

# Wireless Network Esercitazioni

Alessandro Villani  
avillani@science.unitn.it

---

---

---

---

---

---

---

---

## Kismet: ACK

- Tutto i frame di traffico unicast devono ricevere un frame di ACK
- Un data frame utilizzerà il NAV per riservare il canale per il frame di dati, il suo ACK e il SIFS (Short Inter Frame Space)
- In questo modo il sender garantisce al ricevente del frame la possibilità di inviare l'ACK

---

---

---

---

---

---

---

---

## Kismet: ACK

The screenshot shows the Kismet interface with a list of captured frames. The list includes frame numbers, timestamps, source and destination MAC addresses, and frame types. A detailed view of a frame is shown below the list, displaying the frame type (Data), duration, source and destination addresses, and other frame-specific information.

No.	Time	Source	Destination	Type
0	0.000000	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
1	0.000011	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
2	0.000022	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
3	0.000033	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
4	0.000044	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
5	0.000055	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
6	0.000066	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
7	0.000077	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
8	0.000088	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
9	0.000099	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
10	0.000110	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
11	0.000121	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
12	0.000132	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
13	0.000143	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
14	0.000154	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
15	0.000165	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
16	0.000176	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
17	0.000187	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
18	0.000198	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
19	0.000209	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
20	0.000220	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
21	0.000231	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
22	0.000242	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
23	0.000253	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon
24	0.000264	192.168.1.1	192.168.1.2	IEEE 802.11 Beacon

---

---

---

---

---

---

---

---

## Kismet: Data Frame

```
Frame 1 (80 bytes on wire, 80 bytes captured)
Arrival Time: May 12, 2004 19:49:14.350902000
Time delta from previous packet: 0.000000000 seconds
Time since reference or first frame: 0.000000000 seconds
Frame Number: 1
Packet Length: 80 bytes
Capture Length: 80 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
RSSI: 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 (AlliedTe_03:fe:7e)
Fragment number: 0
Sequence number: 2076
Logical-Link Control
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: 0,
Ack: 0, Len: 0
```

---

---

---

---

---

---

---

---

---

---

## Kismet: ACK

```
Frame 2 (10 bytes on wire, 10 bytes captured)
Arrival Time: May 12, 2004 19:49:14.351503000
Time delta from previous packet: 0.000601000 seconds
Time since reference or first frame: 0.000601000 seconds
Frame Number: 2
Packet Length: 10 bytes
Capture Length: 10 bytes
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)
```

---

---

---

---

---

---

---

---

---

---

Attività di Laboratorio

---

---

---

---

---

---

---

---

---

---

### Laboratorio: Ethereal

- Utilizzare ethereal per:
  - Acquisire traffico sul radius server
  - Acquisire traffico sugli AP dedicati al corso
- Analizzare il traffico
- Scrivere un breve report che descriva il tipo di traffico registrato

---

---

---

---

---

---

---

---

### Laboratorio: Radius

- Acquisire traffico sul radius server
  - Radius server configurato appositamente
  - IP: 192.168.91.130
  - Usrid: root
  - Passwd: la solita!

---

---

---

---

---

---

---

---

### Laboratorio: Radius

- I files di configurazione risiedono nella directory /etc/raddb
- Gli utenti con relativa passwd sono memorizzati nel file /etc/raddb/users
- Gli AP preventivamente autorizzati sono nel file /etc/raddb/clients.conf
- Il log delle connessioni sono in /var/log/radius/radius.log
- I files di accounting sono in /var/log/radius/radacct

---

---

---

---

---

---

---

---

### Laboratorio: Traffico a livello 3

- ❑ Utilizziamo i laptop per collegarsi all'AP
- ❑ Lanciare ethereal per acquisire il traffico
- ❑ Lanciare ethereal sul server radius per verificare i pacchetti di autorizzazione e di accounting

---

---

---

---

---

---

---

---

### Laboratorio: Traffico a livello 2

- ❑ Utilizziamo i laptop per collegarsi all'AP
- ❑ Lanciare ethereal con le schede configurate in modalità monitor per acquisire il traffico

---

---

---

---

---

---

---

---