Nomadic Communications Labs

Alessandro Villani
avillani@science.unitn.it

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 is a nice network analyzer, but if you plan to dump a lot of packets use tcpdump

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

Analysis of 802.11 Packets

BackTrack

- We will use a Linux Live distribution: BackTrack
  - http://www.backtrack-linux.org/
- The last version is v:5 R3 (released 13th August 2012)
- 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 password

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 Final*
    - 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
```
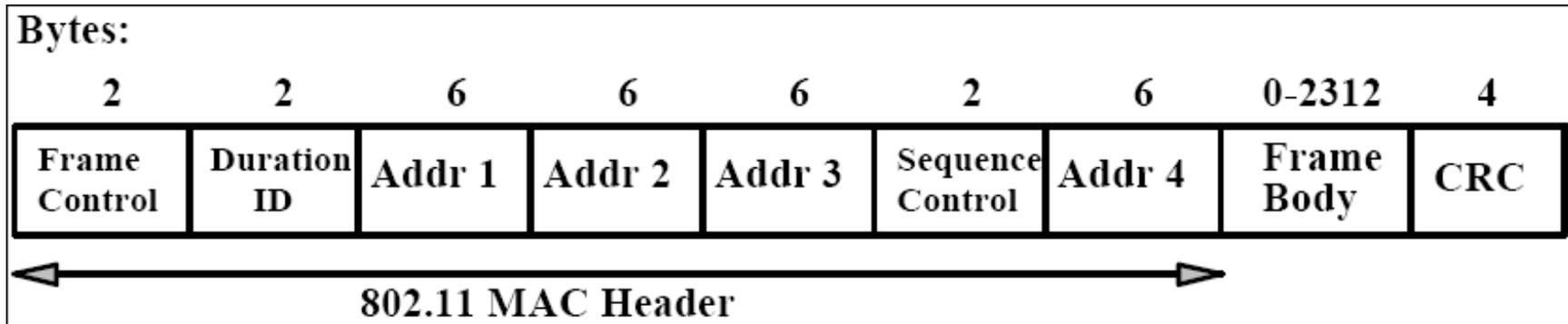
802.11 Frames

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
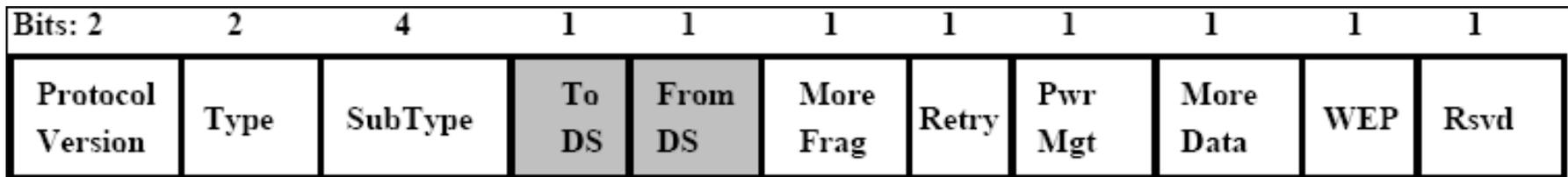
802.11 Frame

- 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:

Bytes:								
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence Control	Addr 4	Frame Body	CRC

802.11 MAC Header

- The Frame Control Field is:

Bits: 2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	SubType	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd

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	Ressociation 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 date among the stations. For instance:
  - **Request to Send (RTS) frame**
  - **Clear to Send (CTS) frame**
  - **Acknowledgement (ACK) frame**: after the arrive of a dates 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 menas 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* e *Sequence Number*

802.11 Frame: 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 AP

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 – Part 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
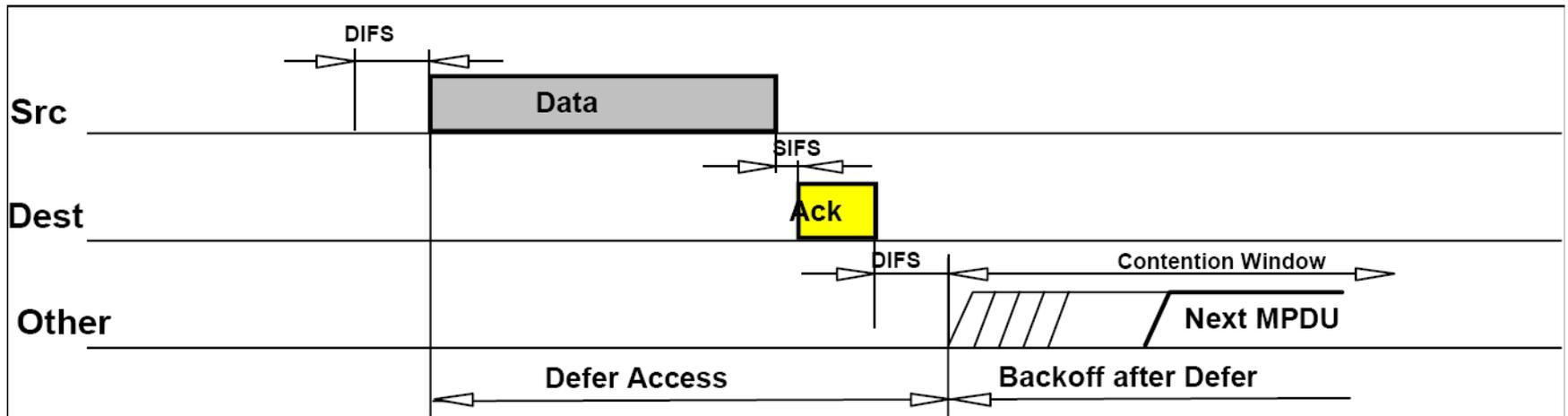
Proxy-Connection: Keep-Alive\r\n

\r\n

Acknowledgment

Control Frame: ACK

- All the unicast traffic frames must receive an ACK frame
- A *date 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)
```

Ad Hoc Networks

Ad Hoc Networks(IBSS)

- The wireless LANs we usually know use the "infrastructured" mode which requires one or more Access Points
- The 802.11 standard specifies an additional mode:
  ## Ad hoc mode
- This mode let the 802.11 network card operate in what the standard defines a network configuration "Independent Basic Service Set (IBSS)"
- In IBSS mode there are no Access Points and the various network cards communicate directly among them in peer-to-peer mode

Ad Hoc Networks(IBSS)

- The Ad Hoc mode allows the users to constitute a wireless LAN autonomously
- Typical applications:
  - Files and resources sharing among laptops
  - Application of first aid in emergency situations (disasters, accidents, fires, …)

Ad Hoc Networks(IBSS)

- Advantages/disadvantages:
  - **Reduced costs:** no AP, no cost of infrastructuration
  - **Reduced setup time:** It is enough that users have the wireless network cards
  - **Performance:** In a communication among two clients is better the Ad Hoc mode, otherwise ... it depends
  - **Reduced access to the net:** Generally there is no access to the wired net, in some cases a single client can share its connection to the others clients, however it is not a good solution!
  - **Management of a complex network:** given the fluidity of the network topology and the lack of a centralized device, the security management and the performance analysis is extremely complex

Ad Hoc Networks(IBSS)

- The first station for a particular Ad Hoc network (that is, the first NIC radio) establishes the IBSS determining the BSSID address:
    - In a infrastructured network the BSSID is the address of the wireless interface of the AP
    - In an Ad Hoc network, the BSSID is (should be – often it is the MAC of the station that is sending the beacon) generated in a random way

Ad Hoc Networks(IBSS)

- A BSSID is reserved, the broadcast BSSID (all the bits to 1):
    - Frames with broadcast BSSID jump all the BSSID filters on the MAC level
    - This address is only used when stations try to identify a net sending a probe request
    - Only the probe request frames can use the BSSID broadcast

Ad Hoc Networks(IBSS)

- Afterwards the first station starts sending beacons, needed to keep the synchronization among the stations
- Note that in infrastrucutured mode, only the Access Point can send beacons

Ad Hoc Networks(IBSS)

- The other stations of the Ad Hoc network will join the network after receiving a beacon and accepting the parameters of IBSS (in particular the interval of beacon) sent in the beacon frame

- All the stations which join the Ad Hoc network must periodically send a beacon if they do not hear a beacon from another station after a very short random delay from when they presumes that beacon had to be sent

Ad-Hoc Network Setup

Ad Hoc Network: Setup

- Start the laptop in linux
- Login with user utente and password utente
- Setup the configuration of the AdHoc Network:
  - sudo /sbin/iwconfig eth0 mode ad-hoc essid AHXX channel y rate xM
    (with x =1,2,5.5,6,…,54)
  - sudo /sbin/ifconfig eth0 10.10.10.zz
    with all the clients in the same Ad Hoc Network use different IP (different zz numbers)

Ad Hoc Network: Setup

- To verify the setup:
      sudo /sbin/iwconfig eth0
  You will obtain something like:

```
 IEEE 802.11g  ESSID:"TEST"

Mode:Ad-Hoc  Frequency:2.432 GHz  Cell: 02:15:00:E2:6F:3E

Bit Rate:54 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=67/100  Signal level=-60 dBm  Noise level=-85 dBm

Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0

Tx excessive retries:0  Invalid misc:40   Missed beacon:0
```

Ad Hoc Network: Setup

- Start netperf in server mode on one of the laptop:

```
user@ad-hoc-1:~> netserv
```

- Run netperf in client mode on the other laptops. For instance:

```
user@ad-hoc-2:~> netperf -l 20 -H xxx.yyy.zzz.www -t
UDP_STREAM -fb
```

Analysis of Ad Hoc Network packets

Probe Request

- Initially empty frame of *Probe Request* with BSSID FF:FF:FF:FF:FF:FF and with SSID either empty or with default SSID or the SSID of the Ad Hoc network

Probe Request (with ID) – Part 1

```
Frame 3 (51 bytes on wire, 51 bytes captured)
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: 00:0e:35:6e:20:39 (10.0.0.11)
    BSS Id: ff:ff:ff:ff:ff:ff (Broadcast)
    Fragment number: 0
    Sequence number: 1
```

Probe Request (with ID) – Part 2

```
IEEE 802.11 wireless LAN management frame
    Tagged parameters (27 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 9
        Tag interpretation: WNLABTEST
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5 11.0 [Mbit/sec]
        Tag Number: 50 (Extended Supported Rates)
        Tag length: 8
        Tag interpretation: Supported rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
    [Mbit/sec]
```

Probe Request (without ID) – Part 1

```
Frame 4 (42 bytes on wire, 42 bytes captured)
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: 00:0e:35:6e:20:39 (10.0.0.11)
    BSS Id: ff:ff:ff:ff:ff:ff (Broadcast)
    Fragment number: 0
    Sequence number: 2
```

Probe Request (without ID) – Part 2

```
IEEE 802.11 wireless LAN management frame
    Tagged parameters (18 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 0
        Tag interpretation:
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5 11.0 [Mbit/sec]
        Tag Number: 50 (Extended Supported Rates)
        Tag length: 8
        Tag interpretation: Supported rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
    [Mbit/sec]
```

Beacon Frame

- Waited for a certain time interval the *Beacon Frame* starts

- In the beacon now there is the BSSID chosen in random way

Beacon Frame – Part 1

```
Frame 32 (82 bytes on wire, 82 bytes captured)
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: 00:0e:35:6e:20:39 (10.0.0.11)
    BSS Id: 02:0e:35:00:13:ab (02:0e:35:00:13:ab)
    Fragment number: 0
    Sequence number: 46
```

Beacon Frame – Part 2

```
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x0000000000019256
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0022
            .... .... .... ...0 = ESS capabilities: Transmitter is a STA
            .... .... .... ..1. = IBSS status: Transmitter belongs to an IBSS
            .... .... .... 00.. = CFP participation capabilities: Station is not CF-
    Pollable (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
```

Beacon Frame – Part 3

```
Tagged parameters (46 bytes)
    Tag Number: 0 (SSID parameter set)
    Tag length: 9
    Tag interpretation: WNLABTEST
    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: 9
    Tag Number: 6 (IBSS Parameter set)
    Tag length: 2
    Tag interpretation: ATIM window 0x0
    Tag Number: 221 (Vendor Specific)
    Tag length: 7
    Tag interpretation: WME IE: type 2, subtype 0, version 1, parameter set 0
    Tag Number: 42 (ERP Information)
    Tag length: 1
    Tag interpretation: ERP info: 0x0 (no Non-ERP STAs, do not use protection, long
preambles)
    Tag Number: 50 (Extended Supported Rates)
    Tag length: 8
    Tag interpretation: Supported rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
[Mbit/sec]
```

Probe Response

- When a new station ask to join the network, it starts sending the frame *Probe Request*

- The first station answers with a frame Probe Response destined to the new station

Probe Response – Part 1

```
Frame 147 (82 bytes on wire, 82 bytes captured)
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 (10.0.0.10)
    Source address: 00:0e:35:6e:20:39 (10.0.0.11)
    BSS Id: 02:0e:35:00:13:ab (02:0e:35:00:13:ab)
    Fragment number: 0
    Sequence number: 143
```

Probe Response – Part 2

```
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x0000000000920D3E
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0022
            .... .... .... ...0 = ESS capabilities: Transmitter is a STA
            .... .... .... ..1. = IBSS status: Transmitter belongs to an IBSS
            .... .... .... 00.. = CFP participation capabilities: Station is not CF-
    Pollable (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
```

Probe Response – Part 3

```
Tagged parameters (46 bytes)
    Tag Number: 0 (SSID parameter set)
    Tag length: 9
    Tag interpretation: WNLABTEST
    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: 9
    Tag Number: 6 (IBSS Parameter set)
    Tag length: 2
    Tag interpretation: ATIM window 0x0
    Tag Number: 221 (Vendor Specific)
    Tag length: 7
    Tag interpretation: WME IE: type 2, subtype 0, version 1, parameter set 0
    Tag Number: 42 (ERP Information)
    Tag length: 1
    Tag interpretation: ERP info: 0x0 (no Non-ERP STAs, do not use protection, long
preambles)
    Tag Number: 50 (Extended Supported Rates)
    Tag length: 8
    Tag interpretation: Supported rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
[Mbit/sec]
```

Data Frame

- Substantially identical to those of an infrastructured wireless network
- Note as the BSSID is always the one transmitted in the *Beacon Frames*

Data Frame – Part 1

```
Frame 361 (92 bytes on wire, 92 bytes captured)
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0008 (Normal)
        Version: 0
        Type: Data frame (2)
        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: 00:0e:35:6e:20:39 (10.0.0.11)
    Source address: 00:0b:cd:8d:30:3b (10.0.0.10)
    BSS Id: 02:0e:35:00:13:ab (02:0e:35:00:13:ab)
    Fragment number: 0
    Sequence number: 111
Logical-Link Control
Internet Protocol, Src Addr: 10.0.0.10 (10.0.0.10), Dst Addr: 10.0.0.11 (10.0.0.11)
```

Data Frame – Part 2

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x495c (correct)
    Identifier: 0x0200
    Sequence number: 0x0200
    Data (32 bytes)

0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70    abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69    qrstuvwabcdefghi
```