Laboratorio di Amministratore di Sistema

3. Progettazione di una rete

3C: Reti wireless

Università di Venezia – Facoltà di Informatica
feb-mag 2014 - A. Memo

ver 2.2

Sommario

1. Tecnologia delle onde radio
2. Terminologia e architetture
3. Standard 802.11
4. 802.11: cenni sul livello MAC
5. Sicurezza
6. Bluetooth *(cenni)*

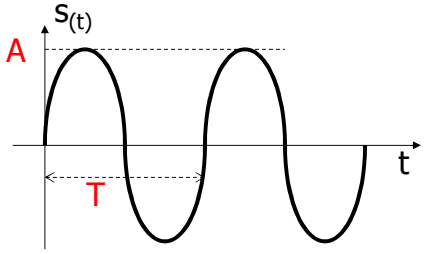
1. Tecnologia delle onde radio

- Frequenze e canali
- Normativa
- Spettro distribuito

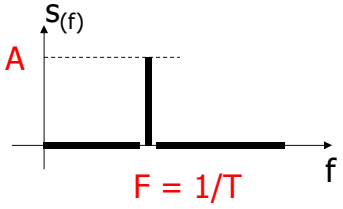
Frequenze e canali (1)

il campo elettromagnetico

la rappresentazione dei segnali nel dominio **spazio/tempo**

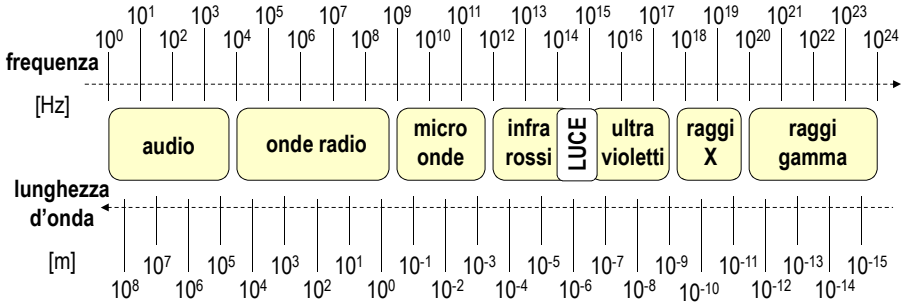


la rappresentazione dei segnali nel dominio della **frequenza**



Frequenze e canali (2)

i concetti di canale, frequenza centrale, banda, spettro



Frequenze e canali (3)

- caratterizzate da frequenza f e lunghezza d'onda λ [c = 299.792.458 m/sec]

$$f \bullet \lambda = c$$

- hanno una interazione differente con i vari materiali in base alla loro lunghezza d'onda

Normativa (1)

in Italia:

- il DPR 30/01/2002 ha modificato il rapporto precedente tra stato e cittadino, basato sulla **concessione**, passando a quello di licenza individuale e autorizzazione globale di servizi di telecomunicazione
- non più solo all'interno di un edificio di proprietà privata, ma anche all'interno del proprio fondo e di collegamento tra due siti (per ora dello stesso proprietario)

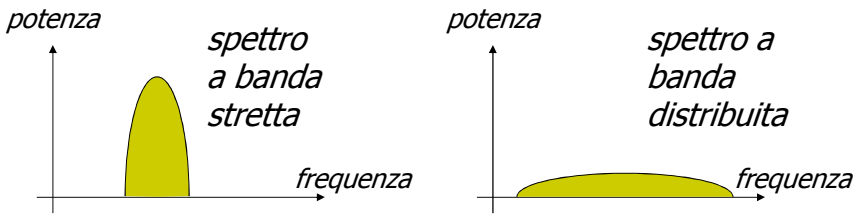
Normativa (2)

nel mondo:

- organismi (l'americano FCC e l'europeo ETSI)
- frequenze ISM (Industriale, Scientifico, Medicale): utilizzo senza licenza ma a potenza irradiata limitata ed in ambito locale
  - UHF ISM 902 - 928 MHz
  - **S-Band ISM** **2,4 – 2,5 GHz** *[microonde e cell]*
  - **C-Band ISM** **5,725 – 5,875 GHz** *[satelliti]*
- lo standard 802.11 divide la S-Band (2.412-2.484 MHz) in 14 canali

Spettro distribuito

- le trasmissioni in banda ISM sono a **spettro distribuito** (*Spread Spectrum*)
- il trasmettitore distribuisce il segnale su un numero elevato di frequenza, al fine di ridurre l'effetto del rumore



2. Terminologia ed architetture

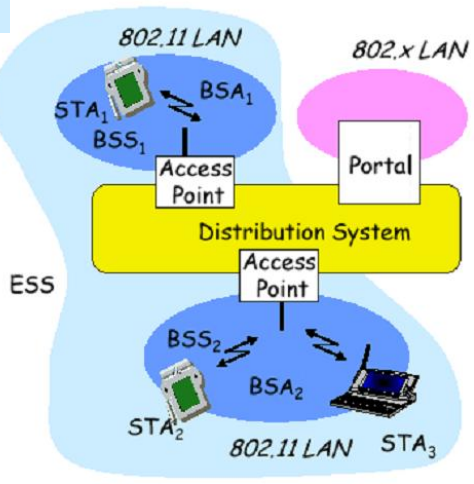
- Glossario wireless LAN
- Architettura reti wireless
- Posizionamento WLAN
- Vantaggi e svantaggi delle reti WLAN

Glossario wireless LAN (1)

- **BSA**, *Basic Service Area*: ogni cella wireless
- **AP**, *Access Point*: interfaccia le aree wired-wireless della LAN, agisce come stazione base per ogni cella
- **STA**, *Station*: una postazione del BSA, detta anche WT, *Wireless Terminal*
- **DS**, *Distribution System*: interconnette più BSA
- **BSS**, *Basic Service Set*: il gruppo di stazioni che operano in un BSA
- **ESS**, *Extended Service Set*: un gruppo di BSS collegate ad una wired LAN tramite AP

Glossario wireless LAN (2)

ESS	**Extended Service Set**
DS	**Distribution System**
AP	**Access Point**
BSS	**Basic Service Set**
BSA	**Basic Service Area**
STA	**Station**



Architettura wireless LAN (1)

- si basa su una struttura cellulare simile al GSM
- le reti wireless possono essere divise in
  - **AD HOC** LAN, stazioni in grado di comunicare direttamente tra loro senza Access Point (dette anche IBSS, da *Indipendent BSS* o *peer-to-peer*)
  - **INFRASTRUCTURED WIRELESS** LAN, stazioni che comunicano tra loro utilizzando uno o più *Access Point*, collegati da un *Distribution System*

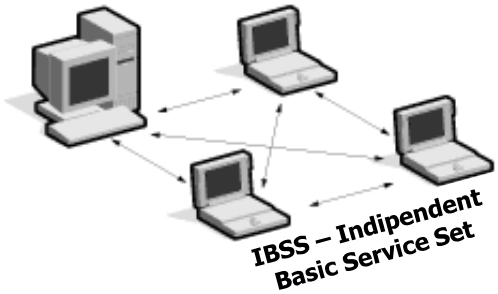
Architettura wireless LAN (2)

compiti degli Access Point:

- collegamento tra rete wireless e rete cablata
- autenticazione, associazione e riassociazione (***roaming***)
- gestione del risparmio energetico delle stazioni (*Power Save Mode*)
- sincronizzazione, in modo che tutte le stazioni agganciate ad un AP siano agganciate ad un clock comune

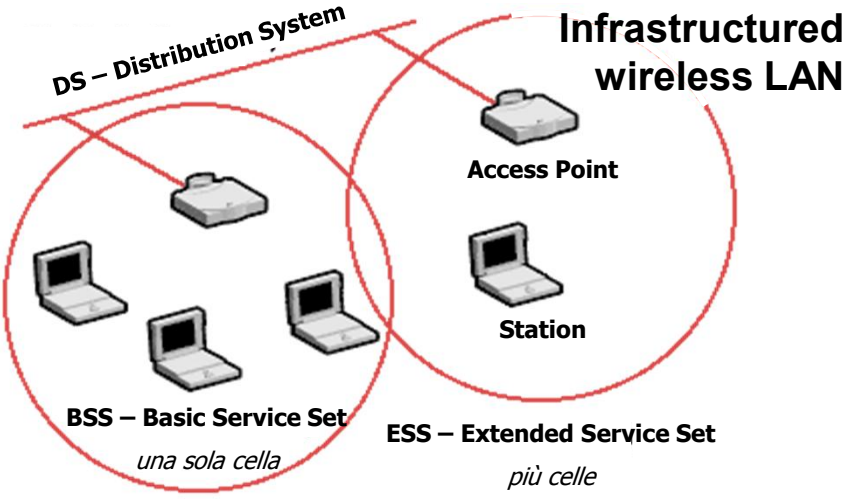
Architettura wireless LAN (3)

Ad Hoc wireless LAN



N.B.: gli host delle reti Ad Hoc devono volgere anche funzioni di router (instradamento distribuito e dinamico)

Architettura wireless LAN (4)



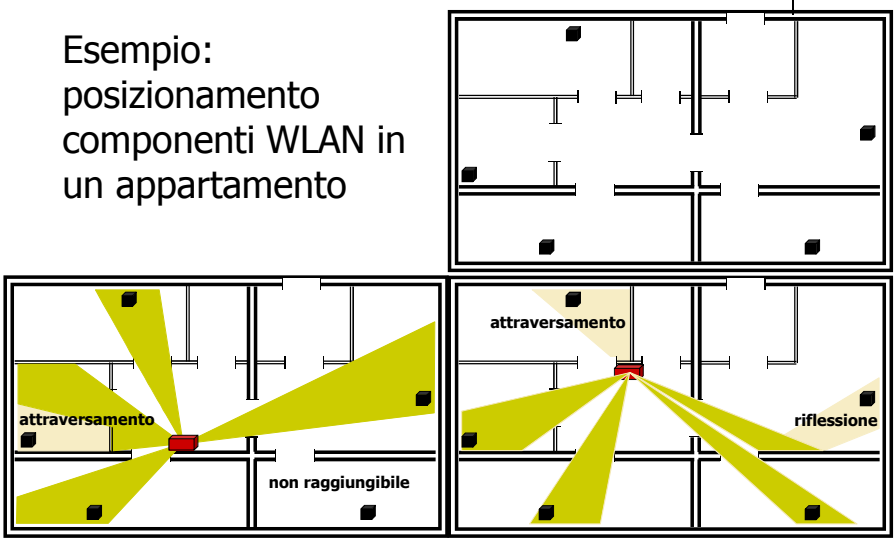
Posizionamento WLAN (1)

Elementi da considerare:

- Access Point baricentrico e a mezza altezza
- utenti allineati otticamente all'Access Point
- attenzione alle schermature metalliche
- analisi delle riflessioni
- analisi degli attraversamenti strutturali

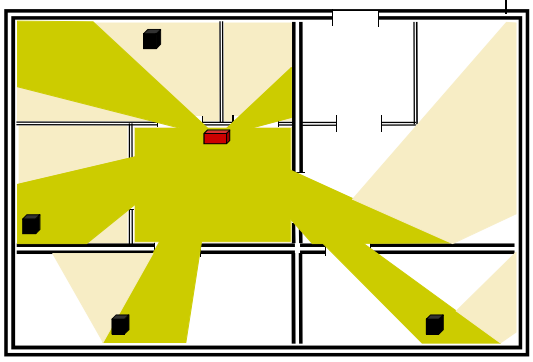
Posizionamento WLAN (2)

Esempio: posizionamento componenti WLAN in un appartamento



Posizionamento WLAN (3)

calcolo della **copertura totale**



area RAGGIUNGIBILE DIRETTAMENTE **37%**
area RAGGIUNGIBILE con UN ATTRAVERSAMENTO **17%**
area RAGGIUNGIBILE CON RIFLESSIONE **18%**
area NON RAGGIUNGIBILE **28%**

Vantaggi delle reti WLAN

- costi e tempi della messa in opera
- non sensibile a degradazione e rottura dei media
- motivazioni di natura logistica
- facilità di riorganizzazione, reti temporanee
- mobilità
- scalabilità
- flessibilità

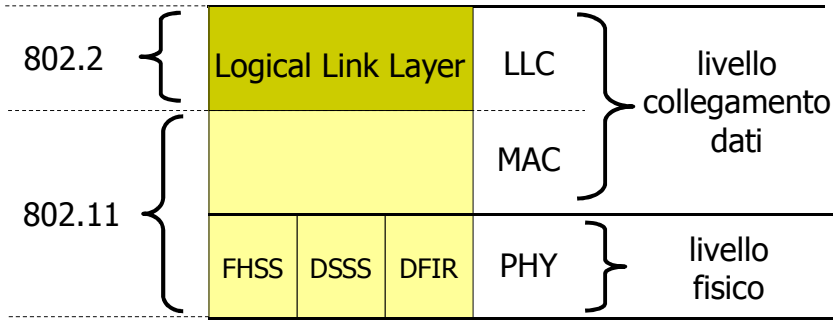
Svantaggi delle reti WLAN

- inaffidabilità del mezzo
- sicurezza
- gestione del roaming
- multipath fading in ricezione
- consumo energetico
- limitata estensione
- limitata standardizzazione
- inquinamento elettromagnetico

3. Standard 802.11

- Standard 802 per le reti LAN
- Evoluzione dell'802.11

Standard 802 per le reti LAN



802	generalità ed architettura di rete	802.5	Token Ring
802.1	protocolli LAN di alto livello	802.11	Wireless LAN
802.2	Logical Link Control e Bridging	802.15	Wireless PAN
802.3	Ethernet	802.16	WiMAX

Evoluzione dell'802.11 (1)

802.11	(*legacy*) approvato nel 1997, revisionato nel 1999 banda da 2,4 GHz, da 1 a 2 Mbps
	nel '99 si è evoluto in due rami
802.11a	rilasciato nel 1999, PHY per WLAN a 5,2 / 5,4 / 5,8 GHz, fino a 54 Mbps
802.11b	approvato nel 1999, PHY più veloce, 2,4 GHz, da 5,5 ad 11 Mbps
802.11g	rilasciato nel 2002, PHY per WLAN a 2,4 GHz, fino a 54 Mbps
802.11n	avviato nel 2004, draft nel 2007, approvato 2009, dual band se usa sia 2,4 che 5,4 Mbps, fino a 300 Mbps
802.11i	*tratta il miglioramento della sicurezza*

Evoluzione dell'802.11 (2)

Specification	Connection Speed	Radio Frequency
802.11	1 or 2 Mbps	2.4 GHz
802.11a	Up to 54 Mbps	5.2-5.4-5.8 GHz
802.11b	5.5 and 11 Mbps	2.4 GHz WiFi
802.11g	Up to 54 Mbps	2.4 GHz
802.11n	Up to 300 Mbps	2.4 e/o 5.4 GHz

La Sicurezza (1)

- Il wireless è un sistema intrinsecamente insicuro
- le onde radio possono attraversare i limiti fisici ambientali ed essere intercettate

La Sicurezza (2)

Tecniche di protezione:

- sicurezza fisica *(limitazione del campo)*
- disabilitazione del DHCP
- Access Point con indirizzo dinamico
- autenticazione dell'accesso
- controllo dell'accesso ai dati
- riservatezza dei dati accessibili

La Sicurezza (3)

Protocolli utilizzabili:

SSID – Service Set Identifier

- etichetta identificativa della rete
- comune a tutti i dispositivi di una WLAN

Cifratura dei messaggi: WEP, WPA, WPA2

WEP – Wired Equivalent Privacy *(1999)*

- chiave di codifica dei dati in trasmissione lunga 64 o 128 bit (40 o 104 + *Initial Vector*)
- schema di crittografia a chiave simmetrica
- *non sicuro (decifrato nel 2003), ora considerato un sottogruppo di WAP*

La Sicurezza (4)

WPA – WiFi Protected Access *(2003)*

- Usa il protocollo TKIP (*Temporal Key Integrity Protocol*) che cambia dinamicamente ad ogni pacchetto la chiave di cifratura in uso combinata con l'*Initial Vector*.
- Utilizzato per l'autenticazione degli utenti
- Autenticazione a chiave unica condivisa, chiamata pre-shared key (lunga 128 bit + 48 bit di Initial Vector)
- *non sicuro, è stato decifrato nel 2009*

WPA2 AES – WiFi Protected Access v2 *(2008)*

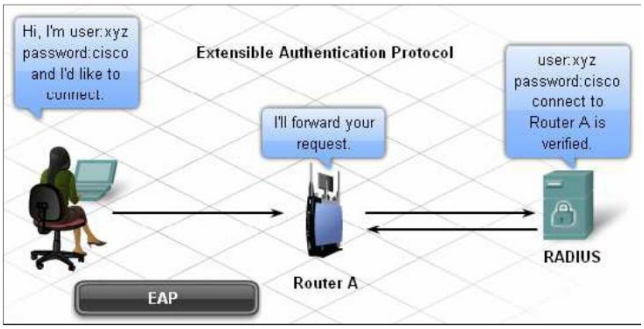
- Adotta un diverso schema di crittografia (AES, da Advanced Encryption Standard)
- *Attualmente ritenuto sicuro*

Autenticazione (1)

- L'autenticazione può avvenire in tre modi:
  - **autenticazione aperta** (senza autenticazione)
  - a **chiave pre-condivisa** (PSK, da Pre-Shared Key), in cui client ed AP vengono configurati con la stessa chiave. L'AP invia una stringa casuale al client, che la cifra con la chiave preimpostata e la restituisce all'AP. Se la stringa ricevuta è decifrabile con la stessa chiave, il client è autenticato
  - ad **autenticazione estensibile** (EAP)

Autenticazione (2)

- ad **autenticazione estensibile** (EAP), quando l'utente comunica con un server di autenticazione interno (backend), ad esempio RADIUS



Cifratura (1)

Wired Equivalency Protocol (WEP)

- *si basa su una autenticazione del tipo a chiave pre-condivisa*
- *La chiave è una stringa di numeri o caratteri lunga 64 o 128 bit*
- *alcuni usano il MAC address del client come chiave (devono essere inseriti manualmente nell'AP)*

Wi-Fi Protected Access (WPA)

- *La chiave è ancora lunga da 64 a 256 bit*
- *Ora però viene generata automaticamente e rimane valida solo per una connessione (TKIP)*

Cifratura (2)

Wi-Fi Protected Access (WPA2-AES)

- *adotta l'algoritmo di cifratura a blocchi AES, da **Advanced Encryption Standard** che garantisce un maggior livello di sicurezza del precedente DES (Data Encryption Standard)*

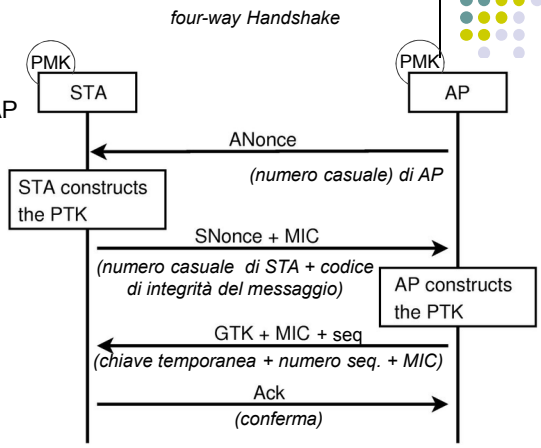
Cifratura (3)

Problemi da risolvere:

- STA deve autenticarsi presso AP
- Entrambi devono stabilire la chiave di sessione PTK

Soluzione:

1. Tramite EAP (autenticazione tramite RADIUS) STA ed AP si autenticano e calcolano localmente la PMK comune
2. Per evitare di scambiarsi la PMK ma per ottenere lo stesso una PTK valida →



PTK	Pairwise Transient Key (o chiave temporanea di sessione) derivata da
PMK	Pairwise Master Key (o chiave di sessione)
GTK	Group Temporary Key (per eventuale multicast)
MIC	Message Integrity Code
nonce	numero valido una volta sola

- PMK
- MAC_{STA}
- MAC_{AP}
- ANonce
- SNonce

La Sicurezza ambientale

- ci sono pareri discordanti sull'influenza dei campi elettromagnetici nell'uomo
- l'A.P. di norma non è classificabile come dannoso (installazione distante dall'uomo, consigliata almeno di 3 m)
- la vera fonte *'pericolosa'* è la scheda dell'WT (si pensi ad un laboratorio wireless)
- un cordless DECT funziona tra i 1880 e 1900 MHz, ed ha una potenza media di 10-20 mW, di picco di 250-600 mW
- un cellulare GSM ha una potenza di picco di 250 mW se opera a 900 MHz o di 125 mW se opera a 1800 MHz
- Un AP ha una potenza di picco di 100 mW ed opera alle frequenze tra 2412 e i 2472 MHz.
- La dannosità delle emissioni radio diminuisce con l'aumentare della frequenza

Qualcosa sta cambiando

- Riconosciuti solo riscaldamenti corporei temporanei
- Gli effetti dipendono dalla frequenza, dall'intensità e dal tempo di esposizione
- Francia ed Inghilterra vietano l'uso dei cellulari nelle scuole primar
- Le ditte di telefonini stanno introducendo avvertenze

Exposure of the general public			Occupational exposure limits		
Power frequency (50 Hz) ELF			**Power frequency (50 Hz) ELF**		
Electric Field strength:	-,--	V/m	Electric Field strength:	1000	V/m
Magnetic flux density:	3	μT	Magnetic flux density:	500	μT
Radiofrequency 1 (900 MHz)			**Radiofrequency 1 (900 MHz)**		
Electric Field strength:	6	V/m	Electric Field strength:	90	V/m
Magnetic flux density:	0,02	μT	Magnetic flux density:	0,30	μT
Power density:	0,1	W/m^2	Power density:	22,5	W/m^2
Radiofrequency 2 (1.800 MHz)			**Radiofrequency 2 (1.800 MHz)**		
Electric Field strength:	6	V/m	Electric Field strength:	127	V/m
Magnetic flux density:	0,02	μT	Magnetic flux density:	0,42	μT
Power density:	0,1	W/m^2	Power density:	45	W/m^2
Radiofrequency 3 (2.100 MHz)			**Radiofrequency 3 (2.100 MHz)**		
Electric Field strength:	6	V/m	Electric Field strength:	137	V/m
Magnetic flux density:	0,02	μT	Magnetic flux density:	0,45	μT
Power density:	0,1	W/m^2	Power density:	50	W/m^2

7. Bluetooth (1)

Rete che permette il trasferimento di informazioni senza cavi tra dispositivi adiacenti di piccole dimensioni

Bluetooth (2)

- operano nella banda dei **2,4 GHz** (interferenze con 802.11x !!!)
- utilizza la tecnica FHSS
- throughput massimo di 1 Mbps
- utilizzano la tecnica TDD, *Time Division Duplex*
- potenze emesse divise per classe
  - classe 1 = 100 mW USB pen
  - classe 2 = 2,5 mW agenda elettronica
  - classe 3 = 1 mW vivavoce

Bluetooth (3)

- si creano piccole reti wireless dette **WPAN**, *Wireless Personal Area Network*
- nello standard Bluetooth vengono chiamate **piconet**, e possono collegare fino a 8/16 dispositivi
- più *piconet* possono collegarsi tra loro, formando una **scatternet**
- gestiscono sia dati che voce
- per determinare i servizi disponibili in un dispositivo si utilizza il protocollo **SDP**, *Service Discovery Protocol*

Bluetooth (4)

Adotta due possibili tecniche di comunicazione:

- **ACL**, *Asynchronous ConnectionLess*, trasmissione asincrona di solo dati alla velocità di
  - 434 Kbps (simmetrica)
  - 723 Kbps / 57,6Kbps (asimmetrica)
- **SCO**, *Synchronous Connection Oriented,* trasmissione sincrona bidirezionale di 64 Kbps di dati e fonia

Infrarossi

- lunghezza d'onda tra 850 e 950 nm
- luce diffusa
- distanza massima di 10 m
- solo per uso interno
- migliora la sicurezza, dato che diminuiscono le possibilità di intrusione
- banda più ampia ⇨ maggiori prestazioni
- una minore copertura e mobilità
- normalmente sfrutta la riflessione del soffitto