.000479000 seconds
  Time since reference or first frame: 0.307663000 seconds
  Frame Number: 10
  Packet Length: 30 bytes
  Capture Length: 30 bytes
  Protocols in frame: wlan
IEEE 802.11
  Type/Subtype: Authentication (11)
  Frame Control: 0x00B0 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 11
    Flags: 0x0
      DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
From DS: 0) (0x00)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = Order flag: Not strictly ordered
  Duration: 258
  Destination address: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  Source address: 00:0b:cd:8d:30:3b (172.31.194.10)
  BSS Id: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  Fragment number: 0
  Sequence number: 13
```

Authentication Request – Part 2

IEEE 802.11 wireless LAN management frame

Fixed parameters (6 bytes)

Authentication Algorithm: Open System (0)

Authentication SEQ: 0x0001

Status code: Successful (0x0000)

Authentication Replay – Part 1

```
Frame 11 (30 bytes on wire, 30 bytes captured)
  Arrival Time: Apr  7, 2005 23:30:17.513426000
  Time delta from previous packet: 0.002836000 seconds
  Time since reference or first frame: 0.310499000 seconds
  Frame Number: 11
  Packet Length: 30 bytes
  Capture Length: 30 bytes
  Protocols in frame: wlan
IEEE 802.11
  Type/Subtype: Authentication (11)
  Frame Control: 0x00B0 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 11
    Flags: 0x0
      DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
From DS: 0) (0x00)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = Order flag: Not strictly ordered
  Duration: 258
  Destination address: 00:0b:cd:8d:30:3b (172.31.194.10)
  Source address: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  BSS Id: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  Fragment number: 0
  Sequence number: 1403
```

Authentication Replay – Part 2

IEEE 802.11 wireless LAN management frame

Fixed parameters (6 bytes)

Authentication Algorithm: Open System (0)

Authentication SEQ: 0x0002

Status code: Successful (0x0000)



Association

Association Request – Part 1

```
Frame 12 (41 bytes on wire, 41 bytes captured)
  Arrival Time: Apr  7, 2005 23:30:17.514662000
  Time delta from previous packet: 0.001236000 seconds
  Time since reference or first frame: 0.311735000 seconds
  Frame Number: 12
  Packet Length: 41 bytes
  Capture Length: 41 bytes
  Protocols in frame: wlan
IEEE 802.11
  Type/Subtype: Association Request (0)
  Frame Control: 0x0000 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 0
    Flags: 0x0
      DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
From DS: 0) (0x00)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = Order flag: Not strictly ordered
  Duration: 258
  Destination address: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  Source address: 00:0b:cd:8d:30:3b (172.31.194.10)
  BSS Id: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  Fragment number: 0
  Sequence number: 14
```

Association Request – Part 2

IEEE 802.11 wireless LAN management frame

Fixed parameters (4 bytes)

Capability Information: 0x0001

....1 = ESS capabilities: Transmitter is an AP

....0. = IBSS status: Transmitter belongs to a BSS

.... 00.. = CFP participation capabilities: No point coordinator

at AP (0x0000)

....0 = Privacy: AP/STA cannot support WEP

....0. = Short Preamble: Short preamble not allowed

....0.. = PBCC: PBCC modulation not allowed

.... 0... = Channel Agility: Channel agility not in use

.... .0.. = Short Slot Time: Short slot time not in use

..0. = DSSS-OFDM: DSSS-OFDM modulation not allowed

Listen Interval: 0x0001

Tagged parameters (13 bytes)

Tag Number: 0 (SSID parameter set)

Tag length: 5

Tag interpretation: WILMA

Tag Number: 1 (Supported Rates)

Tag length: 4

Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 [Mbit/sec]

Association Response – Part 1

```
Frame 13 (36 bytes on wire, 36 bytes captured)
  Arrival Time: Apr  7, 2005 23:30:17.517303000
  Time delta from previous packet: 0.002641000 seconds
  Time since reference or first frame: 0.314376000 seconds
  Frame Number: 13
  Packet Length: 36 bytes
  Capture Length: 36 bytes
  Protocols in frame: wlan
IEEE 802.11
  Type/Subtype: Association Response (1)
  Frame Control: 0x0010 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 1
    Flags: 0x0
      DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
From DS: 0) (0x00)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = Order flag: Not strictly ordered
  Duration: 213
  Destination address: 00:0b:cd:8d:30:3b (172.31.194.10)
  Source address: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  BSS Id: 00:40:96:5e:0d:64 (AironetW_5e:0d:64)
  Fragment number: 0
  Sequence number: 1404
```

Association Response – Part 2

IEEE 802.11 wireless LAN management frame

Fixed parameters (6 bytes)

Capability Information: 0x0001

....1 = ESS capabilities: Transmitter is an AP

....0. = IBSS status: Transmitter belongs to a BSS

.... 00.. = CFP participation capabilities: No point coordinator

at AP (0x0000)

....0 = Privacy: AP/STA cannot support WEP

....0. = Short Preamble: Short preamble not allowed

....0.. = PBCC: PBCC modulation not allowed

.... 0... = Channel Agility: Channel agility not in use

.... .0.. = Short Slot Time: Short slot time not in use

..0. = DSSS-OFDM: DSSS-OFDM modulation not allowed

Status code: Successful (0x0000)

Association ID: 0x001d

Tagged parameters (6 bytes)

Tag Number: 1 (Supported Rates)

Tag length: 4

Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) [Mbit/sec]



Data Frames

Data Frame (ARP) – Part 1

```
Frame 693 (78 bytes on wire, 78 bytes captured)
  Arrival Time: May 12, 2004 19:48:17.767774000
  Time delta from previous packet: 0.006368000 seconds
  Time since reference or first frame: 32.158984000 seconds
  Frame Number: 693
  Packet Length: 78 bytes
  Capture Length: 78 bytes
IEEE 802.11
  Type/Subtype: Data (32)
  Frame Control: 0x0208 (Normal)
    Version: 0
    Type: Data frame (2)
    Subtype: 0
    Flags: 0x2
      DS status: Frame is exiting DS (To DS: 0 From DS: 1) (0x02)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = Order flag: Not strictly ordered
    Duration: 0
  Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
  BSS Id: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
  Source address: 00:00:cd:03:fe:7e (193.205.213.1)
  Fragment number: 0
  Sequence number: 4002
Logical-Link Control
```

Data Frame (ARP) – Part 2

Address Resolution Protocol (request)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (0x0001)

Sender MAC address: 00:00:cd:03:fe:7e (193.205.213.1)

Sender IP address: 193.205.213.1 (193.205.213.1)

Target MAC address: ff:ff:ff:ff:ff:ff (Broadcast)

Target IP address: 193.205.213.177 (193.205.213.177)

Data Frame (Http) – Part 1

```
Frame 1830 (510 bytes on wire, 510 bytes captured)
  Arrival Time: May 12, 2004 19:49:14.356290000
  Time delta from previous packet: 0.001401000 seconds
  Time since reference or first frame: 88.747500000 seconds
  Frame Number: 1830
  Packet Length: 510 bytes
  Capture Length: 510 bytes
IEEE 802.11
  Type/Subtype: Data (32)
  Frame Control: 0x0108 (Normal)
    Version: 0
    Type: Data frame (2)
    Subtype: 0
    Flags: 0x1
      DS status: Frame is entering DS (To DS: 1 From DS: 0) (0x01)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = Order flag: Not strictly ordered
    Duration: 258
    BSS Id: 00:20:a6:50:da:c1 (Proxim_50:da:c1)
    Source address: 00:0b:cd:8d:30:3b (CompaqHp_8d:30:3b)
    Destination address: 00:00:cd:03:fe:7e (193.205.213.1)
    Fragment number: 0
    Sequence number: 2078
Logical-Link Control
```

Data Frame (Http) – Part 2

```
Internet Protocol, Src Addr: 192.168.213.24 (192.168.213.24), Dst Addr: 193.205.213.166
(193.205.213.166)
Transmission Control Protocol, Src Port: 3346 (3346), Dst Port: 3128 (3128), Seq: 1,
Ack: 1, Len: 438
Hypertext Transfer Protocol
GET http://www.google.it/ HTTP/1.0\r\n
    Request Method: GET
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-
excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-
flash, */*\r\n
Accept-Language: en-gb\r\n
Cookie:
    PREF=ID=3e55d6d171be104c:LD=it:TM=1070627809:LM=1070627809:S=PTw_56YWtiEG1MLL\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\n
Host: www.google.it\r\n
Proxy-Connection: Keep-Alive\r\n
\r\n
```

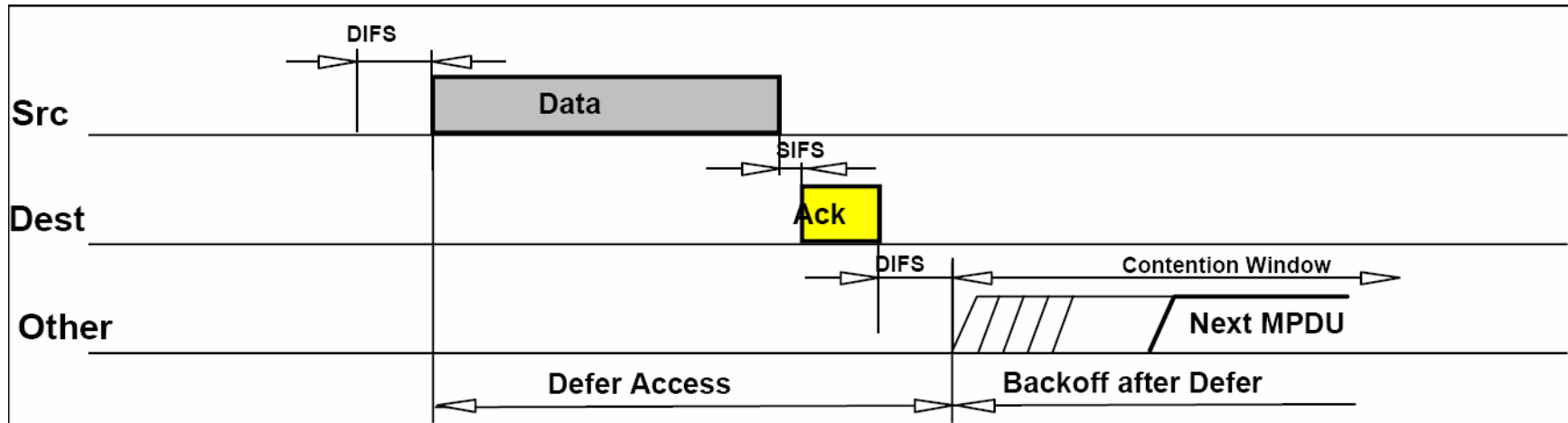


Acknowledgment

Control Frame: ACK

- ❑ All the unicast traffic frames must receive an ACK frame
- ❑ A *data frame* will use NAV to reserve the channel for the *data frame*, his ACK and SIFS (Short Inter Frame Space)
- ❑ With this NAV, the sender ensures to the receiver of the data frame the possibility of sending ACK

Control Frame: ACK



Data Frame: HTTP – Part 1

```
Frame 1 (286 bytes on wire, 286 bytes captured)
  Arrival Time: Apr  8, 2005 10:04:58.768578000
  Time delta from previous packet: 0.000000000 seconds
  Time since reference or first frame: 0.000000000 seconds
  Frame Number: 1
  Packet Length: 286 bytes
  Capture Length: 286 bytes
  Protocols in frame: wlan:llc:ip:tcp:http
IEEE 802.11
  Type/Subtype: Data (32)
  Frame Control: 0x0108 (Normal)
    Version: 0
    Type: Data frame (2)
    Subtype: 0
    Flags: 0x1
      DS status: Frame is entering DS (To DS: 1 From DS: 0) (0x01)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = Order flag: Not strictly ordered
  Duration: 213
  BSS Id: 00:20:a6:50:da:ca (Proxim_50:da:ca)
  Source address: 00:0b:cd:8d:30:3b (CompaqHp_8d:30:3b)
  Destination address: 00:0b:db:73:2b:16 (DellEsgP_73:2b:16)
```

Data Frame: HTTP – Part 2

Fragment number: 0

Sequence number: 2505

Logical-Link Control

Internet Protocol, Src Addr: 172.31.194.10 (172.31.194.10), Dst Addr: 193.205.213.166 (193.205.213.166)

Transmission Control Protocol, Src Port: 3072 (3072), Dst Port: 3128 (3128), Seq: 0, Ack: 0, Len: 214

Source port: 3072 (3072)

Destination port: 3128 (3128)

Sequence number: 0 (relative sequence number)

Next sequence number: 214 (relative sequence number)

Acknowledgement number: 0 (relative ack number)

Header length: 20 bytes

Flags: 0x0018 (PSH, ACK)

Window size: 17047

Checksum: 0xf08e (correct)

Hypertext Transfer Protocol

GET http://www.unitn.it/scienze/ HTTP/1.0\r\n

Accept: */*\r\n

Accept-Language: en-gb\r\n

Pragma: no-cache\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\n

Host: www.unitn.it\r\n

Proxy-Connection: Keep-Alive\r\n

\r\n

ACK Frame

Frame 2 (10 bytes on wire, 10 bytes captured)

Arrival Time: Apr 8, 2005 10:04:58.768639000

Time delta from previous packet: 0.000061000 seconds

Time since reference or first frame: 0.000061000 seconds

Frame Number: 2

Packet Length: 10 bytes

Capture Length: 10 bytes

Protocols in frame: wlan

IEEE 802.11

Type/Subtype: [Acknowledgement \(29\)](#)

Frame Control: 0x00D4 (Normal)

Version: 0

Type: Control frame (1)

Subtype: 13

Flags: 0x0

DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
From DS: 0) (0x00)

.... .0.. = More Fragments: This is the last fragment

.... 0... = Retry: Frame is not being retransmitted

...0 = PWR MGT: STA will stay up

..0. = More Data: No data buffered

.0.. = WEP flag: WEP is disabled

0... = Order flag: Not strictly ordered

Duration: 0

Receiver address: 00:0b:cd:8d:30:3b (CompaqHp_8d:30:3b)



Analysis of 802.11 Packets

BackTrack

- We will use a Linux Live distribution: BackTrack
 - <http://www.remote-exploit.org/backtrack.html>
- It has all the tools we need for wireless sniffing and monitoring, and we don't need to install any program on the laptop or ask for root passwd

BackTrack: Startup

- ❑ Currently we can use two different versions: *V3.0 Final* or *V:4.0 Beta*
- ❑ For *Version 3.0 Final*
 - Boot from CD (`BT3 Graphics mode`)
- ❑ For *Version 4.0 Beta*
 - Boot from DVD (`Text mode`)
 - Login as root:
 - ❑ Login: `root`
 - ❑ Password: `toor`
 - Start the graphics mode:
 - ❑ `startx`

BackTrack: iwconfig

- ❑ To get the Wireless Network Card parameters:

- iwconfig

- ❑ The result is something like:

```
eth0      IEEE 802.11b  ESSID:"science-wifi"  
Mode:Managed  Frequency:2.462 GHz  Access Point: 00:40:96:5E:0D:64  
Bit Rate:11 Mb/s   Tx-Power=20 dBm   Sensitivity=8/0  
Retry limit:7    RTS thr:off   Fragment thr:off  
Encryption key:off  
Power Management:off  
Link Quality=46/100  Signal level=-73 dBm  Noise level=-88 dBm  
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0  
Tx excessive retries:0  Invalid misc:34  Missed beacon:0
```

BackTrack: iwconfig

- ❑ To put the wireless Network Card in monitor mode (listening the channel 7):

- `iwconfig eth0 mode monitor channel 7`

- ❑ If we give the iwconfig command again, the result is something like:

```
eth0      unassociated  ESSID:off/any
Mode:Monitor  Frequency=2.442 GHz  Access Point: Not-Associated
Bit Rate:0 kb/s  Tx-Power=20 dBm  Sensitivity=8/0
Retry limit:7  RTS thr:off  Fragment thr:off
Encryption key:off
Power Management:off
Link Quality:0  Signal level:0  Noise level:0
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0  Invalid misc:51  Missed beacon:0
```



Tools for the analysis of the performances of a network

IPERF

- Several tools exist for the performances measurement of a network each one with different purposes:
 - Iperf:
 - <http://dast.nlanr.net/Projects/Iperf/>
 - d-itg:
 - <http://www.grid.unina.it/software/ITG/>
 - Netperf:
 - <http://www.netperf.org/netperf/NetperfPage.html>

Iperf: Setup

- Iperf has a many options:
- Issue the command `iperf -- help` for the full list
- The most interesting one:
 - `-u`: use UDP instead of TCP (SUGGESTED)
 - `-s`: run iperf in server mode
 - `-c`: run iperf in client mode
 - `-b`: the offered load in bit/sec
 - `-d`: run a bidirectional test simultaneously
 - `-r`: run a bidirectional test individually

IPERF: Setup

- ❑ To run IPERF as server (IP Address 192.168.10.30) :
 - `iperf -u -s`
- ❑ To run IPERF as a client:
 - `iperf -c 192.168.10.30 -u -b20M -i 5 -t 40`
 - Where:
 - ❑ `-i 5` means a report any 5 seconds
 - ❑ `-t 40` means a simulation 40 seconds long
 - ❑ `-u` means UDP transfer mode
 - ❑ `-b 20M` means 20Mbit/sec offered load (bandwidth for iperf)



Analysis of the performances of a Wireless network

Iperf: the test

- We want to measure how the performances vary changing some parameters of the configuration of the AP
- After every modification of a parameter run N times Iperf (N>20, runtime>20sec each):
 - Analyze the data set and remove any point clearly wrong (but you have to describe the procedure you adopted)
 - Compute average, standard deviation, ...
 - It is of interest also the best result!

Iperf: the test

- For our APs, you can try to:
 - Change the threshold for RTS/CTS
 - Change the threshold for fragmentation
 - Change the speed used
 - Change UDP Packet Size
 - ...

Iperf: Examples

- For example for a CISCO AP:

| Speed 11 Mb/sec | Speed 1 Mb/sec |
|--|--|
| 10.0 sec, 2.75 MBytes→ 2.30 Mbits/sec | 10.4 sec, 872 KBytes→ 684 Kbits/sec |
| 10.0 sec, 3.20 MBytes→ 2.67 Mbits/sec | |

- Therefore approximately:
 - Speed ratio: $11/1 = 11$
 - Performance ratio: $2.49 / 0.684 = 3.64$

Iperf: Suggestion

- ❑ There is no point to use a `-b` parameters too high
- ❑ For instance, if the speed configured on the AP is 11, then you can use `-b11M` during the iperf tests, and so on

Iperf: Suggestion

- For Fragmentation: choose the threshold so that you have:
 - No – fragmentation
 - 2 fragments
 - 3 fragments
 - ...
- For CTS/RTS threshold, you have just to enable/disable it

Iperf: The Report

- ❑ All the groups have to test all the speeds available (both b & g), one client, uplink, downlink
- ❑ Add to you report one or more of the following
 - Measure the maximum throughput with 2, 3 ... clients
 - RTS/CTS
 - Fragmentation
 - UDP Packet Size
 - TCP instead of UDP
 - ...

IPERF: AP Cisco

- Cisco 1310:
 - IP: 192.168.10.5
 - SSID: NCG
 - Login: empty
 - Passwd: `Cisco`
 - Channel: 7
- Cisco 1230B:
 - IP: 192.168.10.10
 - SSID: NCB
 - Login: empty
 - Passwd: `Cisco`
 - Channel: 13

Iperf: LinkSys

- LinkSys WAP54G:
 - IP: 192.168.10.15
 - SSID: NCL
 - Login: empty
 - Password: `admin`
 - Channel: 1

Iperf: setup

- ❑ Server: 192.168.10.30
- ❑ Login: `root`
- ❑ Passwd: `students`
- ❑ Connect all the device (the 3 AP and the laptop-server) to the switch
- ❑ Startup of services:
 - `/etc/init.d/networking restart`
 - `/etc/init.d/dhcp3-server restart`
 - `iperf -u -s`

Iperf: setup

- Use Backtrack & Wireshark to verify the setup of the testbed
 - The setup of the speed in both directions
 - The packet size using fragmentation, verifying MTU, iperf parameters, ...
 - The RTS/CTS

Iperf: setup

- ❑ Run backtrack on a laptop used as *control station*
- ❑ Run Wireshark and start to acquire data from the wireless interface. As an example:
 - Observe the missing data/problems of the tools
 - Fix the speed a 1/2/11/54Mb
 - Acquire a good number of data frames
 - Possibly analyze the interarrival time between frames

Lab Report

- You have to:
 - Describe the setup of the test
 - Describe the result obtained with schemes, examples (small dump of some significant packets), graphs and tables
 - Do a theoretical analysis of the expected results
 - Write down a short description of the data obtained and point out all the unexpected result you got!
 - **VERY IMPORTANT:** Do some analysis on the data (Average, Max, Min, Standard Deviation, ...)
 - Write some conclusions

Lab Report

- We will put on the website some good reports of the previous years
- We will put online a latex template