Nomadic Communications Labs

Alessandro Villani
avillani@science.unitn.it

Radius

AAA

- Given an high number of access points
- Given a large amount of users
- We have the requirement of managing in centralized way the AAA (Authentication, Authorization, Accounting) process

Radius Protocol

- RADIUS *(Remote Authentication Dial-In Service*) is a client/server protocol
- Defined in RFC 2865, available on IETF site:
  http://www.ietf.org/rfc.html
- The UDP port 1812 is used for authentication
- The Accounting for RADIUS is defined in RFC 2866
- The UDP port 1813 is used for accounting

Radius Protocol

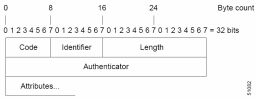
- A NAS (*Network Access Server*) communicates with a RADIUS server to authenticate a user (login and passwd)
- The NAS can receive specific configuration information from the RADIUS server for the user
- RADIUS uses a series of retransmission mechanisms in case of time-out

Radius Protocol

- The transitions among the client and the server RADIUS are authenticated by a shared key (never sent on the net)
- This mechanism is uncomfortable to manage: a change of the password requires the updating of all the NAS
- All the users' passwords are sent in encrypted form from the client towards the server

Radius Protocol: Packets

- The scheme of a RADIUS Packet



- ***Code***: it identifies the following types of package:
  - Access-Request (1)
  - Access-Accept (2)
  - Access-Reject (3)
  - Accounting-Request (4)
  - Accounting-Response (5)
  - Access-Challenge (11)

Radius Protocol: Packets

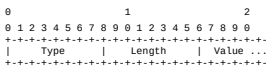
- ***Identifier***: it is used to associate requests to answers and to identify duplicate requests
- ***Length***: the length of the whole packet
- ***Authenticator:*** it is used to authenticate the answer of the server. Two types of Authenticator are defined :
  - Request-Authentication: used in *Access-Request* e *Accounting-Request packets*
  - Response-Authenticator: used in *Access-Accept*, *Access-Reject*, *Access-Challenge*, and *Accounting-Response packets*

Radius Protocol: Packets

- The Authenticator field is a pseudo-random number of 128-bits and it must be unpredictable
- Some implementations do not respect the unpredictability!
- 128-bit Response Authenticator = MD5(Code + Identifier + Length + Request Authenticator + Attributes + Shared Secret)

Radius Protocol: Packets

- ***Attributes***: this variable length field contains a list of zero or more attributes
- The format of an attribute is the following:



- Some of the types defined are:
  - 1 User-Name
  - 2 User-Password
  - 4 NAS-IP-Address
  - 5 NAS-Port
  - 32 NAS-Identifier
  - 40-59 Accounting

Radius Protocol: Packets

- ***Access-Request***: sent from a NAS to a RADIUS server. It contains the information needed by the RADIUS server to determine if the client requiring access through the NAS can be accepted
- ***Access-Accept***: When the RADIUS server receives an Access-Request, it will send back an Access-Accept if the values of all the attributes in the Access-Request are acceptable. Access-Accept will give the configuration information necessary to the NAS

Radius Protocol: Packets

- ***Access-Reject***: When the RADIUS server receives an Access-Request, it will send an Access-Reject if some of the values of any attribute in the Access-Request is unacceptable
- ***Access-Challenge***: when the RADIUS server receives an Access-Request, it can send to the NAS an Access-Challenge, which will require an answer. The NAS will answer with a new Access-Request

Radius Protocol: Packets

- ***Accounting-Request***: sent to an accounting RADIUS server from a NAS, giving information about accounting. When the RADIUS server receive the Accounting-Request, it will answer with an Accounting-Response
- ***Accounting-Response***: sent from the accounting RADIUS server to the NAS to confirm the receiving of the Accounting-Request

Radius Protocol: Accounting

- When a client uses a RADIUS server for the accounting:
  - The NAS will send at the beginning of the service an Accounting-Start message that describes the type of service provided and the user information
  - The server will answer confirming the receipt
  - At the end of the provided service, the NAS will send a packet of Accounting-Stop which describes the type of provided service and optionally some statistics as the time elapsed, the input and output octet, or the input and output packets
  - The NAS will keep on trying to send the Accounting-Request packets until it receives an acknowledgement from the server

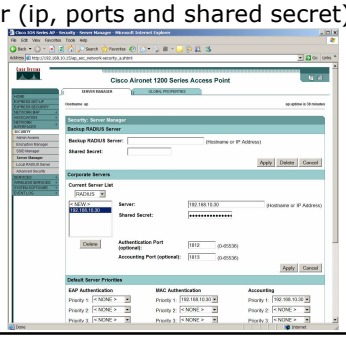
Radius Protocol: comments

- Radius can exhibit very low performance and loss of data when used in big installations, given that it does not include mechanisms for the congestion control
- It has been proposed a new protocol→ *DIAMETER* (that use TCP)
- Anyway Radius is still the most used protocol for AAA!

Cisco AP 1200
and Radius Configuration

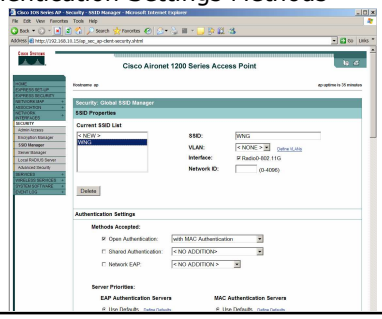
Cisco AP 1200 & Radius Configuration

- We have to configure the default radius server (ip, ports and shared secret)



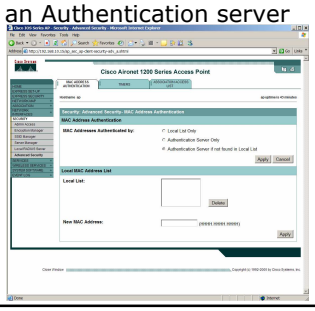
Cisco AP 1200 & Radius Configuration

- Then we need to change the Authentication Settings Methods



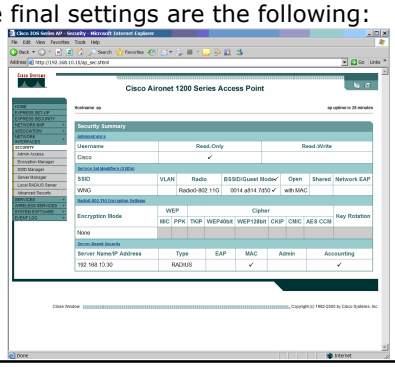
Cisco AP 1200 & Radius Configuration

- Finally we have to force that for the MAC Addresses Authentication the AP has to contact an Authentication server



Cisco AP 1200 & Radius Configuration

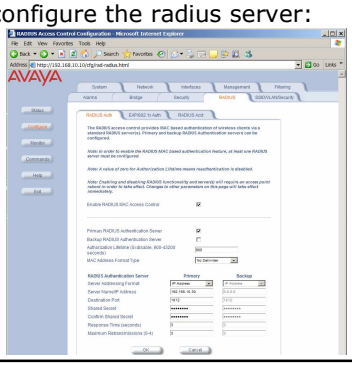
- The final settings are the following:



Avaya AP-3
and Radius Configuration

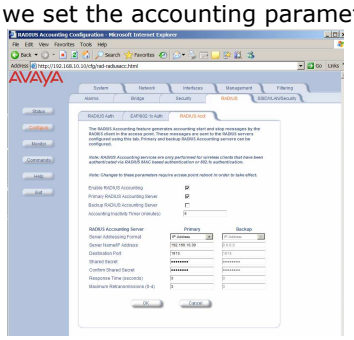
Avaya AP-3 & Radius Configuration

- We configure the radius server:



Avaya AP-3 & Radius Configuration

- Then we set the accounting parameters



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

WireShark: Radius Accounting

- The authentication through RADIUS of the MAC address of a Wireless card is translated in:
  - As User Id the MAC address of the network card
  - As password:
    - The shared secret configured on the AP for Avaya AP
    - The MAC address of the wireless card for CISCO AP

WireShark: Radius Authentication

Access Request (Code = 1)

```
Frame 9 (107 bytes on wire, 107 bytes captured)
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.25 (172.31.194.25), Dst Addr: 192.168.194.168
    (192.168.194.168)
User Datagram Protocol, Src Port: 6001 (6001), Dst Port: radius (1812)
    Source port: 6001 (6001)
    Destination port: radius (1812)
    Length: 73
    Checksum: 0xb4dd (correct)
Radius Protocol
    Code: Access Request (1)
    Packet identifier: 0xd2 (210)
    Length: 65
    Authenticator: 0x5D170000B9760000D55F00008C410000
    Attribute value pairs
        t:User Name(1) l:15, Value:"00904b-649170"
        t:User Password(2) l:18, Value:BCA8373AA383F48F1CE20A230CFE7D0D
        t:NAS IP Address(4) l:6, Value:172.31.194.25
        t:NAS Port(5) l:6, Value:0
```

WireShark: Radius Authentication

Accepted Access (Code = 2)

```
Frame 10 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:80:5f:41:fb:95, Dst: 00:00:cd:03:fe:7e
Internet Protocol, Src Addr: 192.168.194.168 (192.168.194.168), Dst Addr: 172.31.194.25
    (172.31.194.25)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 6001 (6001)
    Source port: radius (1812)
    Destination port: 6001 (6001)
    Length: 28
    Checksum: 0xae8b (correct)
Radius Protocol
    Code: Access Accept (2)
    Packet identifier: 0xd2 (210)
    Length: 20
    Authenticator: 0x97E2EFA2A29FDCB8F223CA43D655A499
```

WireShark: Radius Authentication

- It is possible to analyze in plain the content of encrypted fields
- Edit→Preferences→Protocols
- Selecting Radius it is possible to set up the shared secret

WireShark: Accounting on Avaya AP

- The accounting procedure for the Avaya AP require only to register the starting time of the session and his end

WireShark: Accounting on Avaya AP

Accounting Request (Code = 4): Start

```
Frame 11 (132 bytes on wire, 132 bytes captured)
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.25 (172.31.194.25), Dst Addr: 192.168.194.168
    (192.168.194.168)
User Datagram Protocol, Src Port: 6002 (6002), Dst Port: radius-acct (1813)
    Source port: 6002 (6002)
    Destination port: radius-acct (1813)
    Length: 98
    Checksum: 0x38f9 (correct)
Radius Protocol
    Code: Accounting Request (4)
    Packet identifier: 0xd3 (211)
    Length: 90
    Authenticator: 0x7726EA20EDC039C0CD37B7232FF23D0E
    Attribute value pairs
        t:User Name(1) l:15, Value:"00904b-649170"
        t:Acct Session Id(44) l:15, Value:"00904b-649170"
        t:NAS identifier(32) l:10, Value:"Avaya-15"
        t:NAS IP Address(4) l:6, Value:172.31.194.25
        t:NAS Port(5) l:6, Value:2
        t:NAS Port Type(61) l:6, Value:Wireless IEEE 802.11(19)
        t:Acct Authentic(45) l:6, Value:Radius(1)
        t:Acct Status Type(40) l:6, Value:Start(1)
```

WireShark: Accounting on Avaya AP

Accounting Response (Code = 5)

```
Frame 12 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:80:5f:41:fb:95, Dst: 00:00:cd:03:fe:7e
Internet Protocol, Src Addr: 192.168.194.168 (192.168.194.168), Dst Addr: 172.31.194.25
    (172.31.194.25)
User Datagram Protocol, Src Port: radius-acct (1813), Dst Port: 6002 (6002)
    Source port: radius-acct (1813)
    Destination port: 6002 (6002)
    Length: 28
    Checksum: 0xa6e1 (correct)
Radius Protocol
    Code: Accounting Response (5)
    Packet identifier: 0xd3 (211)
    Length: 20
    Authenticator: 0xE3ACA0C57C3FCAED9B081887B3F10FBB
```

WireShark: Accounting on Avaya AP

Accounting Request (Code = 4): Stop

```
Frame 13 (132 bytes on wire, 132 bytes captured)
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.25 (172.31.194.25), Dst Addr: 192.168.194.168
    (192.168.194.168)
User Datagram Protocol, Src Port: 6002 (6002), Dst Port: radius-acct (1813)
    Source port: 6002 (6002)
    Destination port: radius-acct (1813)
    Length: 98
    Checksum: 0x6372 (correct)
Radius Protocol
    Code: Accounting Request (4)
    Packet identifier: 0xd4 (212)
    Length: 90
    Authenticator: 0x0E739E4CD09F9C3DC8ED9CA383454D35
    Attribute value pairs
        t:User Name(1) l:15, Value:"00904b-649170"
        t:Acct Session Id(44) l:15, Value:"00904b-649170"
        t:NAS identifier(32) l:10, Value:"Avaya-15"
        t:NAS IP Address(4) l:6, Value:172.31.194.25
        t:NAS Port(5) l:6, Value:2
        t:NAS Port Type(61) l:6, Value:Wireless IEEE 802.11(19)
        t:Acct Authentic(45) l:6, Value:Radius(1)
        t:Acct Status Type(40) l:6, Value:Stop(2)
```

WireShark: Accounting on Avaya AP

Accounting Response (Code = 5)

```
Frame 14 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:80:5f:41:fb:95, Dst: 00:00:cd:03:fe:7e
Internet Protocol, Src Addr: 192.168.194.168 (192.168.194.168), Dst Addr: 172.31.194.25
    (172.31.194.25)
User Datagram Protocol, Src Port: radius-acct (1813), Dst Port: 6002 (6002)
    Source port: radius-acct (1813)
    Destination port: 6002 (6002)
    Length: 28
    Checksum: 0x6c6b (correct)
Radius Protocol
    Code: Accounting Response (5)
    Packet identifier: 0xd4 (212)
    Length: 20
    Authenticator: 0x7B5864A3F47B3C3C7E8ECFFA292BF4E8
```

WireShark: Accounting on Cisco AP

- The accounting procedure for the Cisco AP registers many more information that for Avaya AP:
  - Input octects
  - Output octects
  - Input packets
  - Output packets
  - Session Time

WireShark: Accounting on Cisco AP

Accounting Request (Code = 4): Start

```
Frame 1 (242 bytes on wire, 242 bytes captured)
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.32 (172.31.194.32), Dst Addr: 192.168.194.168
    (192.168.194.168)
User Datagram Protocol, Src Port: 2375 (2375), Dst Port: radacct (1813)
Radius Protocol
    Code: Accounting Request (4)
    Packet identifier: 0x1 (1)
    Length: 200
    Authenticator: 0xE8B22BAA94A8C9C33513B03547064CA7
    Attribute value pairs
        t:Acct Status Type(40) l:6, Value:Start(1)
        t:User Name(1) l:14, Value:"000bcd8d303b"
        t:Acct Session Id(44) l:10, Value:"  700001"
        t:Acct Authentic(45) l:6, Value:Local(2)
        t:NAS Port(5) l:6, Value:37
        t:Calling Station Id(31) l:14, Value:"000bcd8d303b"
        t:NAS identifier(32) l:15, Value:"CISCO 350 - 2"
        t:NAS IP Address(4) l:6, Value:172.31.194.32
        t:Vendor Specific(26) l:17, Vendor:Cisco(9)
            t:Cisco AV Pair(1) l:11, Value:"vlan-id=0"
        t:Vendor Specific(26) l:34, Vendor:Cisco(9)
            t:Cisco AV Pair(1) l:28, Value:"nas-location=Malga - Atrio"
        t:Vendor Specific(26) l:27, Vendor:Cisco(9)
            t:Cisco AV Pair(1) l:21, Value:"auth-algo-type=open"
        t:Vendor Specific(26) l:19, Vendor:Cisco(9)
            t:Cisco AV Pair(1) l:13, Value:"ssid=WNTEST"
        t:Acct Delay Time(41) l:6, Value:0
```

WireShark: Accounting on Cisco AP

Accounting Request (Code = 4): Stop

```
Frame 3 (193 bytes on wire, 193 bytes captured)
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.32 (172.31.194.32), Dst Addr: 192.168.194.168
    (192.168.194.168)
User Datagram Protocol, Src Port: 2378 (2378), Dst Port: radacct (1813)
Radius Protocol
    Code: Accounting Request (4)
    Packet identifier: 0x2 (2)
    Length: 151
    Authenticator: 0x0D7AA97243A5E220748D78B57A306BFE
    Attribute value pairs
        t:Acct Status Type(40) l:6, Value:Stop(2)
        t:User Name(1) l:14, Value:"000bcd8d303b"
        t:Acct Session Id(44) l:10, Value:"  700001"
        t:Acct Authentic(45) l:6, Value:Local(2)
        t:Acct Input Octets(42) l:6, Value:2406852
        t:Acct Output Octets(43) l:6, Value:100908
        t:Acct Input Packets(47) l:6, Value:2495
        t:Acct Input Gigawords(52) l:6, Value:0
        t:Acct Output Gigawords(53) l:6, Value:0
        t:Acct Output Packets(48) l:6, Value:521
        t:Acct Session Time(46) l:6, Value:125
        t:NAS Port(5) l:6, Value:37
        t:Calling Station Id(31) l:14, Value:"000bcd8d303b"
        t:NAS identifier(32) l:15, Value:"CISCO 350 - 2"
        t:NAS IP Address(4) l:6, Value:172.31.194.32
        t:Acct Terminate Cause(49) l:6, Value:Lost Carrier(2)
        t:Acct Delay Time(41) l:6, Value:2
```

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 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

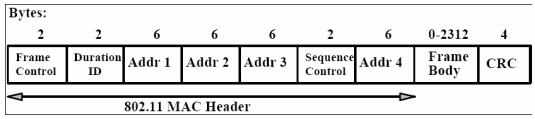
- The Monitor Mode (plus applications like WireShark or Kismet) allows us to analyze the frames of a 802.11 communication
- 802.11 defines several types of frame which stations (NIC and AP) use to communicate among them and to manage and check the wireless link

802.11 Frame

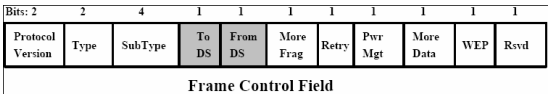
- Each frame has a control field that defines the version of the 802.11 protocol, the type of frame, and several flags like if WEP is active, if the management power is active, ...
- Every frame contains MAC addresses of the source and destination station, a frame number, the frame body and a frame check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

802.11 Frame

- Frame format:



- The Frame Control Field is:



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*

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: 0.000368000 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

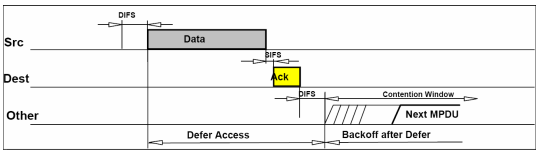
```
Internet Protocol, Src Addr: 192.168.213.24 (192.168.213.24), Dst Addr: 193.205.213.166
    (193.205.213.166)
Transmission Control Protocol, Src Port: 3346 (3346), Dst Port: 3128 (3128), Seq: 1,
    Ack: 1, Len: 438
Hypertext Transfer Protocol
    GET http://www.google.it/ HTTP/1.0\r\n
        Request 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)
```