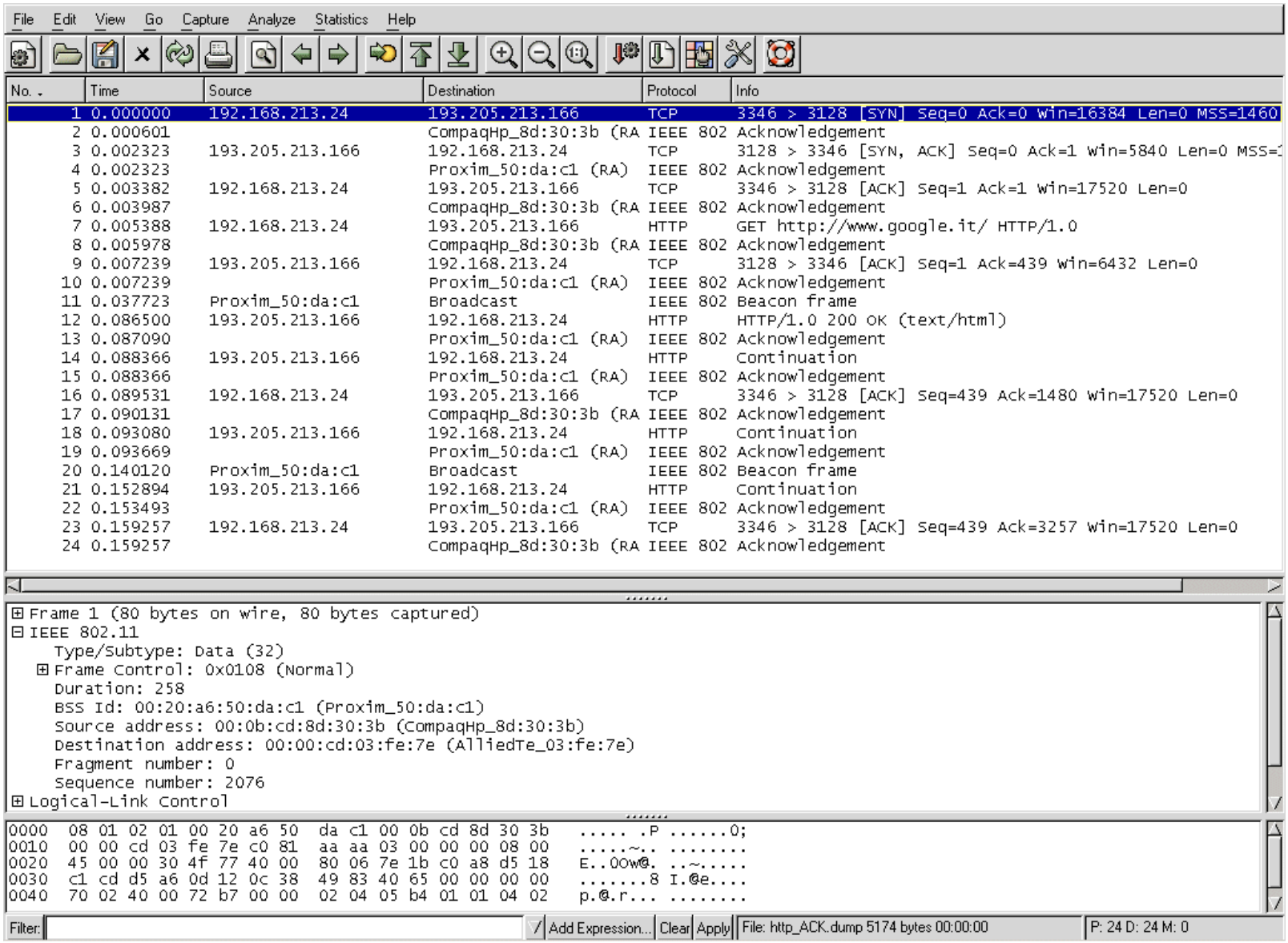
Wireless Network Esercitazioni

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


File Edit View Go Capture Analyze Statistics Help
No. Time Source Destination Protocol Info
1 0.000000 192.168.213.24 193.205.213.166 TCP 3346 > 3128 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
2 0.000601 CompaqHp_8d:30:3b (RA IEEE 802 Acknowledgement
3 0.002323 193.205.213.166 192.168.213.24 TCP 3128 > 3346 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
4 0.002323 Proxim_50:da:c1 (RA) IEEE 802 Acknowledgement
5 0.003382 192.168.213.24 193.205.213.166 TCP 3346 > 3128 [ACK] Seq=1 Ack=1 Win=17520 Len=0
6 0.003987 CompaqHp_8d:30:3b (RA IEEE 802 Acknowledgement
7 0.005388 192.168.213.24 193.205.213.166 HTTP GET http://www.google.it/ HTTP/1.0
8 0.005978 CompaqHp_8d:30:3b (RA IEEE 802 Acknowledgement
9 0.007239 193.205.213.166 192.168.213.24 TCP 3128 > 3346 [ACK] Seq=1 Ack=439 Win=6432 Len=0
10 0.007239 Proxim_50:da:c1 (RA) IEEE 802 Acknowledgement
11 0.037723 Proxim_50:da:c1 Broadcast IEEE 802 Beacon frame
12 0.086500 193.205.213.166 192.168.213.24 HTTP HTTP/1.0 200 OK (text/html)
13 0.087090 Proxim_50:da:c1 (RA) IEEE 802 Acknowledgement
14 0.088366 193.205.213.166 192.168.213.24 HTTP Continuation
15 0.088366 Proxim_50:da:c1 (RA) IEEE 802 Acknowledgement
16 0.089531 192.168.213.24 193.205.213.166 TCP 3346 > 3128 [ACK] Seq=439 Ack=1480 Win=17520 Len=0
17 0.090131 CompaqHp_8d:30:3b (RA IEEE 802 Acknowledgement
18 0.093080 193.205.213.166 192.168.213.24 HTTP Continuation
19 0.093669 Proxim_50:da:c1 (RA) IEEE 802 Acknowledgement
20 0.140120 Proxim_50:da:c1 Broadcast IEEE 802 Beacon frame
21 0.152894 193.205.213.166 192.168.213.24 HTTP Continuation
22 0.153493 Proxim_50:da:c1 (RA) IEEE 802 Acknowledgement
23 0.159257 192.168.213.24 193.205.213.166 TCP 3346 > 3128 [ACK] Seq=439 Ack=3257 Win=17520 Len=0
24 0.159257 CompaqHp_8d:30:3b (RA IEEE 802 Acknowledgement
Frame 1 (80 bytes on wire, 80 bytes captured)
IEEE 802.11
Type/Subtype: Data (32)
Frame Control: 0x0108 (Normal)
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 (AlliedTe_03:fe:7e)
Fragment number: 0
Sequence number: 2076
Logical-Link Control
0000 08 01 02 01 00 20 a6 50 da c1 00 0b cd 8d 30 3b
0010 00 00 cd 03 fe 7e c0 81 aa aa 03 00 00 00 08 00
0020 45 00 00 30 4f 77 40 00 80 06 7e 1b c0 a8 d5 18
0030 c1 cd d5 a6 0d 12 0c 38 49 83 40 65 00 00 00 00
0040 70 02 40 00 72 b7 00 00 02 04 05 b4 01 01 04 02
Filter: Add Expression... Clear Apply File: http_ACK.dump 5174 bytes 00:00:00 P: 24 D: 24 M: 0

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
    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 (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