Animatori Digitali

1 - Reti

G. Vinciguerra

gvinci@gmail.com

2016

Presentazioni

Chi sono

Guido Vinciguerra

Docente di Laboratorio di Informatica IIS “A. Maserati” - Voghera

Consulente indipendente (sistemista)

Sommario

1. Introduzione
2. Teoria sulle reti, brevi cenni
3. Reti Wireless
4. Orientarsi

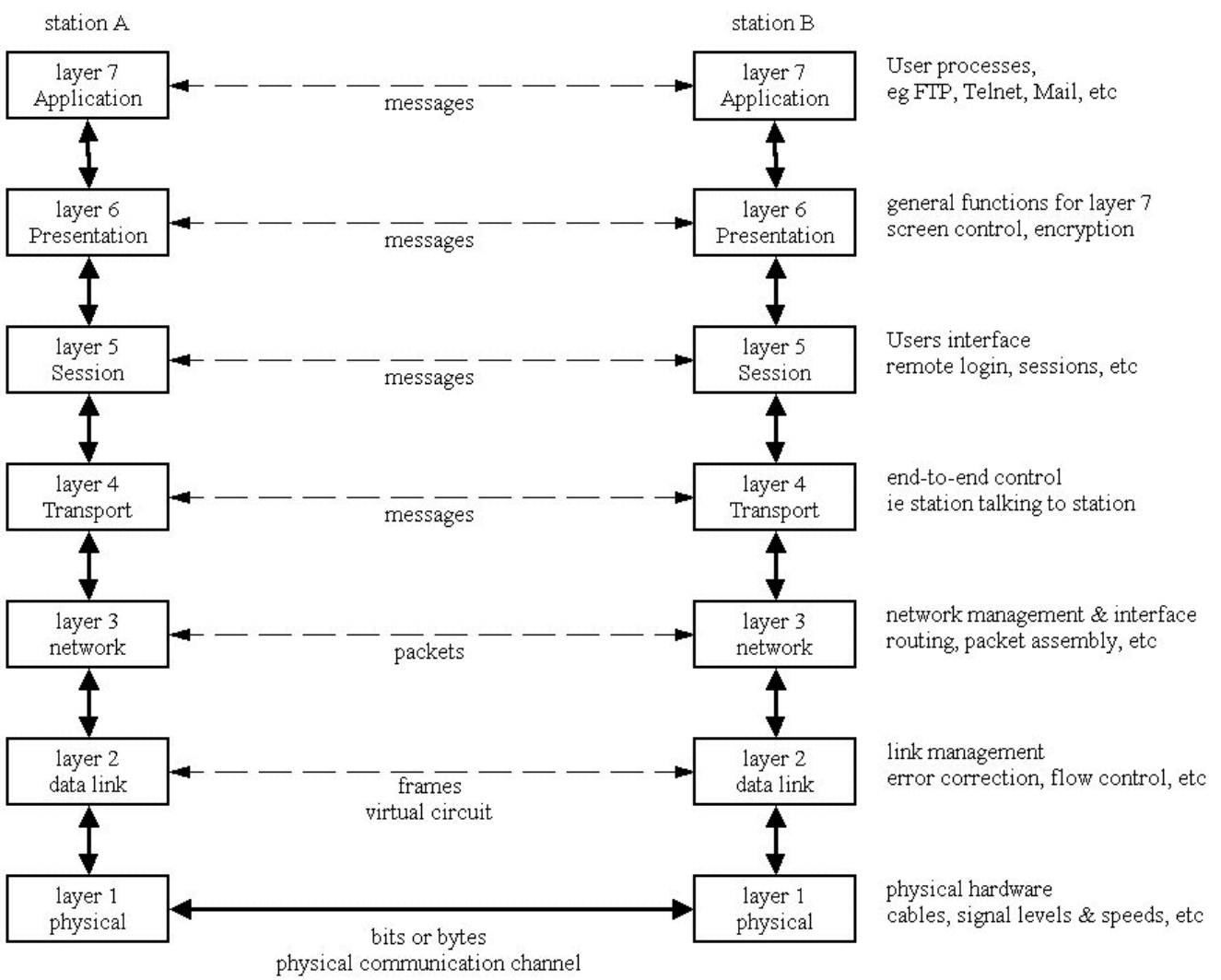
Modello ISO/OSI

Caratteristiche

- Modello teorico che definisce i riferimenti per la progettazione di sistemi di trasmissione dati
- Si basa sul concetto di livello
- Suddivisione dei sistemi in 7 livelli differenziati
- Ogni livello comunica solo con i livelli adiacenti
- Si possono instaurare comunicazioni tra sistemi sono “allo stesso livello”

Modello ISO/OSI

Livelli



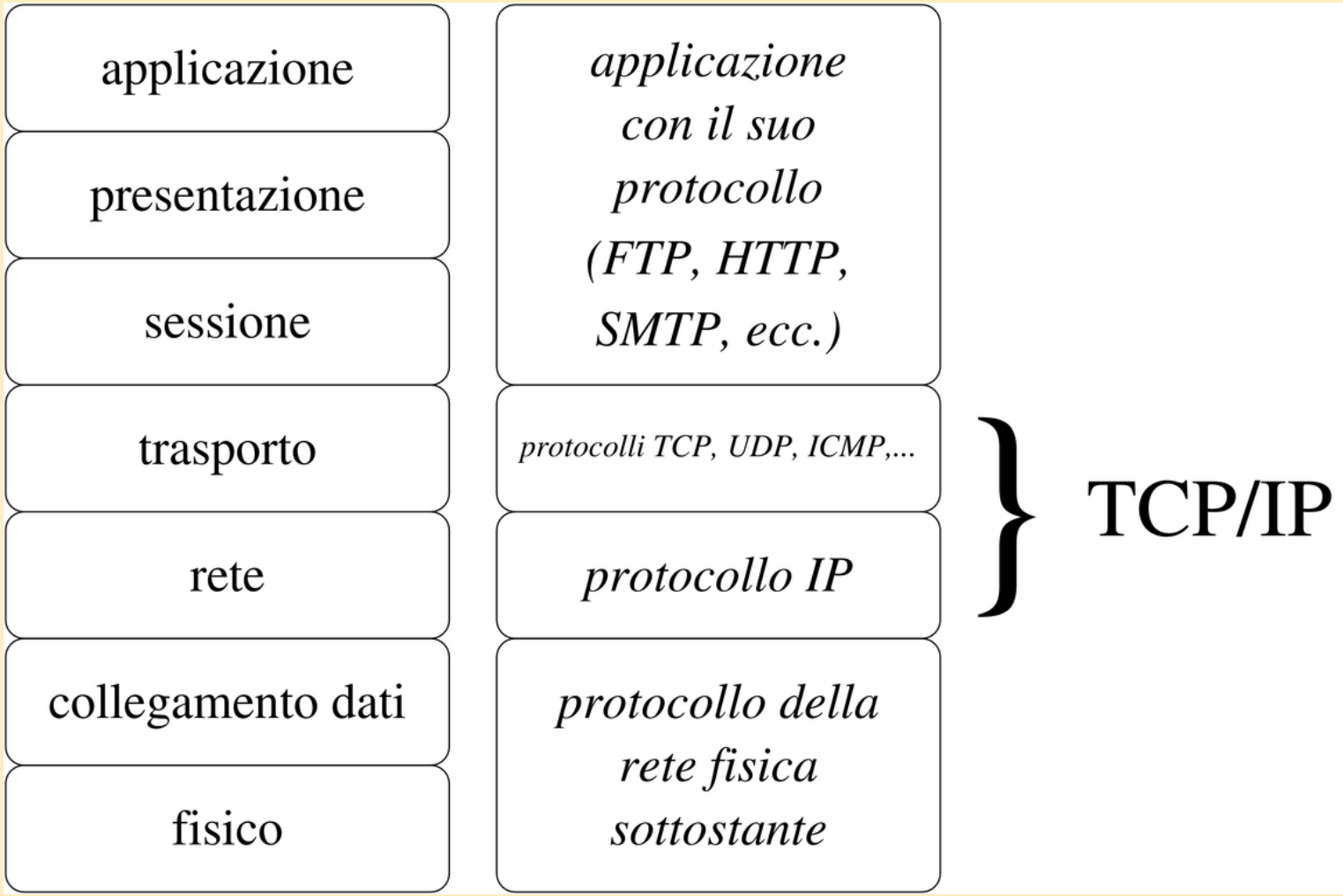
Suite TCP/IP

TCP/IP

- Standard de facto
- Non è un modello ma un gruppo di protocolli
- Basato sul modello ISO/OSI

Suite TCP/IP

Livelli



Suite TCP/IP

Livello 1

- Livello Fisico
- Trasmissione dei segnali (di varia natura) su un canale trasmissivo

Mezzi trasmissivi (per reti locali)

- Rame (doppino telefonico, cavo coassiale): costo ridotto, estensione limitata, ridotta tolleranza ai disturbi, velocità di trasmissione accettabile
- Fibra: costo elevato, elevata estensione, alta tolleranza ai disturbi, velocità di trasmissione elevata
- "Etere": costo elevato, estensione molto limitata, tolleranza ai disturbi bassa, velocità di trasmissione bassa (con tempi di "reazione" lenti)

Livello 1

Apparati

- Repeater
- Repeater Hub

Livello 1

Repeater

- "Rinfresca" il segnale
- Utilizzato quando il mezzo trasmissivo non permette il collegamento a lunghe distanze

Repeater Hub

- Rinfresca il segnale
- Distribuisce il segnale
- ... in modo stupido: ogni segnale che arriva su una porta viene trasmesso su TUTTE le altre
- Attualmente non più fabbricati
- Velocità di trasmissione 10/100 Mb/s
  (... attenzione Mb = Mega bit; MB = Mega byte, ovvero 8 bit)

Livello 2

Caratteristiche

- Livello Data Link
- Divisione dei pacchetti in frame
- Consegna dei pacchetti al destinatario in base a indirizzi MAC o HW

Indirizzi HW

- indirizzo formato da 6 byte espressi solitamente in esadecimale
  es. 74:2f:68:4f:4a:89
- indirizzo HW perché legato alla scheda di rete (NIC) ed univoco a livello mondiale
- indirizzo di broadcast ff:ff:ff:ff:ff:ff

Livello 2

Apparati di livello 2

- Bridge
- Switching Hub

Bridge

- Apparato a due interfacce (ponte)
- Originariamente utile per suddividere segmenti di rete con limitati interazioni
- Successivamente utilizzato per far colloquiare reti di tipo 2 differenti
- Attualmente integrato in molti dispositivi di livello 2

Livello 2

Access Point

Livello 2

Switch

- Apparato a n interfacce (esteticamente molto simile al repeater hub)
- I frame vengono analizzati e lo switch decide su quali porte inoltrarli
- Drastica diminuzione delle collisioni
- Possibilità di trasmissione a banda “piena”
- Possibilità di collegarvi moduli in fibra
- Possibilità di realizzare switch “modulari” aggregando componenti differenti chassis switch
- Velocità di trasmissione 10/100/1000/10000 Mb/s
- Possibilità di utilizzo delle VLAN (802.1Q)

Livello 2

VLAN

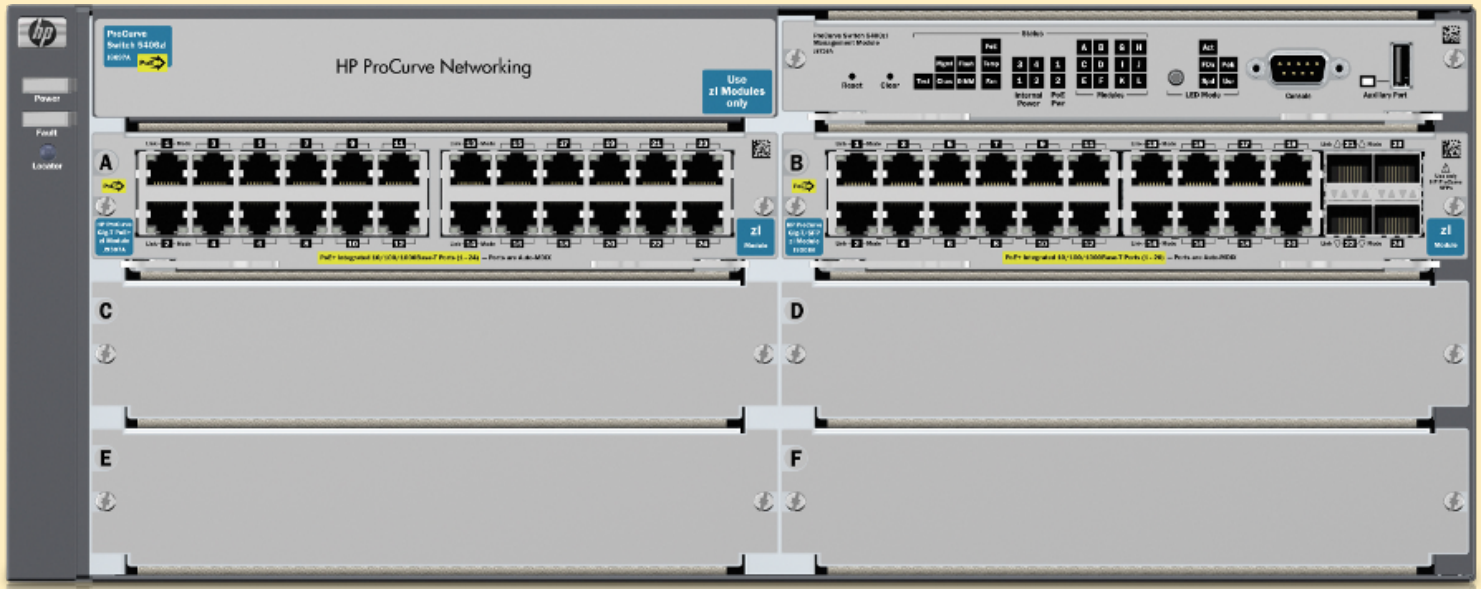
- Suddivisione logica di un dispositivo di livello 2 in più lan
- Convivenza sullo stesso mezzo trasmissivo di più LAN
- Convivenza sulla stessa NIC di più LAN
- Utili per abbattere i costi di cablaggio

Livello 2

Switch

Livello 2

Switch



Livello 3

Caratteristiche

- Internet protocol
- Instradamento dei pacchetti
- Identificazione delle stazioni attraverso un indirizzo (indirizzo IP) composto da 4 byte
- Solitamente rappresentato in forma decimale "puntata"
  es. 192.168.0.1

Indirizzi IP

- Suddivisione dei bit dell'indirizzo in due parti
- Bit che identificano la rete
- Bit che identificano l'host (il sistema)
- 192.168.0.1
  `nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh`
  `11000000.10101000.00000000.00000001`

IP

Host e reti

- Numero di bit per rete ed host definiti da una “maschera”
- Maschera composta da 32 bit i cui primi n ad 1 identificano i bit riservati alla rete (netmask)
  es.
  `nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh`
  `11111111.11111111.11111111.00000000`
  `255.255.255.0`

IP

Classi IP

Gli IP sono stati suddivisi in classi che si differenziano il differente numero di bit dedicati a rete e host in base ai bit iniziali dell'indirizzo

- Classe A: indirizzi che iniziano con 0...
  0 – 127
  8 bit rete - 24 bit host
- Classe B: indirizzi che iniziano con 10...
  128 – 191
  16 bit rete - 16 bit host
- Classe C: indirizzi che iniziano con 110...
  192 – 223
  24 bit rete - 8 bit host

IP

host / rete / broadcast

- Dato un indirizzo IP ed una maschera è possibile determinare l'indirizzo della rete con una semplice AND

```
IP: 192.168.0.1
netmask:  255.255.255.0
11000000.10101000.00000000.00000001
11111111.11111111.11111111.00000000
AND bit a bit
11000000.10101000.00000000.00000000
192.168.0.0
```

- Mettendo a 1 tutti i bit dedicati all'host si trova l'indirizzo di broadcast

```
11000000.10101000.00000000.11111111
192.168.0.255
```

IP

Come si "ragiona" in IP

- Se la stazione A vuole comunicare con la stazione B deve conoscerne l'indirizzo
- La stazione A verifica se è sulla stessa rete del destinatario
- In caso positivo la connessione "passa" a livello 2
- In caso negativo i pacchetti vengono inviati alla stazione (router) che si occupa di instradarli

IP

Routing statico

```
gvinci@toshibone2:~$ /sbin/route -n
Tabella di routing IP del kernel
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.25.0.1      0.0.0.0         UG    0      0        0 wlan0
10.0.0.0        172.20.0.1      255.255.255.0   UG    0      0        0 tap0
10.1.0.0        172.20.0.1      255.255.255.0   UG    0      0        0 tap0
84.253.153.82   172.25.0.1      255.255.255.255 UGH   0      0        0 wlan0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlan0
172.20.0.0      0.0.0.0         255.255.0.0     U     0      0        0 tap0
172.25.0.0      0.0.0.0         255.255.0.0     U     2      0        0 wlan0
192.168.10.0    172.20.0.1      255.255.255.0   UG    0      0        0 tap0
gvinci@toshibone2:~$
```

IP

Indirizzi per reti private

Sono riservati per l'utilizzo in ambito privato alcune classi IP:

- 10.0.0.0/8 per la classe A
- 172.16.0.0/12 per la classe B (ovvero 172.16-31.0.0)
- 192.168.0.0/16 per la classe C (ovviamente con netmask a 24bit)

TCP/IP

NAT

Network Address Translation

- Permette la modifica degli IP dei pacchetti che transitano da un IS/AS
- Source NAT: modifica dell'IP sorgente (masquerade)
- Destination NAT: modifica dell'IP destinazione

TCP/IP

Livello 4

Livello Trasporto

- Gestione delle trasmissioni dei dati tra sorgente e destinazione
- Suddivisione dei protocollo tra connessi e non
- TCP: protocollo connesso utilizzato per trasmissioni affidabili
- UDP: protocollo non connesso utilizzato per trasmissioni veloci

TCP/UDP implementano il concetto di "porta"

- Le porte permetto di instaurare differenti connessioni contemporanee per gestire servizi differenti
- Le porte sono 65536 (2^{16})
- É possibile effettuare il NAT anche delle porte (NAPT)

Wireless

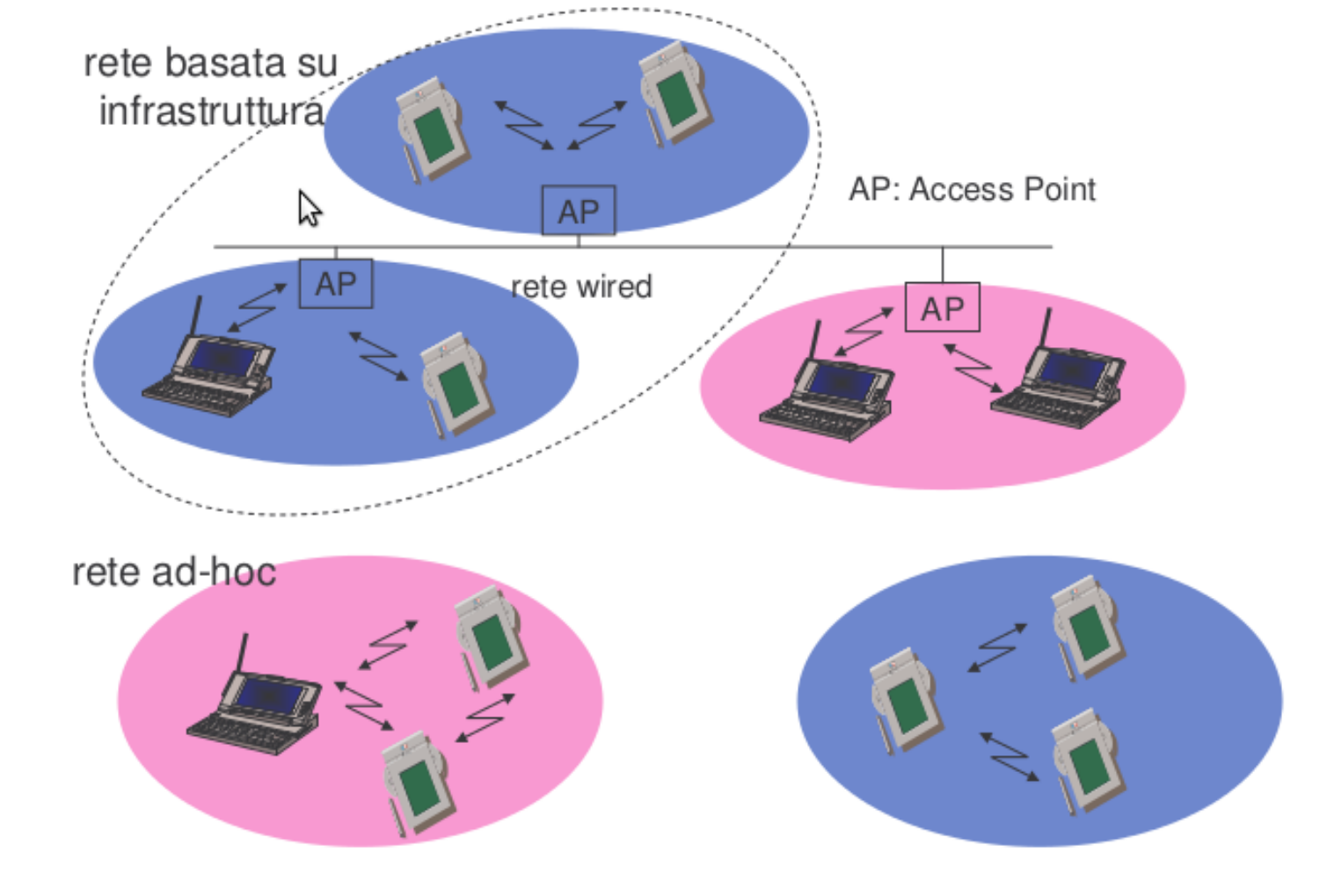
Nomi

- Wireless
- WLAN
- Wi-Fi

Come chiamarle?
Wireless

Introduzione

Ad-hoc e infrastruttura



Infrastruttura

Caratteristiche

- Comunicazione solo tra nodi wireless ed access point (AP)
- AP agisce da bridge verso altre reti wireless o wired (diverse reti wireless formano una rete wireless logica)
- La maggior parte delle funzionalità risiede nell'AP, mentre i client wireless rimangono molto semplici
- Infrastruttura non implica necessariamente la presenza di una rete fissa wired

Standard

IEEE 802.11

- 802.11b
- 802.11a
- 802.11g
- 802.11n

Standard

802.11b

- Nasce nel 1999
- Velocità intorno ai 5.5Mb/s
- Frequenze intorno ai 2.4GHz

802.11a

- Nasce nel 2001
- Velocità intorno ai 54Mb/s (reali 20Mb/s)
- Frequenze intorno ai 5GHz

Standard

802.11g

- Nasce nel 2003
- Velocità intorno ai 54Mb/s (reali 20Mb/s)
- Frequenze intorno ai 2.4GHz (pienamente compatibile con b)
- alcune implementazioni (non standard) accoppiano più canali per avere velocità maggiori

802.11n

- Nasce nel 2007 (draft) 2009 (ufficiale)
- Velocità intorno ai 100Mb/s (reale 52Mb/s)
- Frequenze intorno ai 2.4 GHz o 5 GHz (dual band)
- Utilizza la tecnologia MIMO (antenne differenti per trasmissione/ricezione)

Standard

802.11i

- Migliora i meccanismi di sicurezza ed autenticazione

802.11e

- QoS (Quality of Service) Enhancement

802.11

Un po' di nomenclatura

Access Point

- stazione integrata nella LAN wireless e nel sistema di distribuzione

Stazione (STA)

- terminale con meccanismi di accesso al mezzo wireless e contatto radio con l'access point

Basic Service Set (BSS)

- gruppo di stazioni che usano la stessa radiofrequenza

Distribution System

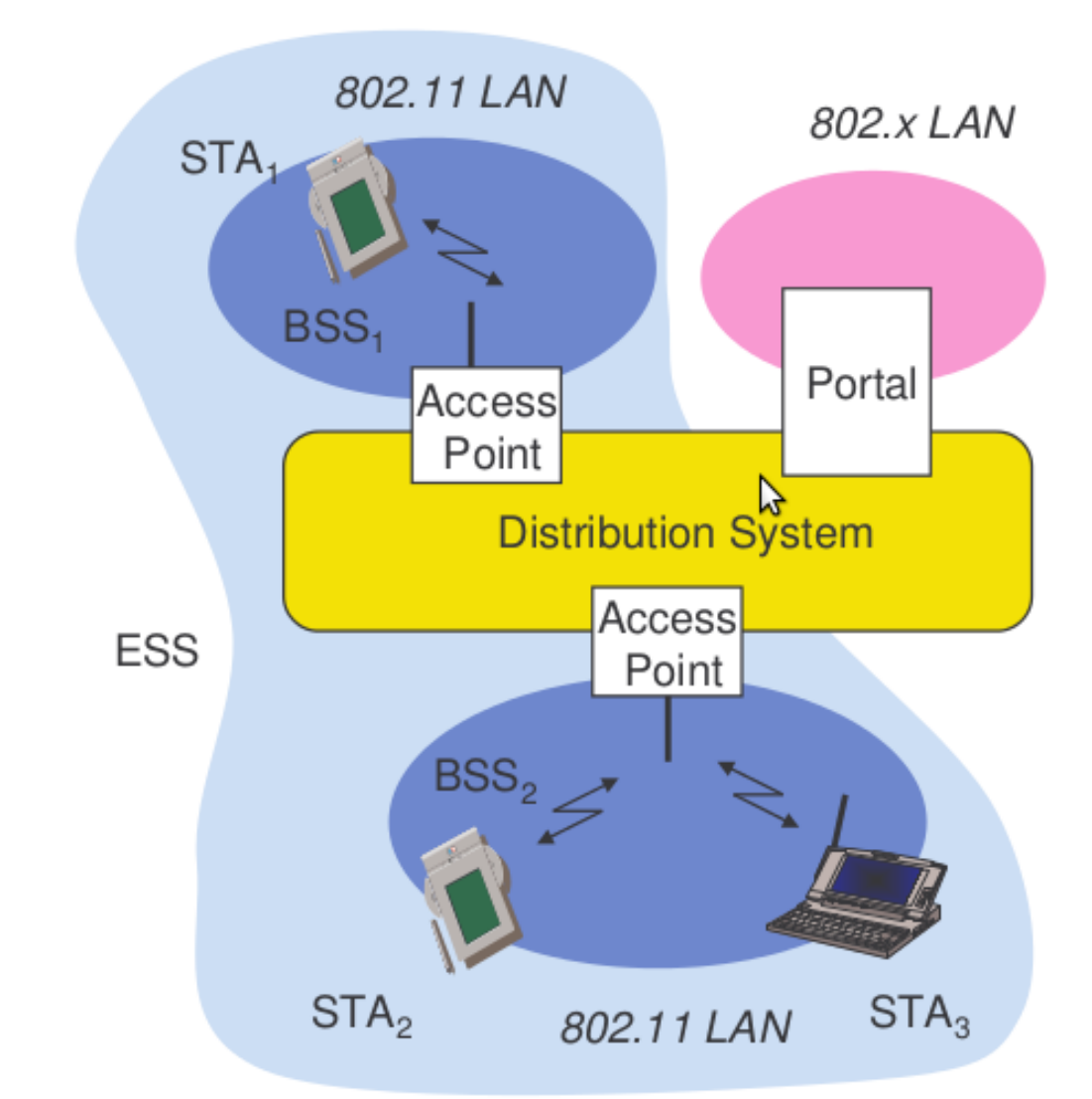
- rete di interconnessione per formare una rete logica basata su diversi BSS (ESS: Extended Service Set)

Portale

- bridge ad altre reti (wired)

802.11

Nomenclatura



Sicurezza

Crittografia

- WEP
  - Wired Equivalent Privacy
  - implementato da tutti gli AP (parte dello standard 802.11)
  - basato su una chiave a lunghezza fissa condivisa
  - si è rivelato poco sicuro violabile in pochi istanti
- WPA
  - Wi-Fi Protected Access
  - Creato come soluzione "tampone" per sopperire ai difetti di WEP
- WPA2 e 802.11i
  - Nasce nel 2004
  - Utilizza la crittografia AES
  - Permette l'utilizzo di una chiave condivisa (PSK)
  - o di chiavi differenti da associare ad ogni client con l'ausilio di un server di autenticazione (Radius)

Reti Wireless

Configurazioni "home"

- Rete aperta
  - Accesso libero non crittografato
  - Privacy nulla
  - Spesso utilizzata con il controllo dei MAC (da definire su ogni AP)
- Rete con PSK
  - Comunicazioni protette da WPA2 Personal
  - Chiave di crittografia condivisa (shared)
  - Spesso utilizzata con il controllo dei MAC (da definire su ogni AP)
  - Con l'aumentare del numero di utenti la configurazione tende a diventare "aperta"

Reti Wireless

Configurazioni "business"

- 802.1x
  - Necessario un server radius per l'autenticazione
  - Configurazione più "complessa" di ogni AP
  - Configurazione più "complessa" di ogni STA
  - Architettura di rete inalterata
  - Permette un accesso realmente protetto ai servizi della rete LAN cablata
- Captive portal
  - Rete aperta
  - Sull'ESS non sono presenti servizi di nessun tipo
  - Per accedere alla rete esterna (tipicamente internet) è necessario autenticarsi su un sito web (captive portal)
  - Il CP generalmente recupera gli utenti da un server (radius)

Architettura fisica

Attività iniziali

- Pianta dell'edificio/area da coprire
- Schema di livello 1, 2 e 3 della rete esistente
- Schema dei collegamenti elettrici
- Definizione degli obiettivi
  (come devo utilizzare la rete? chi la usa? quanti dispositivi?)

Architettura fisica

Note sulla rete elettrica

- Gli AP necessitano di alimentazione elettrica
- Molti AP "moderni" implementano lo standard IEEE 802.3af (Power Over Ethernet)
  Possono essere cioè alimentati direttamente attraverso il cavo di rete
  A tal fine è necessario uno switch che supporti PoE
  (costi raddoppiati rispetto a quelli "standard")
- In alternativa è possibile utilizzare un "iniettore"

Architettura fisica

Copertura

- Il raggio di copertura ideale di un AP varia in base a molti fattori:
  - Potenza dell'emettitore
  - Guadagno
- In un ambiente ideale (campo aperto) un AP mediamente copre un'area di circa 200m di raggio
- Nella realtà in edifici con elementi architettonici ed arredamento variegati una valutazione è molto più complessa
- Possono essere utilizzati metodi empirici per la valutazione della copertura

Architettura fisica

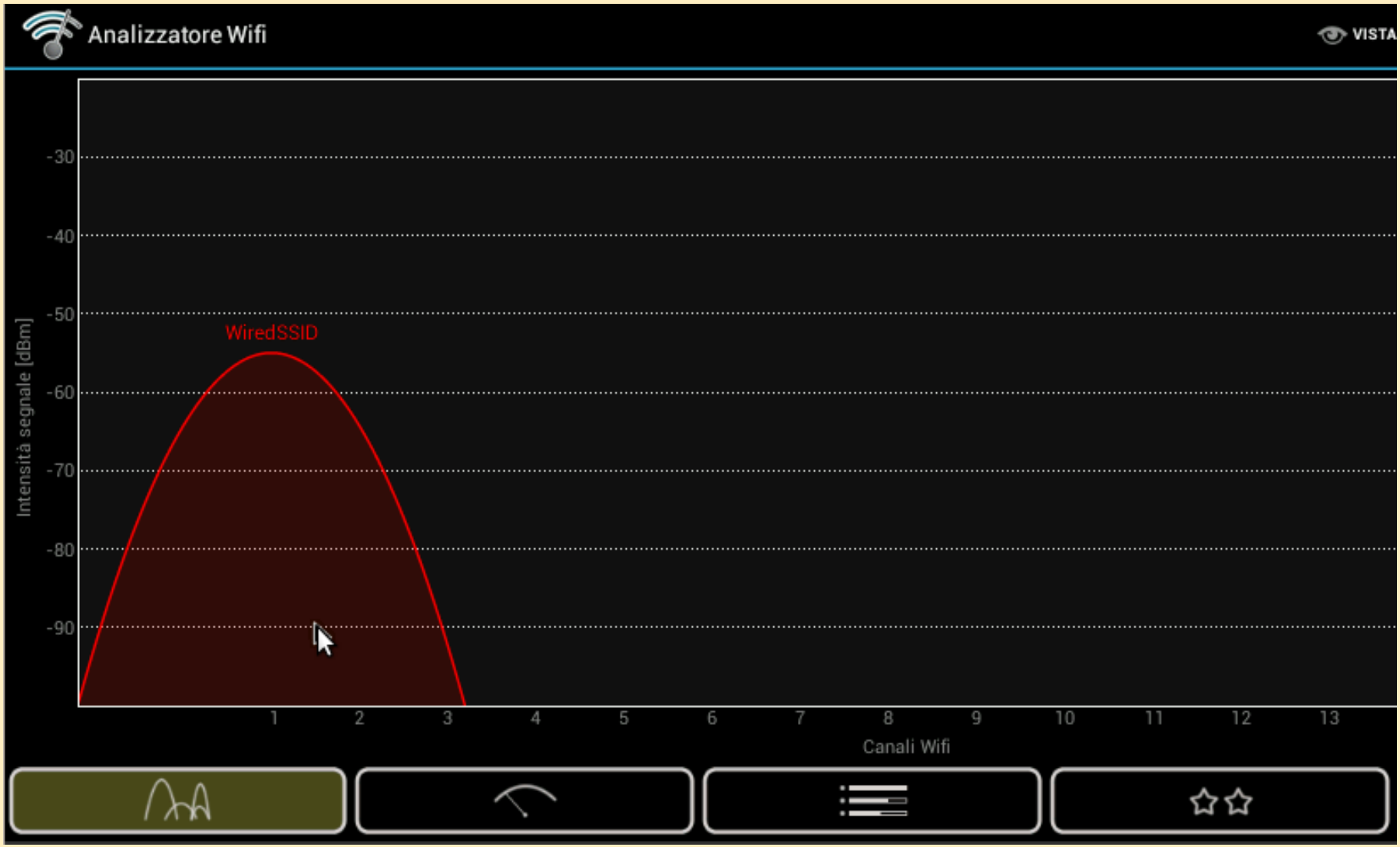
Verifica della copertura

Software di analisi Wi-Fi:

- InSSIDer
  per Windows, MAC, Android
- wavemon
  per GNU/Linux
- Wi-Fi Analyzer
  per Android

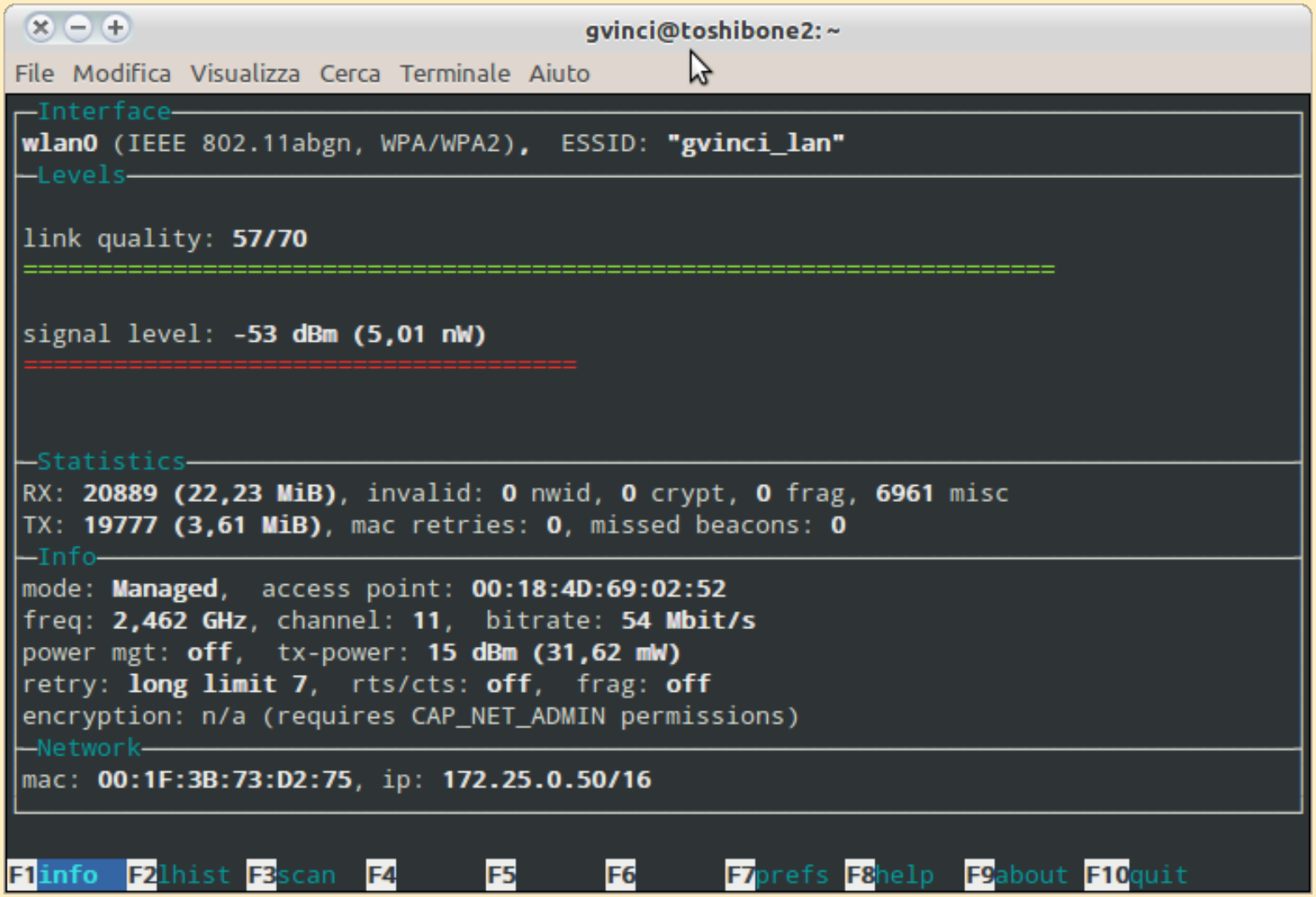
Architettura fisica

Wi-Fi analizer



Architettura fisica

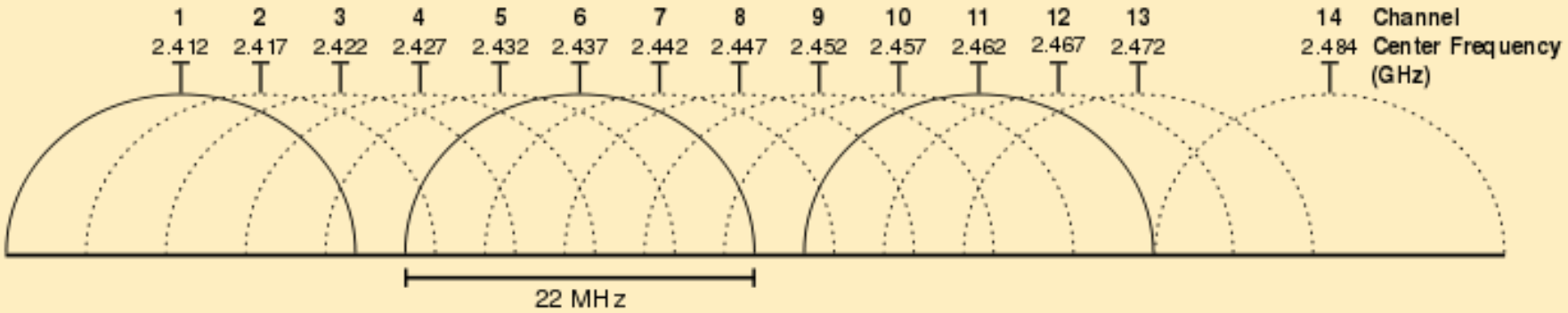
wavemon



Architettura fisica

Sovrapposizione dei canali

- Ogni BSS lavora in un range di frequenze nell'intorno dei 2.4 o 5 GHz
- Negli standard più diffusi b/g/n sono ricavati dei canali da 22MHz che si sovrappongono parzialmente
- BSS vicine che lavorano su canali che si sovrappongono possono "disturbarsi"
- É quindi necessario utilizzare per BSS limitrofe canali "distanti" 5 posizioni l'uno dall'altro



Documentazione

- Avere chiara la situazione
- Poter operare con cognizione di causa in caso di malfunzionamenti
- Poter pianificare con facilità modifiche/espansioni
- Poter pianificare passaggi di consegne meno traumatici
- Poter ottenere consulenze meno onerose e più precise
- Essere indipendenti

Documentazione

Strumenti

- Documenti salvati su pc o server locale (Office, LibreOffice, ecc.)
- Documenti salvati su cloud (Dropbox, Google Drive, ecc)
- Documenti creati su cloud (Google Drive, Office, ecc.)

Scenari

Nella migliore delle ipotesi

- Schema di livello 1
- Schema di livello 2
- Schema di livello 3
- Tipologia di assegnazione IP
- Schema di indirizzamento
- Inventario armadi di rete
- Catalogazione server (molto precisa)
- Procedure di disaster & recovery
- Catalogazione client (grossolana)
- Riferimenti linea internet (assistenza tecnica)

Scenari

Più verosimile

- Tipologia di assegnazione IP
- Schema di indirizzamento
- Catalogazione server

Non così raro

- Tipologia di assegnazione IP

Raro

- ... nessuno sa niente

Scenari

Come operare

- Determinare la configurazione IP generale
- Catalogare apparati di rete (di qualsiasi livello)
- Determinare schema di livello 1
- Determinare schema di livello 2
- Determinare schema di livello 3
- Catalogare i server (IP, funzioni, credenziali accesso)
- Catalogare "grossolanamente" i client (PC, stampanti, ecc.)