

Wireless Network

Esercitazioni



Alessandro Villani
avillani@science.unitn.it



Reti Ad Hoc

Reti Ad Hoc (IBSS)

- Tipicamente le wireless LANs che conosciamo utilizzano la modalità "infrastrutturata" che richiede uno o più access points
- Lo standard 802.11 specifica una modalità supplementare:

Ad hoc mode

- Questa modalità consente alla scheda di rete 802.11 di operare in quello che lo standard definisce una configurazione di rete "*Independent Basic Service Set (IBSS)*"
- In modalità IBSS non ci sono access points e le varie schede di rete comunicano direttamente fra loro in modalità peer-to-peer

Reti Ad Hoc (IBSS)

- La modalità Ad Hoc permette agli utenti di costituire una wireless LAN autonomamente
- Applicazioni tipiche:
 - Condivisione files e risorse fra laptop
 - Applicazioni di pronto intervento in situazioni di emergenza (disastri, incidenti, incendi, ...)

Reti Ad Hoc (IBSS)

□ Vantaggi/svantaggi:

- **Costi ridotti:** no Ap, nessun costo di infrastrutturazione
- **Ridotti tempi di setup:** Basta che gli utenti abbiano le schede wireless
- **Performance:** In una comunicazione fra due client è meglio l'Ad Hoc mode, altrimenti ... dipende
- **Accesso ridotto alla rete:** In generale non c'è accesso alla rete cablata, al più uno dei client può condividere la propria connessione, comunque non è una buona soluzione!
- **Gestione della rete complicata:** data la fluidità della topologia di rete e la mancanza di un device centralizzato la gestione della sicurezza e l'analisi delle prestazioni è estremamente complessa

Reti Ad Hoc (IBSS)

- La prima stazione attiva per una data rete *Ad Hoc* (ovvero la prima radio NIC) stabilisce l'IBSS determinando l'indirizzo BSSID:
 - Nel caso di una rete infrastrutturata il BSSID è l'indirizzo dell'interfaccia wireless dell'AP
 - Nel caso di una rete Ad Hoc il BSSID è generato in maniera casuale

Reti Ad Hoc (IBSS)

- Un BSSID è riservato, il *broadcast BSSID* (tutti i bit a 1):
 - I frame con broadcast BSSID saltano tutti i filtri sul BSSID del livello MAC
 - Questo indirizzo è utilizzato solo quando le stazioni cercano di individuare una rete inviando una probe request
 - Solo i frame di probe possono utilizzare il broadcast BSSID

Reti Ad Hoc (IBSS)

- Dopodichè la prima stazione inizia ad inviare beacons, necessari per mantenere la sincronizzazione fra le stazioni
- Notare che in modo infrastrutturato, solo gli Access Point possono inviare i beacons

Reti Ad Hoc (IBSS)

- ❑ Le altre stazioni della rete *Ad Hoc* si uniranno alla rete dopo aver ricevuto un beacon e aver accettato i parametri dell'IBSS (in particolare l'intervallo dei beacon) inviati nel beacon frame
- ❑ Tutte le stazioni che si uniscono alla rete *Ad Hoc* devono inviare un beacon periodicamente se non sentono a loro volta un beacon da un'altra stazione dopo un ritardo casuale molto breve da quando si presume che il beacon dovesse essere inviato



Analisi pacchetti Reti Ad Hoc

Probe Request

- Inizialmente frame di Probe Request con BSSID FF:FF:FF:FF:FF:FF con SSID vuoto o con SSID di default o con quello della rete *Ad Hoc*

Probe Request (con ID) – Parte 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 (con ID) – Parte 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 (senza ID) – Parte 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 (senza ID) – Parte 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

- Atteso un certo intervallo di tempo iniziano i Beacon Frame
- Nei beacon ora c'è il BSSID scelto in modo random

Beacon Frame – Parte 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 – Parte 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 – Parte 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

- Quando si presenta una nuova stazione questa comincia ad inviare i frame Probe Request
- La prima stazione risponde con un frame Probe Response destinato alla nuova stazione

Probe Response – Parte 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 – Parte 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 – Parte 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

- ❑ Sostanzialmente identici a quelli di un rete wireless infrastrutturata
- ❑ Notare come il BSSID sia sempre quello trasmesso nei beacon

Data Frame – Parte 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 – Parte 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
```



Host AP

Host AP

- Il software sviluppato dal progetto Host AP permette di trasformare un normale pc in un Access Point
- Il sito principale del progetto è:
<http://hostap.epitest.fi/>
- È composto fondamentalmente da due componenti:
 - I driver Host AP
 - Il daemon hostapd

Host AP: il driver

- Il driver Host Ap supporta le schede con chipset Intersil Prism2/2.5/3
- Il firmware di questi chipset supporta una modalità detta Host AP. In questa modalità il firmware si occupa di vari servizi time critical come l'invio dei beacon e l'ack dei frame
- Il driver implementa le funzionalità base richieste per:
 - Inizializzare e configurare le schede
 - Per inviare e ricevere frames
 - Per acquisire statistiche

Host AP: il driver

- Inoltre, implementa altre funzionalità 802.11:
 - Autenticazione (deautenticazione)
 - Associazione (riassociazione e disassociazione)
 - Trasmissione fra due stazioni wireless
 - Supporto per il Power saving mode

Host AP: il daemon

- `hostapd` è un daemon che esegue nello spazio utente per la gestione dell'Access Point e dei server di autenticazione
- Implementa:
 - IEEE 802.11 access point management
 - IEEE 802.1X/WPA/WPA2/EAP Authenticators
 - RADIUS authentication server
 - Parzialmente IAPP - 802.11f

Host AP: configurazione

- ❑ Dopo aver installato il software, la configurazione a run time può essere fatta utilizzando i wireless tools standard per linux, in particolare `iwconfig`
- ❑ `iwconfig` potrà essere utilizzato per impostare la modalità della scheda, il canale, l'ESSID:
 - `iwconfig wlan0 essid WNLABHOSTAP`
 - `iwconfig wlan0 channel 8`
 - `iwconfig wlan0 mode master`

Host AP: QoS

- Politecnico di Torino e CSP hanno sviluppato dei moduli per il supporto di QoS basandosi su Host AP
- Il progetto si chiama Host Qs:
<http://www.inlab.csp.it/tools/wireless/hostqs/>



Dump Pacchetti Host AP

Dump pacchetti Host AP

- Come ci si può facilmente aspettare non c'è alcuna apprezzabile differenza fra i pacchetti inviati da un AP vero e quelli inviati da un computer con Host AP installato!

Host AP: Beacon Frame – Parte 1

Frame 287 (64 bytes on wire, 64 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: 00:09:5b:54:7e:9d (10.0.0.1)

BSS Id: 00:09:5b:54:7e:9d (10.0.0.1)

Fragment number: 0

Sequence number: 2400

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Timestamp: 0x00000000623C7390

Beacon Interval: 0.102400 [Seconds]

Host AP: Beacon Frame – Parte 2

```
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
Tagged parameters (28 bytes)
  Tag Number: 0 (SSID parameter set)
  Tag length: 11
  Tag interpretation: WNLABHOSTAP
  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: 3 (DS Parameter set)
  Tag length: 1
  Tag interpretation: Current Channel: 8
  Tag Number: 5 ((TIM) Traffic Indication Map)
  TIM length: 4
  DTIM count: 0
  DTIM period: 1
  Bitmap Control: 0x00 (mcast:0, bitmap offset 0)
```

Host AP: Probe Response – Parte 1

Frame 289 (58 bytes on wire, 58 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: 00:0e:35:6e:20:39 (10.0.0.101)

Source address: 00:09:5b:54:7e:9d (10.0.0.1)

BSS Id: 00:09:5b:54:7e:9d (10.0.0.1)

Fragment number: 0

Sequence number: 2401

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Timestamp: 0x00000000623D96DA

Beacon Interval: 0.102400 [Seconds]

Host AP: Beacon Frame – Parte 2

```
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
Tagged parameters (22 bytes)
  Tag Number: 0 (SSID parameter set)
  Tag length: 11
  Tag interpretation: WNLABHOSTAP
  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: 3 (DS Parameter set)
  Tag length: 1
  Tag interpretation: Current Channel: 8
```

Host AP: Data – Ping verso AP

Frame 839 (92 bytes on wire, 92 bytes captured)

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: 00:09:5b:54:7e:9d (10.0.0.1)

Source address: 00:0e:35:6e:20:39 (10.0.0.101)

Destination address: 00:09:5b:54:7e:9d (10.0.0.1)

Fragment number: 0

Sequence number: 56

Logical-Link Control

Internet Protocol, Src Addr: 10.0.0.101 (10.0.0.101), Dst Addr: 10.0.0.1 (10.0.0.1)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x3f5c (correct)

Identifier: 0x0200

Sequence number: 0x0c00

Data (32 bytes)

Host AP: ACK dall'AP

Frame 840 (10 bytes on wire, 10 bytes captured)

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: 00:0e:35:6e:20:39 (10.0.0.101)

Host AP: Log delle sessioni

- Host Ap può produrre il logging delle varie sessioni e transazioni

Host AP: Log sessione – Parte 1

Received 30 bytes management frame

```
RX frame - hexdump(len=30): b0 00 3a 01 00 09 5b 54 7e 9d 00 0e 35 6e 20 39 00 09 5b 54
    7e 9d 40 02 00 00 01 00 00 00
```

MGMT

mgmt::auth

authentication: STA=00:0e:35:6e:20:39 auth_alg=0 auth_transaction=1 status_code=0 wep=0

New STA

wlan0: STA 00:0e:35:6e:20:39 IEEE 802.11: authentication OK (open system)

wlan0: STA 00:0e:35:6e:20:39 WPA: event 0 notification

authentication reply: STA=00:0e:35:6e:20:39 auth_alg=0 auth_transaction=2 resp=0

Received 30 bytes management frame

```
RX frame - hexdump(len=30): b2 00 3a 01 00 0e 35 6e 20 39 00 09 5b 54 7e 9d 00 09 5b 54
    7e 9d c0 0e 00 00 02 00 00 00
```

MGMT (TX callback) ACK

mgmt::auth cb

wlan0: STA 00:0e:35:6e:20:39 IEEE 802.11: authenticated

Host AP: Log sessione – Parte 2

Received 47 bytes management frame

```
RX frame - hexdump(len=47): 00 00 3a 01 00 09 5b 54 7e 9d 00 0e 35 6e 20 39 00 09 5b 54
    7e 9d 50 02 01 00 0a 00 00 0b 57 4e 4c 41 42 48 4f 53 54 41 50 01 04 82 84 0b 16
```

MGMT

mgmt::assoc_req

association request: STA=00:0e:35:6e:20:39 capab_info=0x01 listen_interval=10

new AID 1

wlan0: STA 00:0e:35:6e:20:39 IEEE 802.11: association OK (aid 1)

Received 36 bytes management frame

```
RX frame - hexdump(len=36): 12 00 3a 01 00 0e 35 6e 20 39 00 09 5b 54 7e 9d 00 09 5b 54
    7e 9d d0 0e 01 00 00 00 01 c0 01 04 82 84 0b 16
```

MGMT (TX callback) ACK

mgmt::assoc_resp cb

wlan0: STA 00:0e:35:6e:20:39 IEEE 802.11: associated (aid 1, accounting session 4268FE09-00000000)

wlan0: STA 00:0e:35:6e:20:39 WPA: event 1 notification