Wireless Network Esercitazioni

Alessandro Villani
avillani@science.unitn.it

IEEE 802.11b in breve

IEEE 802.11b in breve

- Lo standard 802.11b è parte della famiglia degli standard IEEE 802 che riguarda le specifiche delle Local Area Network (LAN)
- Ad esempio:
  - 802.3 è la specifica per CSMA/CD alla base di Ethernet
  - 802.1q è la specifica delle VLAN
- Gli standard pubblicati sono disponibili all'indirizzo:

http://standards.ieee.org/getieee802/portfolio.html

IEEE 802.11b in breve: Frequenze

- 802.11b opera nella banda ISM (*Industrial, Scientific and Medical*) a 2.4 GHz
- Sono frequnze non licenziate!

Regione	Frequenze
USA	2.4000 – 2.4835 GHz
Europa	2.4000 – 2.4835 GHz
Francia	2.4465 – 2.4835 GHz
Spagna	2.4450 – 2.4750 GHz
Giappone	2.4000 – 2.4835 GHz 2.4710 – 2.4970 GHz

IEEE 802.11b in breve: Frequenze

- In Europa 13 Canali
- La tabella seguente riassume i canali utilizzabili:

Regione	Canali (5MHz)
USA	1 - 11
Europa	1 - 13
Giappone	1 – 13 + 14
Francia	10 - 13
Spagna	10 - 11

IEEE 802.11b in breve: Frequenze

- La frequenza centrale di ciascun canale è riportata nella tabella a fianco
- La frequenza centrale del canale dista 5MHz
- Un canale è largo 22 MHz
- Per non disturbarsi devono distare 25 MHz

3 canali non-overlapping 1,6,11(USA) 1,7,13(EU)

Canale	Frequenza
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz
12	2467 MHz
13	2472 MHz

IEEE 802.11b in breve: Frequenze

Figure 143—European channel selection—non-overlapping

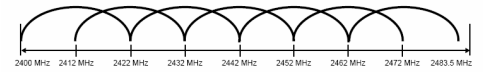


Figure 144—European channel selection—overlapping

IEEE 802.11b in breve: Potenza

- La potenza che può essere irradiata dipende dalle aree geografiche

Potenza Massima Emessa	Regione
1000 mW	USA
100 mW	Europa
10 mW	Giappone

IEEE 802.11b in breve: Velocità

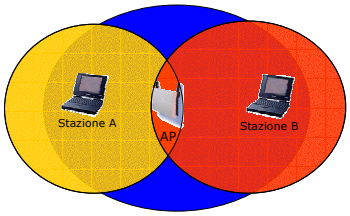
- Le velocità supportate dallo standard sono:

  1, 2, 5.5, 11 Mbps
- La velocità è correlata con la distanza
- La tabella seguente riporta quanto dichiarato da Avaya per i propri AP:

Campo	11 Mbs	5,5 Mbs	2 Mbs	1 Mbs
Ambiente aperto	160 m	270 m	400 m	550 m
Ambiente semi-aperto	50 m	70 m	90 m	115 m
Ambiente chiuso	25 m	35 m	40 m	50 m

IEEE 802.11b in breve: RTS/CTS

- Problema dell'Hidden Node

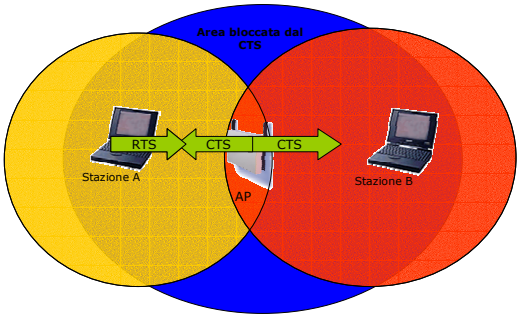


- A comunica con AP (e non con B)
- B comunica con AP (e non con A)

IEEE 802.11b in breve: RTS/CTS

- B trasmette
- A non sente la trasmissione di B e inizia a trasmettere → COLLISIONE
- Per prevenire questa situazione lo standard prevede il meccanismo del RTS/CLS:
  i pacchetti più lunghi di una soglia assegnata vengono trasmessi solo dopo uno scambio RTS/CTS

IEEE 802.11b in breve: RTS/CTS



IEEE 802.11b in breve: WEP

- 802.11 definisce un meccanismo per proteggere la riservatezza dei dati ed autenticare AP/TM:
  WEP (Wired Equivalent Privacy)
- L'algoritmo di crittazione è un RC4 (un sistema di crittazione basato su una chiave condivisa)
- La chiave condivisa è lunga 40 bit ed è concatenata a un vettore di inizializzazione (IV) lungo 24 bit → Chiave a 64 bit

IEEE 802.11b in breve: WEP

- Evoluzione rispetto allo standard: chiave a 128 bit, con chiave condivisa a 104 bit e IV a 24 bit
- Sono state evidenziate vari debolezze del WEP e delle sue implementazioni (chiave troppo corta, prevedibilità dell'IV, ...)

IEEE 802.11b in breve: BSS/ESS

- Un AP e i terminali mobili ad esso associati formano un Basic Service Set (BSS).
- Due o più BSS collegate formano insieme un Extended Service Set (ESS) se forniscono dei servizi aggiuntivi (supporto per il roaming, ...)
- L'Independent Basic Service Set (IBSS), è la forma più semplice → rete Ad Hoc

IEEE 802.11b in breve: SSID

- L'SSID (Service Set IDentiy) è una stringa che identifica la WLAN (max 32 byte)
- L'SSID lungo 0 corrisponde ad una identità di broadcast ed è utilizzato nel probing delle reti disponibili
- Su alcuni AP si può inibire la trasmissione dell'SSID, in modo che solo chi conosce l'SSID della WLAN si possa associare

IEEE 802.11b in breve: DTIM

- **DTIM Period.** Il Delivery Traffic Indicator Map (DTIM) è utilizzato dal TM in power saving mode
- Specifica all'AP quanti periodi di beacon il TM sarà in power saving mode e quando sarà "sveglio" ed in grado di scoprire se ci sono dati diretti al TM stesso

Installazione di un Access Point
Avaya Ap3

Access Point: Avaya AP3

- Access Point Avaya AP3
- Configurabili via seriale:
  - Cavo null-modem
  - Baud Rate: 9600
  - Parity: none
  - Data bit: 8
  - Stop bit: 1
  - Flow Control: none
  - Default passwd: public
  - Line feed con Carriage Returns

Access Point: Boot

```
-------------------------------------
           PowerOn Selftests
-------------------------------------

Running SDRAM test........OK

SDRAM Size: 16 Mbyte

CPU id: 4401a104

CPU Frequency: 228.1 MHz

Checking timers....OK

FLASH Manufacturer: Intel (89)

FLASH Device: E28F320J3A(16)

FLASH Size: 8 Mbyte (32 blocks of 256
kbyte each)

Scanning PCI-Bus...

 SYSTEM SLOT
------------
Vendor ID: Intel Corporation (1011)
Device ID: 21285 (1065)

 SLOT: 1
---------
Vendor ID: National Semiconductor
(100b)
Device ID: DP83815 (0020)

 SLOT: 2
---------
Vendor ID: Texas Instruments (104c)
Device ID: PCI1225 (ac1c)

 SLOT: 3
---------
EMPTY

-------------------------------------
              Selftests OK
-------------------------------------

Executing Original BSP/BootLoader.
Version 2.0.10

Loading image...2641768 + 276792 +
2441816

[Avaya Wireless AP-3]> Please enter
password:
```

Access Point: Configurare via CLI

- Elenco comandi disponibili: ?
- Per una breve descrizione del comando basta non specificare alcun parametro:

```
[Avaya-Wireless-AP-3]> reboot
Command Description:
The reboot command reboots the device in the specified number of
seconds.

Command Usage:
reboot <number of seconds> <CR>

Examples:
reboot 0 <CR>
reboot 100 <CR>
```

Access Point: Configurare via CLI

- Elenco dei parametri visualizzabili:
  show ?
- Elenco dei parametri che iniziano per ip:
  show ip?
- Per l'elenco dei parametri impostabili esattamente come sopra:
  set ip?

Access Point: Configurazione

- Gli AP Avaya hanno di default l'IP 10.0.0.1
- È quindi possibile raggiungerli anche via rete utilizzando un cross oppure uno switch/hub e mettendosi nella stessa sottorete
- Col software allegato c'è anche un tool per trovare gli AP installati

Access Point: Modifica IP Address

- …

```
[Avaya Wireless AP-3]> set ipaddrtype static

[Avaya Wireless AP-3]> set ipaddr 192.168.91.123

[Avaya Wireless AP-3]> set ipgw 192.168.91.1

[Avaya Wireless AP-3]> show network
IP/Network Group Parameters
===========================

IP Address              :               192.168.91.123
Subnet Mask             :               255.0.0.0
Default Router          :               192.168.91.1
Default TTL             :                     64
Address Type            :                  static
```

Access Point: Interfaccia WEB

Access Point: Aggiornare il Firmware

- Il firmware è disponibile all'indirizzo:
  http://support.avaya.com/
- Per aggiornare il firmware si utilizza un server tftp (Trivial File Transfer Protocol)
- Utilizzando la CLI:

```
[Avaya-Wireless-AP-3]> download 193.205.194.21 Avaya/AV_AP3.bin img
File Avaya/AV_AP3.bin is being downloaded from 193.205.194.21.

File Avaya/AV_AP3.bin has been downloaded successfully.

[Avaya Wireless AP-3]> reboot 0
```

Access Point: Aggiornare il Firmware

Access Point: Interfaccie Wireless

- In questi AP si possono inserire diversi tipi di schede con diverse proprietà:
  - Sono supportate due lunghezze massime per la chiave WEP (Silver: 64, Gold: 128)
  - Sono disponibili schede per i diversi set di canali (ETSI: Canali 1-13, World: Canali 1-11)
  - Oltre alle schede 802.11b ci sono moduli 802.11a e 802.11b/g

Access Point: Configurazione

- Oltre ai parametri della rete dovremo configurare per l'interfaccia wireless:
  - Il canale da utilizzare
    - Eventualmente si può impostare la scelta automatica del canale
  - L'SSID della WLAN
    - Eventualmente si abilita il Closed System: non sono autorizzati a connettersi i terminali con SSID any
  - La soglia per l'attivazione del RTS/CTS
    - Di default è disabilitato

Access Point: Configurazione

- In base agli AP potremmo impostare:
  - Più SSID sulla stessa interfaccia wireless
  - Lo standard utilizzato
  - Le velocità supportate
  - La potenza utilizzata
- Altre configurazioni importanti:
  - Cambiare le passwd di amministratore
  - Impostare la chiave WEP
  - Configurare un server con syslog o SNMP
  - Abilitare un server radius per il controllo dei MAC address
  - Abilitare un server 802.1x