assioma sa
Via Vergiò 8
CH-6932 Breganzona
Tel +41 (0)91 961 21 61
Fax +41 (0)91 961 21 62
www.assioma.ch

"Wireless LAN: usi ed abusi"

Agenda

- TECNOLOGIA
- SCENARI D'IMPLEMENTAZIONE
- PROBLEMATICHE DI SECURITY
- RACCOMANDAZIONI
- LINKS & TOOLS
- ULTERIORE DOCUMENTAZIONE

Tecnologia

WLAN: trasmissione dati senza filo, tecnologia radio SST

- Spread Spectrum Tecnology
- nata durante la seconda Guerra Mondiale
- normativa europea ETSI
- architettura cellulare
- algoritmi di compressione, protezione ed encryption
- limitazione disturbi radio
- bassa potenza

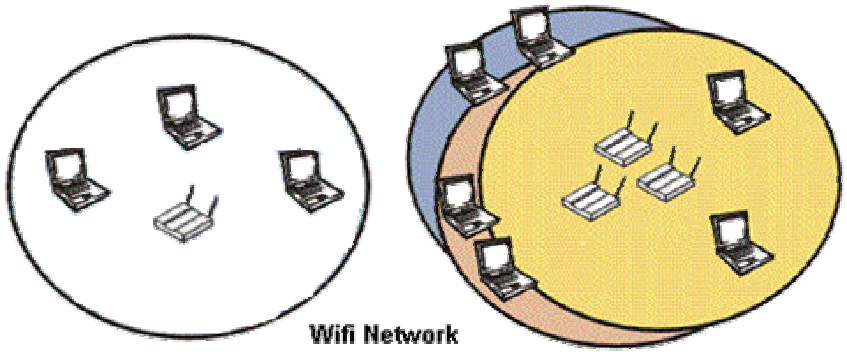
Standard IEEE 802

802.1	Internetworking
802.2	LLC (Logical Link Control)
802.3	CSMA/CD - Ethernet
802.4	Token Bus LAN
802.5	Token Ring LAN
802.6	MAN (Metropolitan Area Network)
802.7	Broadband Techincal Advisory Group
802.8	Fiber-Optic Techical Advisory Group
802.9	Integrated Voice/Data Networks
802.10	Network Security
802.11	**Wireless Networks**
802.12	100 Base VG – AnyLAN, Demand Priority Access Lan

Tecnologia

IEEE 802.11

- banda ISM (Industrial Scientific Medical)
- spread spectrum = maggior robustezza rispetto a IR
- 1997 = standard IEEE 802.11 (1 o 2 Mbps)
- scarso successo, velocità scarsa



Tecnologia

IEEE 802.11b = Wi-Fi (Wireless Fidelity)

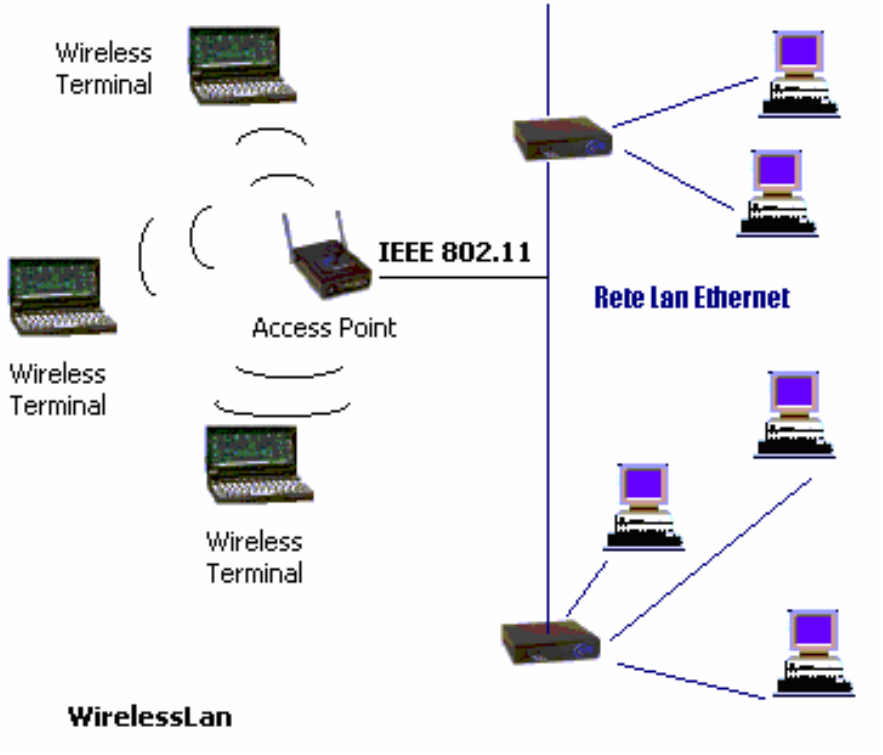
- da 5.5 a 11 Mbit/s
- compatibilità con lo standard precedente
- scarso successo, velocità scarsa
- 1999 = WECA (Wireless Ethernet Compatibility Alliance)
- Nokia, 3Com, Apple, Cisco System, Compaq, IBM,ed altre
- obiettivi = certificazione, interoperabilità e compatibilità

Standard	Frequenza / Data Rate
IEE 802.11	2,4 Ghz / 1-2 Mbps
IEE 802.11b (Wi-Fi)	**2,4 Ghz / 5,5 - 11 Mbps**
IEE 802.11a (Wi-Fi 5)	**5- 40 Ghz / fino a 54 Mbps**
IEE 802.11g	2,4 Ghz / fino a 54 Mbps
IEE 802.15.1	nuovo standard

Tecnologia

Wi-Fi (IEEE 802.11b) - Caratteristiche

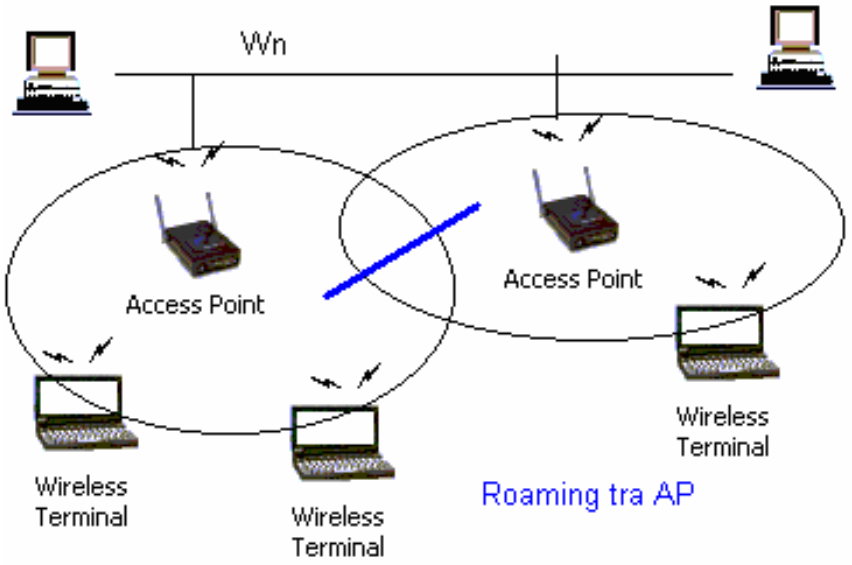
- specifiche per il livello fisico (Phisical Layer) e MAC (Media Access Control) per la realizzazione di WLAN
- come estensione, o alternativo ad una rete fissa
- Access Point (Ap) = bridge che collegano la sottorete wireless con quella cablata
- Wireless Terminal (WT) = dispostivi che usufruiscono dei servizi di rete
- I WT possono essere qualsiasi tipo (MT)



Tecnologia

Wi-Fi (IEEE 802.11b) - Caratteristiche

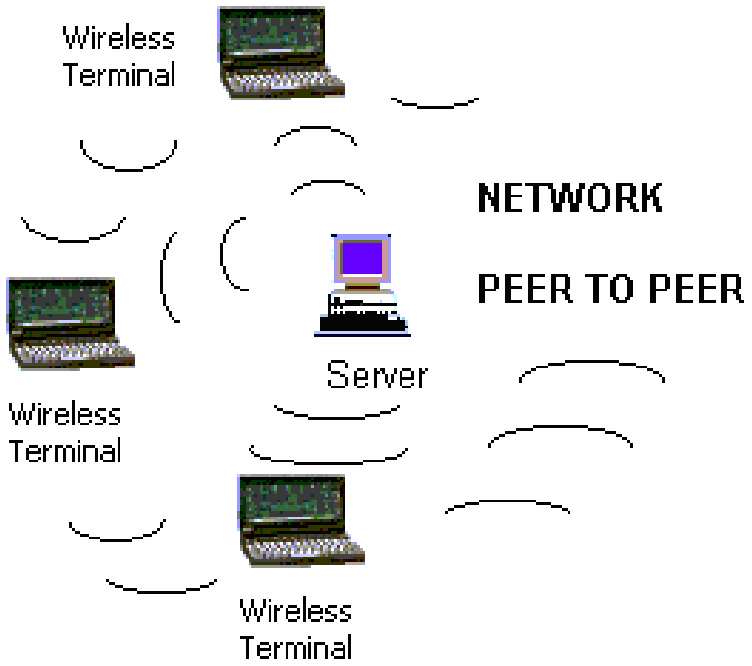
- tipologia "Client Server"
- più dispositivi di rete su un Access Point
- roaming tra access point = mobilità operativa



Tecnologia

Wi-Fi (IEEE 802.11b) - Caratteristiche

- modalità “ad hoc” o “infrastructure”
- protocollo MAC CSMA/CA
- WEP (Wired Equivalent Privacy) = autenticazione e cifratura
- WEP 64 bit = secret key (chiave segreta) 40 bit + IV a 24 bit
- WEP 128 bit = dove si ha una chiave a 104 bit con IV a 24 bit
- WEP 156 e 256 bit = nuove implementazioni



Tecnologia

Wi-Fi (IEEE 802.11b) - Caratteristiche

- Tecniche di modulazione
  - FHSS = spettro espanso a salto di frequenza
  - DSSS = spettro espanso a modulazione di sequenza diretta

Tecnologia

Wi-Fi (IEEE 802.11b) – DSSS (Direct Sequence Spread Spectrum)

- A “sequenza diretta” e “banda larga”
- Ogni bit ridondato in sequenze dette “chip”
- Vantaggi:
  - maggior banda di trasmissione radio
  - miglior ricezione
  - integrità del segnale
  - maggior robustezza, distribuendo il segnale attraverso l'intero spettro di frequenze
  - Il segnale non rimare stabile su una singola frequenza, consentendo a più utenti di operare simultaneamente
  - Interoperabile con 802.11 (1-2 Mbps)

Tecnologia

Wi-Fi (IEEE 802.11b) – FHSS (Frequency Hopping Spread Spectrum)

- il segnale ad una data frequenza viene fatto "saltare" da una canale all'altro (1 Mhz), distribuendosi su una una banda di frequenze (fino a 1600 hops/s)
- Gamma di frequenza: 2402-2480 Ghz (totale 79 hops-set)
- Utilizzata da “Bluetooth”
- Non equivale a maggiore sicurezza
- Vantaggi:
  - buona immunità all'interferenza
  - consente a più utenti di condividere lo stesso insieme di frequenze cambiando automaticamente la frequenza di trasmissione
  - maggiore stabilità di connessione
  - riduzione delle interferenze tra canali di trasmissione

Tecnologia

Wi-Fi (IEEE 802.11b) - Caratteristiche

- velocità di trasmissione dati variabile per adattarsi al canale un data rate fino a 11 Mbps (1, 2 , 5.5, 11)
- scelta automatica della banda di trasmissione meno occupata
- scelta automatica dell'access point in funzione della potenza del segnale e del traffico di rete
- roaming trasparente (numero arbitrario di celle parzialmente sovrapposte)

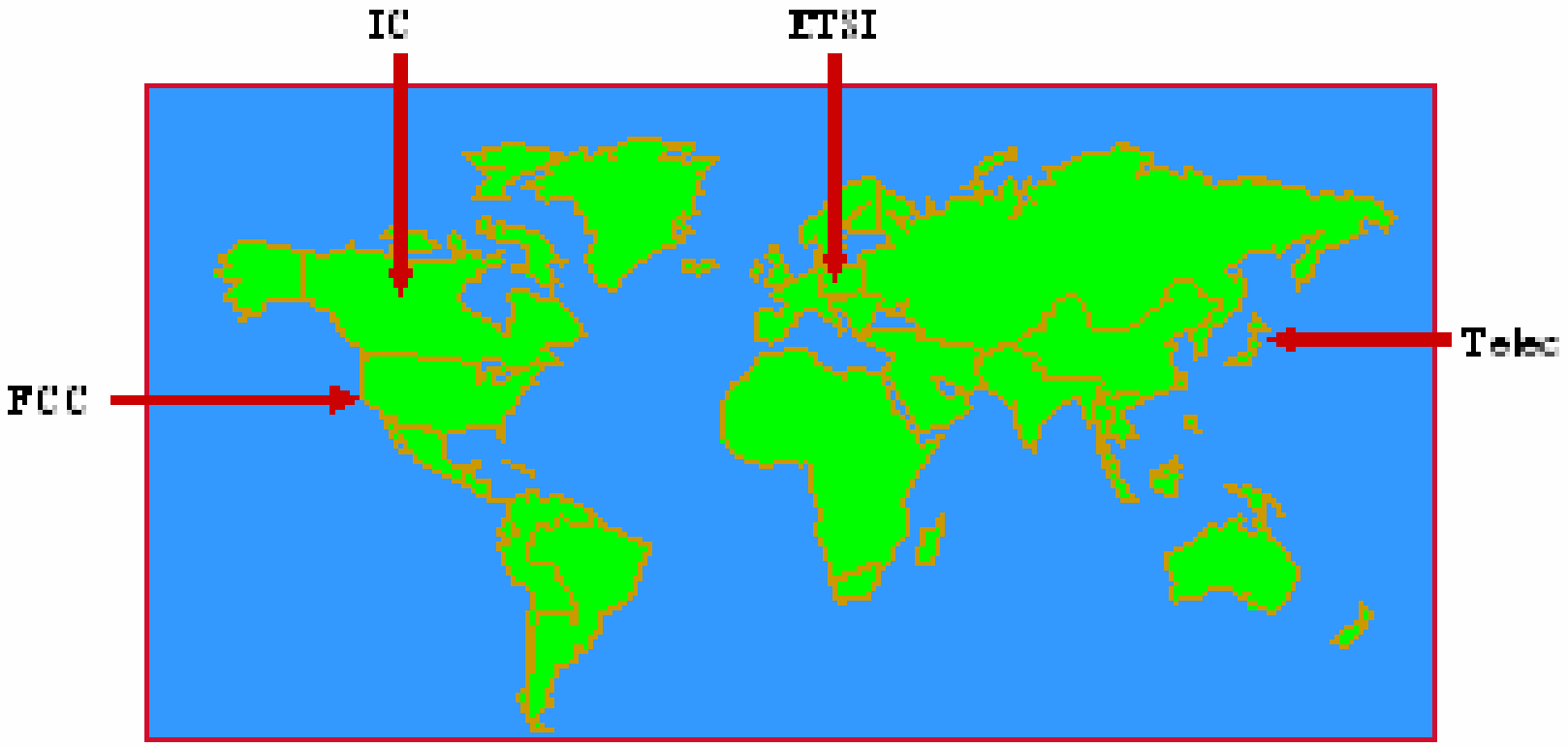
Tecnologia

Wi-Fi (**IEEE 802.11g**) – Nuovo Standard

- 802.11g opera a 2.4 Ghz (compatibile con 802.11b), fino a 54 Mbps
- versioni draft (<54Mbps)
- tecnologie proprietarie transitorie (es. AirPlus), basate su chipset ad alte prestazioni (~20-30 Mbps)
- metà 2003 probabile piena operatività

Tecnologia

Enti regolamentatori



ETSI = European Telecommunications Standards Institute
Normativa = ETS 300-328

Tecnologia

Antenne – Fattori principali

Direzionalità:

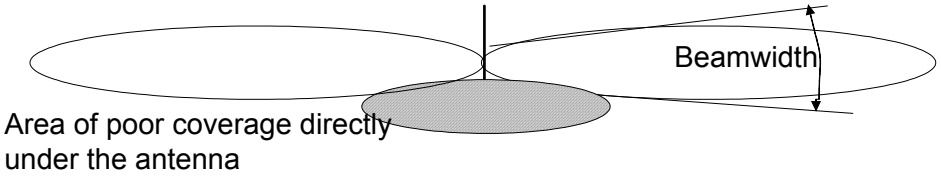
- Omnidirezionale (copertura 360°)
- Direttiva (angolo di radiazione limitato)

Guadagno:

- Misurato in dB (decibel)
- Maggiore guadagno = maggiore copertura in determinate direzioni

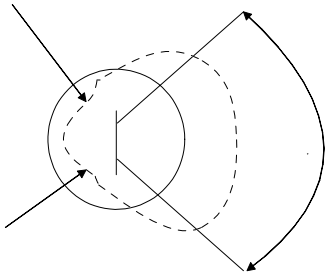
Tecnologia

- Antenne omnidirezionali
  - Maggior copertura sulla lunga distanza
  - Livello di energia direttamente sotto l'antenna inferiore
  - Minore copertura dell'area sotto l'antenna

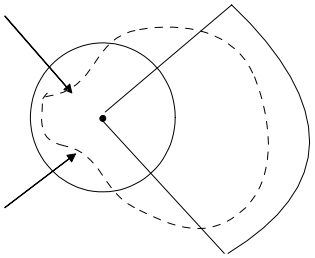


Tecnologia

- Antenne direttive:
  - L'are di copertura va in una determinata direzione
  - L'energia è condensata verso una specifica area
  - Pochissima energia verso retro dell'antenna



Side View
(Vertical Pattern)



Top View
(Horizontal Pattern)

Tecnologia

Mini-dipolo da 2.2 dBi

Tecnologia

Verticale da 5.14dBi

Montaggio a palo

Tecnologia

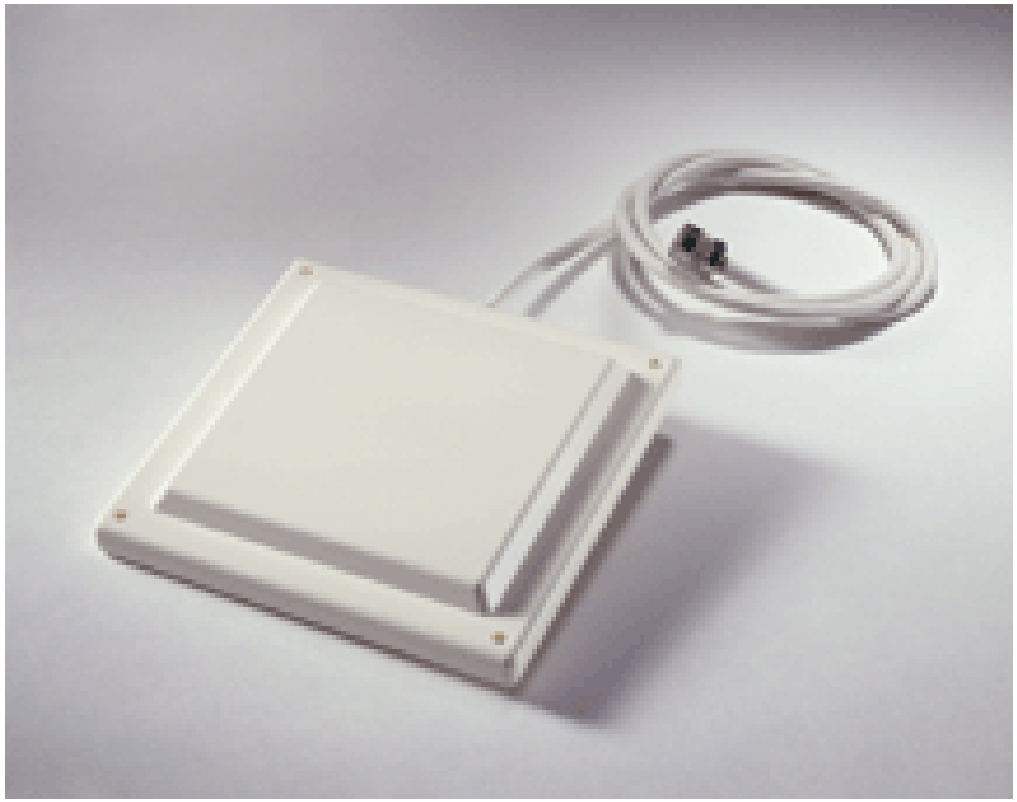
Omni da 12dBi

Montaggio a palo

Tecnologia

Antenna direttiva da 8.5dBi – ang. rad. 55°

Montaggio a Parete



Tecnologia

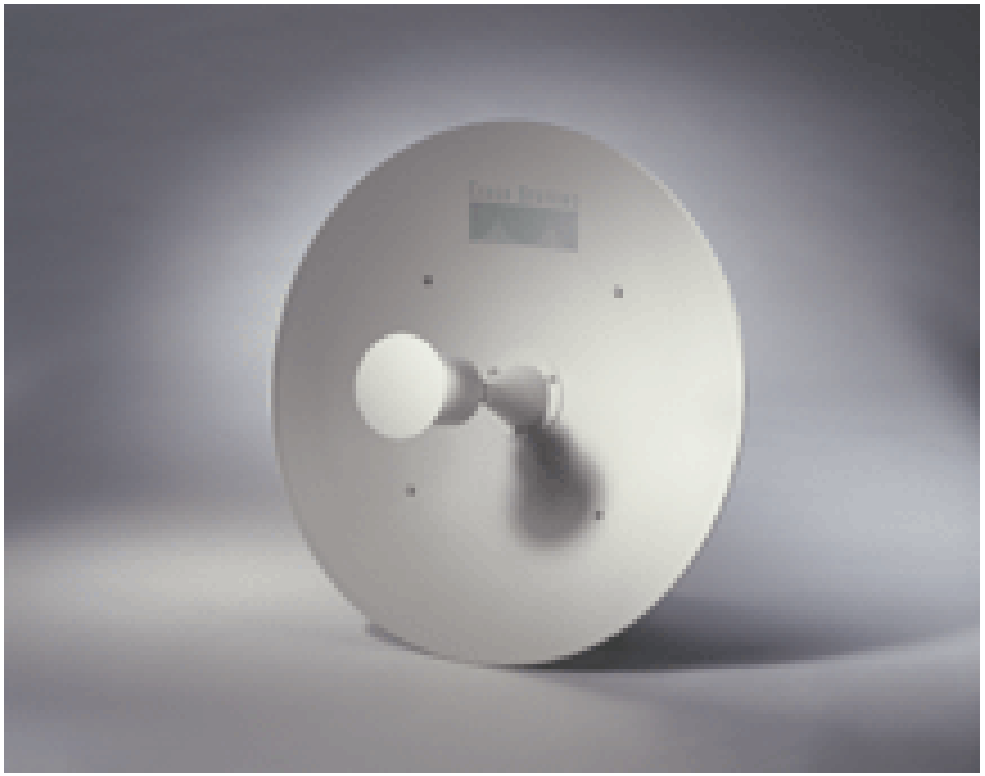
Direttiva Yagi da 13.5dBi – ang. rad. 25°

Montaggio a palo o parete

Tecnologia

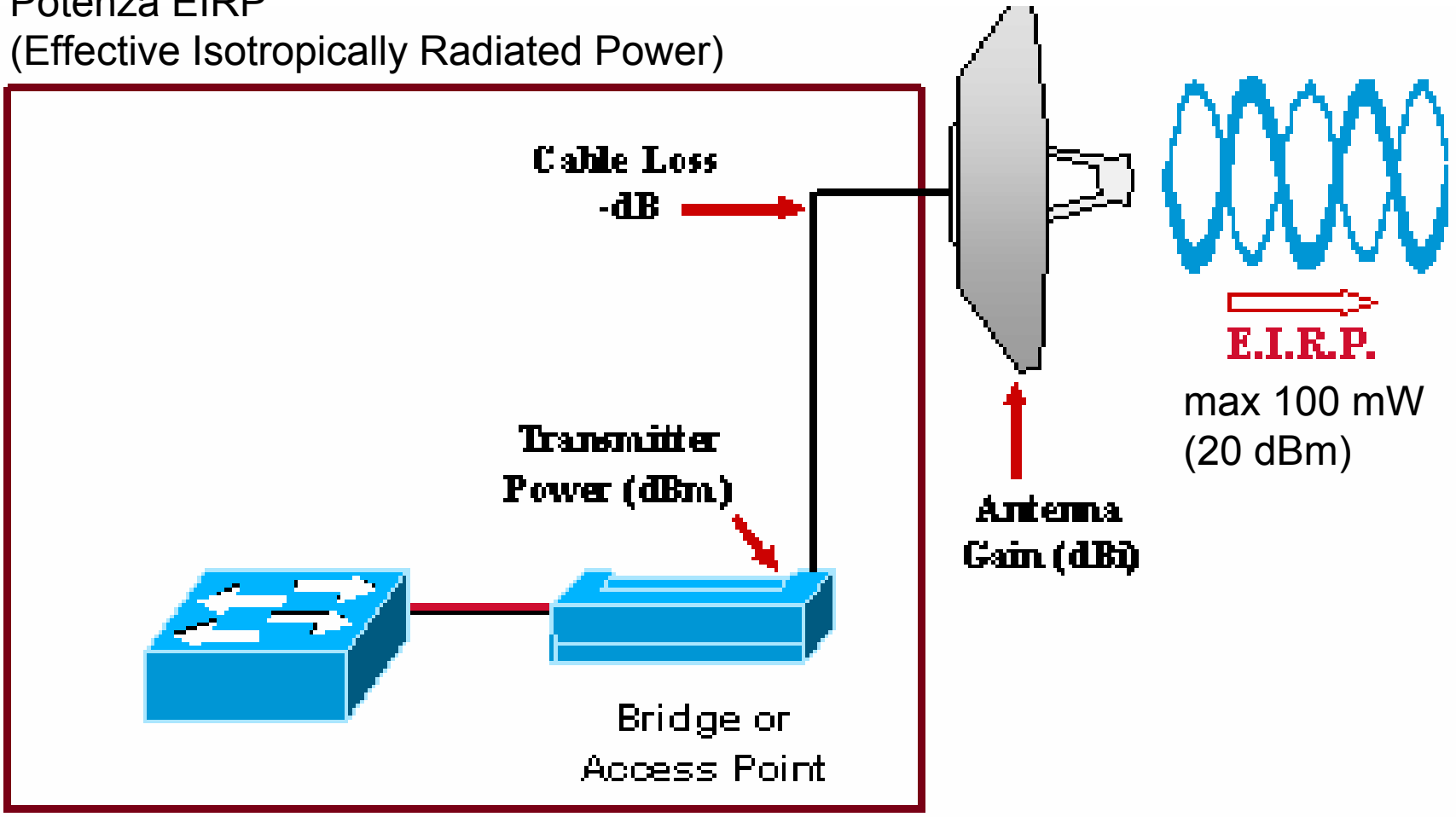
Parabola direttiva da 21dBi – ang. rad. 12°

Montaggio a palo



Tecnologia

Potenza EIRP
(Effective Isotropically Radiated Power)

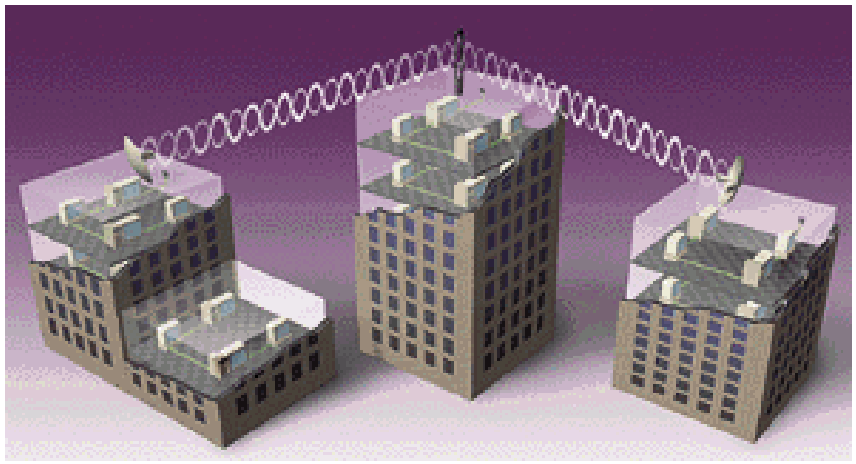


max 100 mW
(20 dBm)

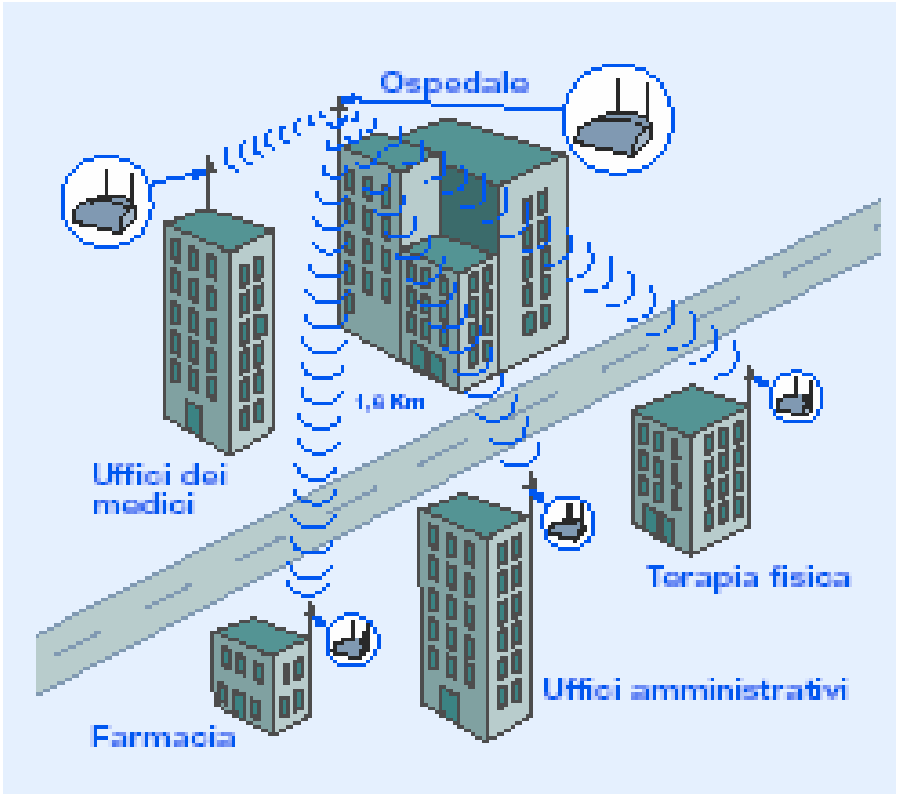
Applicazioni

Applicazioni:

- LAN-TO-LAN (bridging)
- fino a 11Mbit
- velocità in funzione dell'antenna
- aziende soggette a frequenti cambiamenti strutturali e che quindi devono essere collegate solo temporaneamente oppure molto rapidamente (ad esempio, fiere)
- aeroporti, sale congressi, alberghi



Scenari d'implementazione



Bridging multi-punto

Requisiti

- copertura di rete totale
- distanze di diversi chilometri

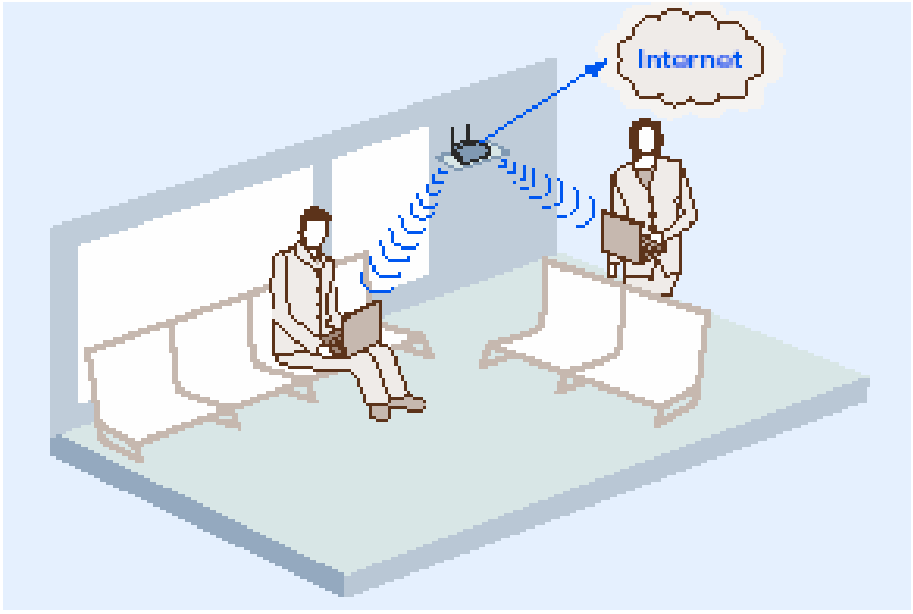
Soluzione

- Wireless LAN nell'intero complesso
- antenne omnidirezionali e Yagi

Vantaggi

- eliminazione dei costi associati alle comunicazioni
- velocità elevate
- copertura dell'intera struttura

Scenari d`implementazione



Luoghi pubblici molto frequentati (Hot Spot)

Requisiti

Per garantire la produttività, mantenere la competitività e in generale completare il lavoro assegnato, gli utenti utenti devono poter accedere a Internet da fuori sede.

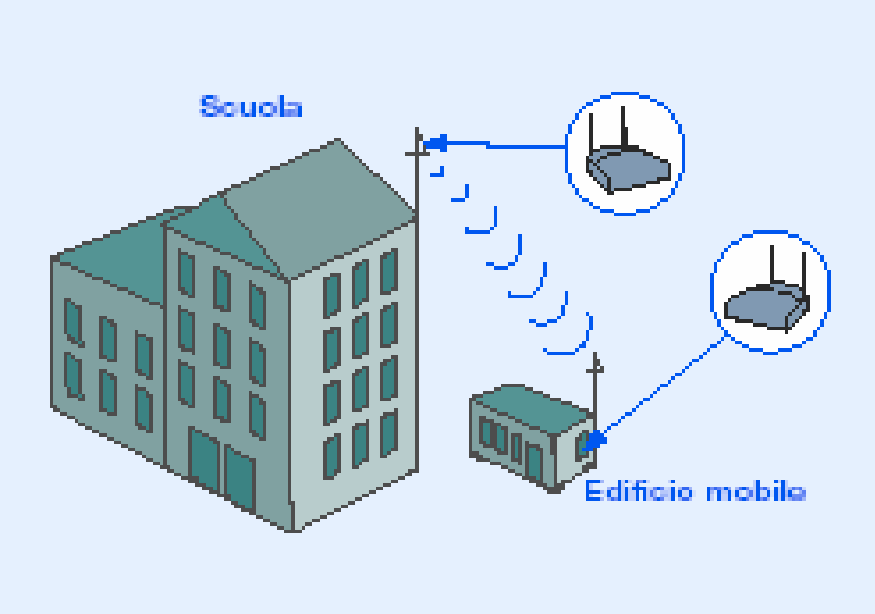
Soluzione

- unica connessione a Internet (cable modem, DSL)
- condivisione di un Access Point

Vantaggi

- I professionisti che viaggiano per lavoro possono essere molto più produttivi
- I locali pubblici possono aumentare il proprio business

Scenari d`implementazione



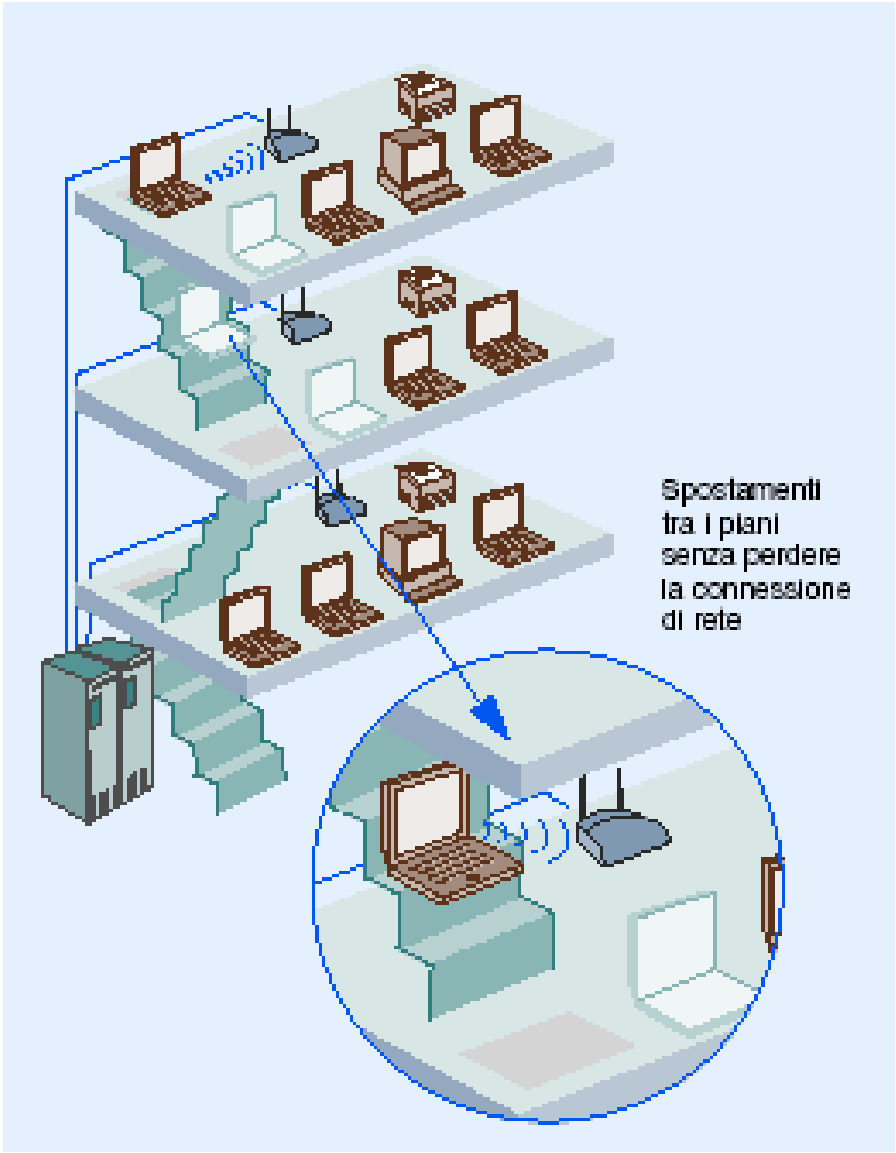
Bridging punto-punto

Requisiti
È necessario estendere la connettività di rete nelle nuove aule, ma senza investire ingenti somme in spazi destinati ad essere occupati solo temporaneamente.

Soluzione
- Access Point nell'edificio mobile
- bridge verso un Access Point installato nell'edificio principale.

Vantaggi
- Eliminazione della necessità di effettuare costosi ricablaggi e installazioni disordinate.
- Nessun impatto sulla produttività. Gli studenti e i docenti possono collegarsi immediatamente in rete.

Scenari d`implementazione



Roaming seamless

Requisiti

- Consentire agli utenti di PC portatili di rimanere collegati ovunque si trovino per lavoro

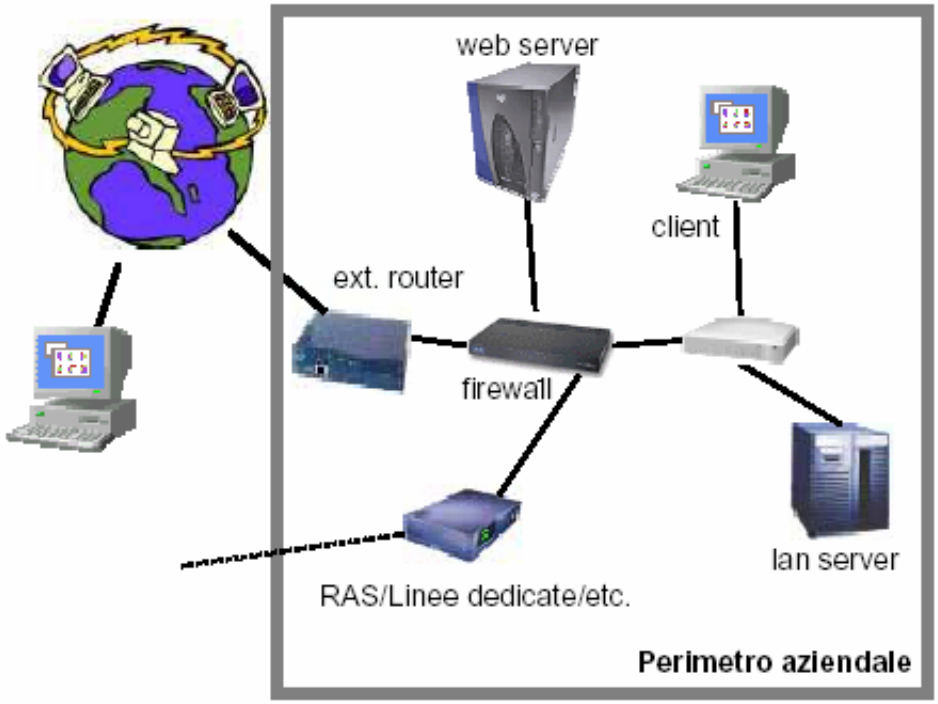
Soluzione

- I PC portatili, desktop e handheld vengono equipaggiati con schede di rete WLAN
- Gli Access Point vengono distribuiti e installati strategicamente in tutto l'ambiente di rete
- Gli Access Point vengono collegati al backbone della rete e possono essere facilmente installati e gestiti in remoto da una postazione centrale

Wireless (802.11)

e relative problematiche di security.

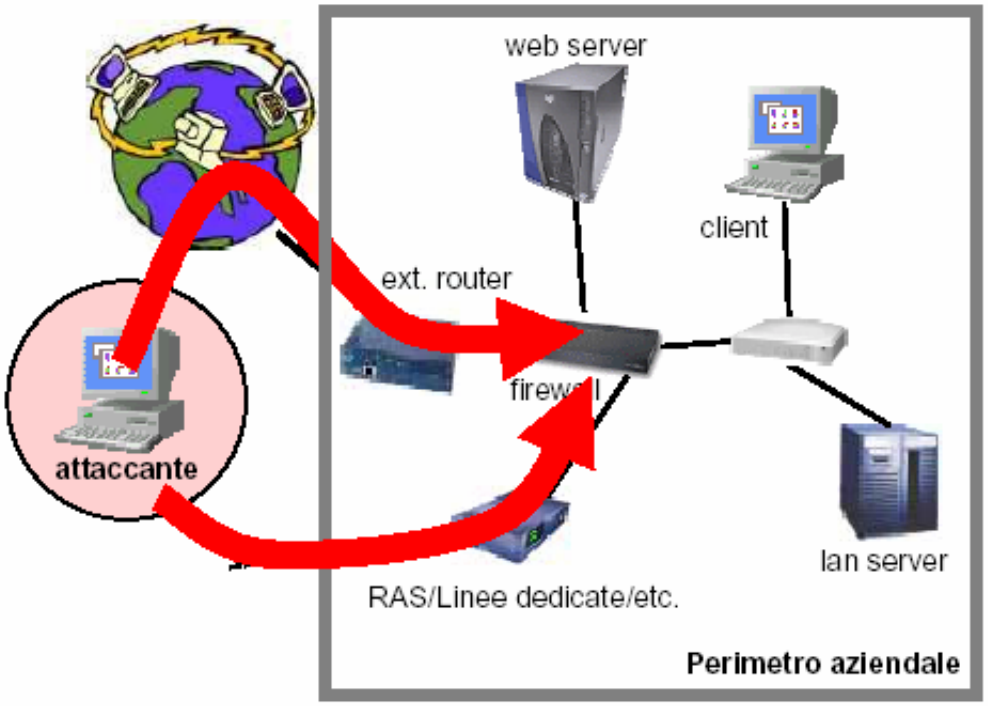
Rete „wired"



Esempio di rete aziendale "classica":

- rete privata (LAN)
- connessione ad Internet
- zona smilitarizzata (DMZ)
- RAS, Linee dedicate, VPN

Rete „wired"

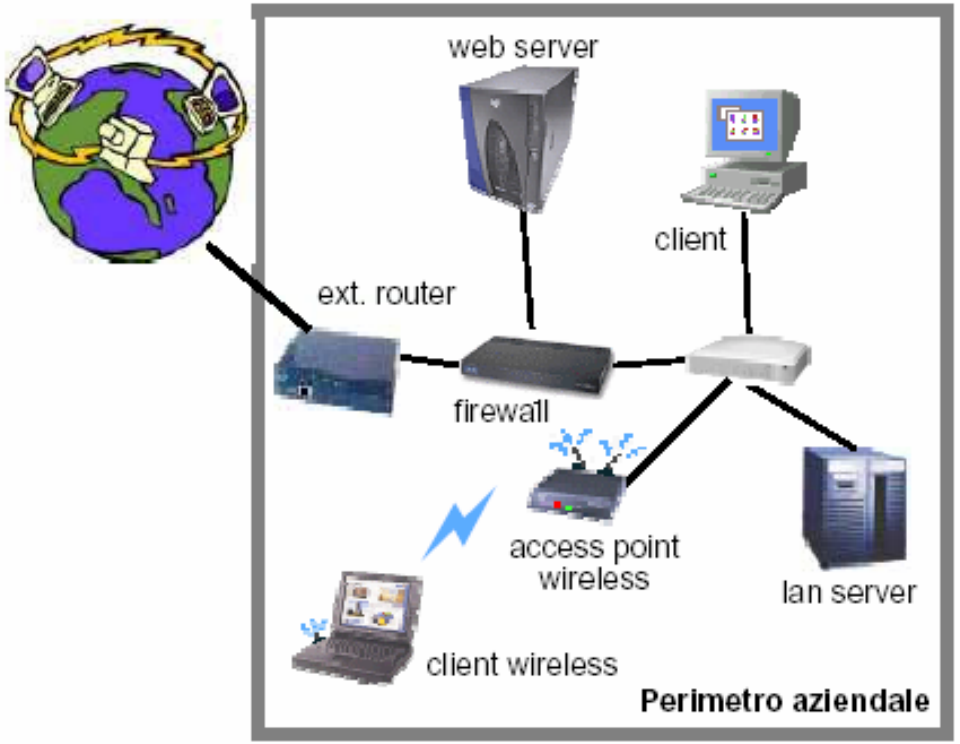


Esempio di rete aziendale "classica":

- rete privata (LAN)
- connessione ad Internet
- zona smilitarizzata (DMZ)
- RAS, Linee dedicate, VPN

Attacchi provenienti da Internet o tramite RAS/Linee dedicate, etc.

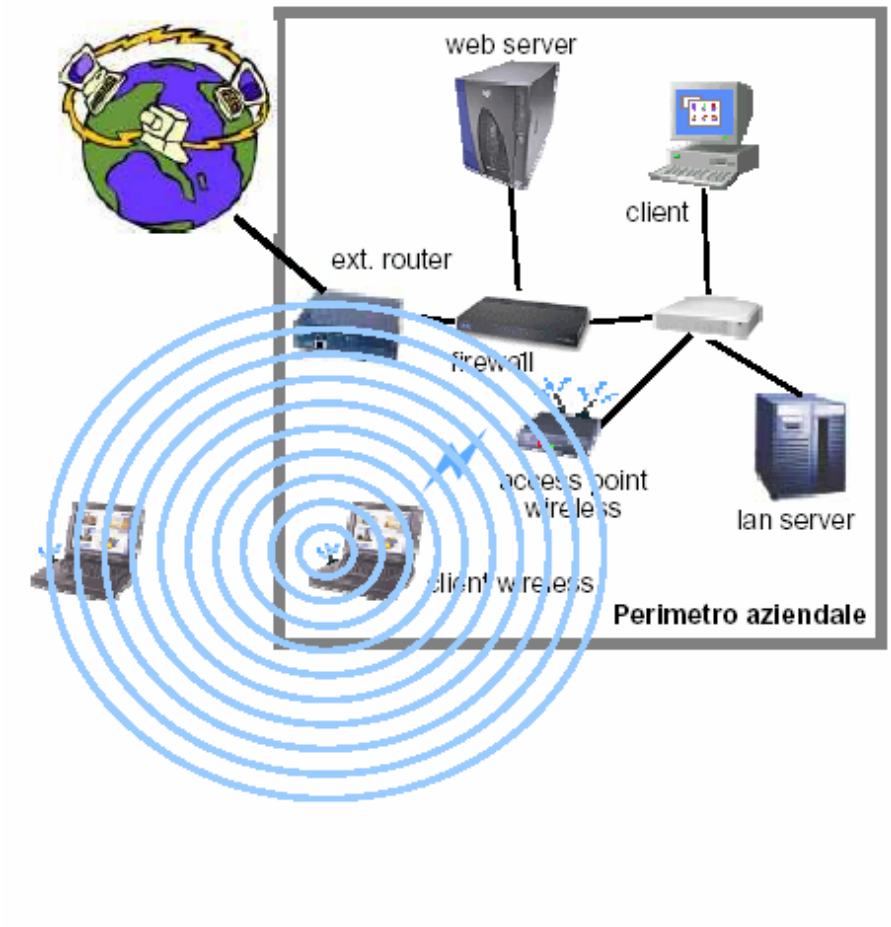
Rete „wireless"



Esempio di rete aziendale "wireless":

- rete privata (LAN)
- connessione ad Internet
- zona smilitarizzata (DMZ)
- access point wireless
- utenti wireless

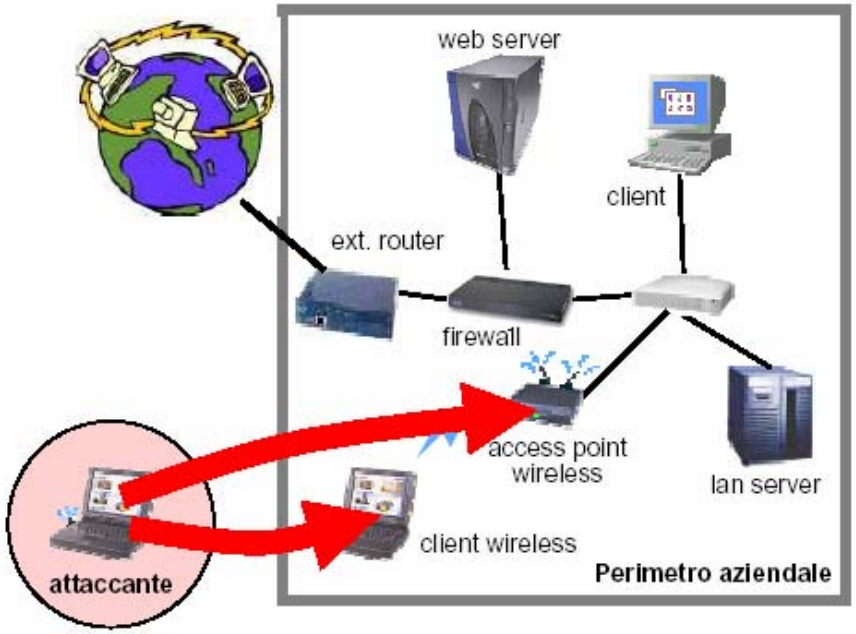
Rete „wireless"



Esempio di rete aziendale "wireless":

- i dati viaggiano nell'etere
- gli utenti si associano con gli "Access Point"
- per utilizzare il computer senza cavi in qualsiasi parte dell'azienda...
- ...o all'esterno dell'azienda

Rete „wireless"

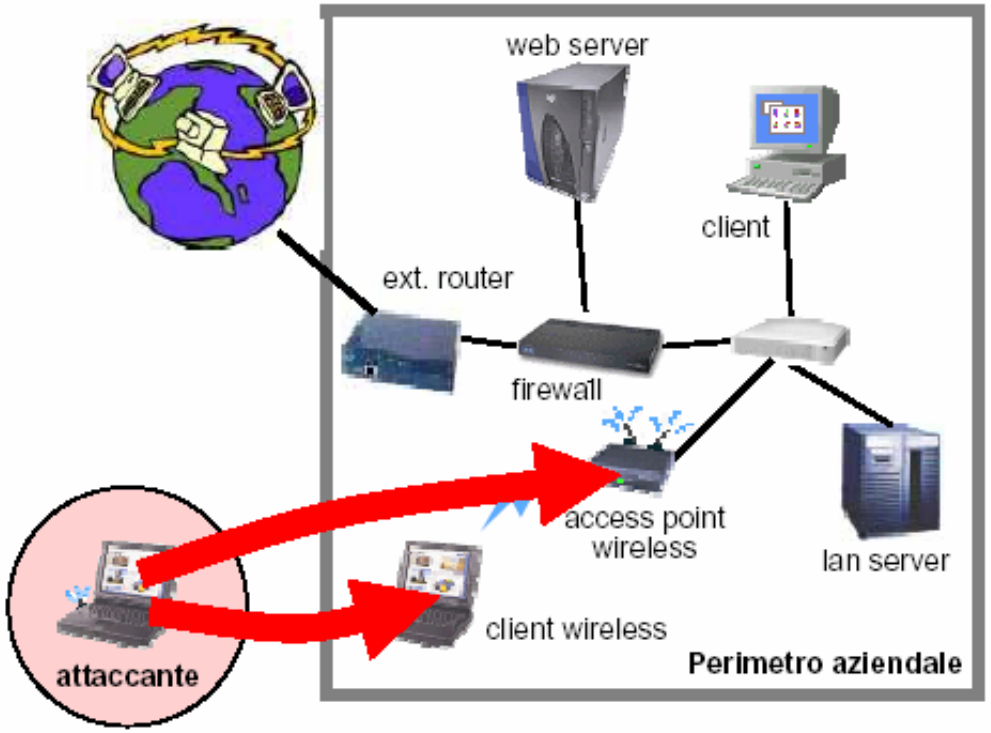


Attacchi provenienti "dall'etere", per es. da un hacker posizionato all'esterno del perimetro aziendale.

Esempio di rete aziendale "wireless":

- i dati viaggiano nell'etere
- gli utenti si associano con gli "Access Point"
- per utilizzare il computer senza cavi in qualsiasi parte dell'azienda...
- ...o all'esterno dell'azienda

Rete „wireless"

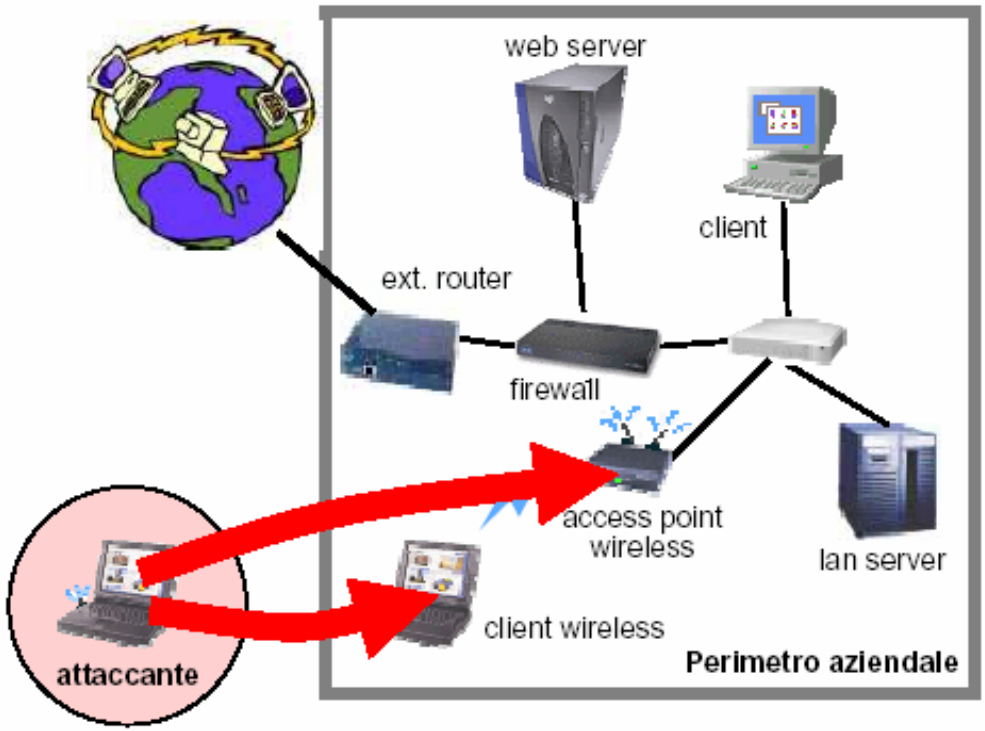


Nessuna misura di sicurezza...

Perché insicure?

- dati non limitati al perimetro fisico (aria,finestre, muri, ...)
- dati viaggiano in chiaro
- associazione con AP senza autenticazione
- AP posizionati direttamente sulla LAN
- DoS

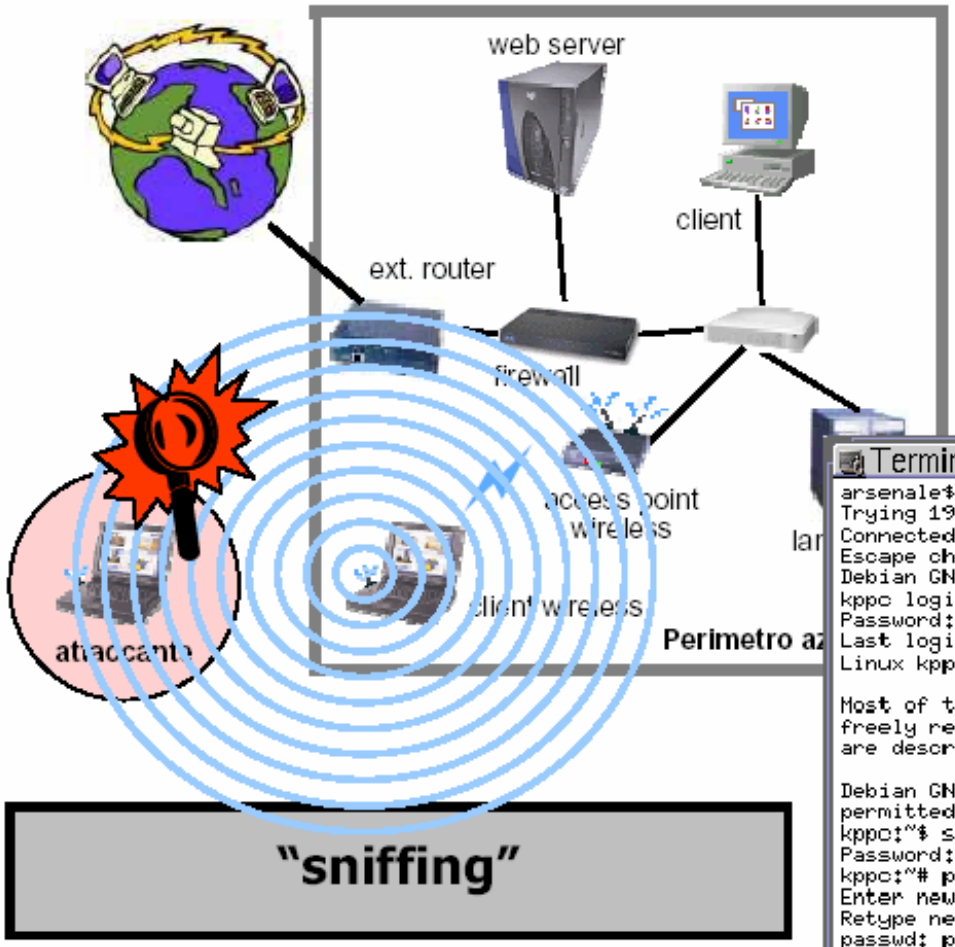
Dati non limitati al perimetro fisico



"Parking lot attack"

- per le loro caratteristiche, le onde radio attraversano muri, pareti, spazi aperti, vetri, etc.
- un attaccante che possa posizionarsi in un range fino a 30-50 metri da un AP può effettuare un apparecchiature standard
- con un antenna dedicata, il range aumenta

Dati viaggiano in chiaro



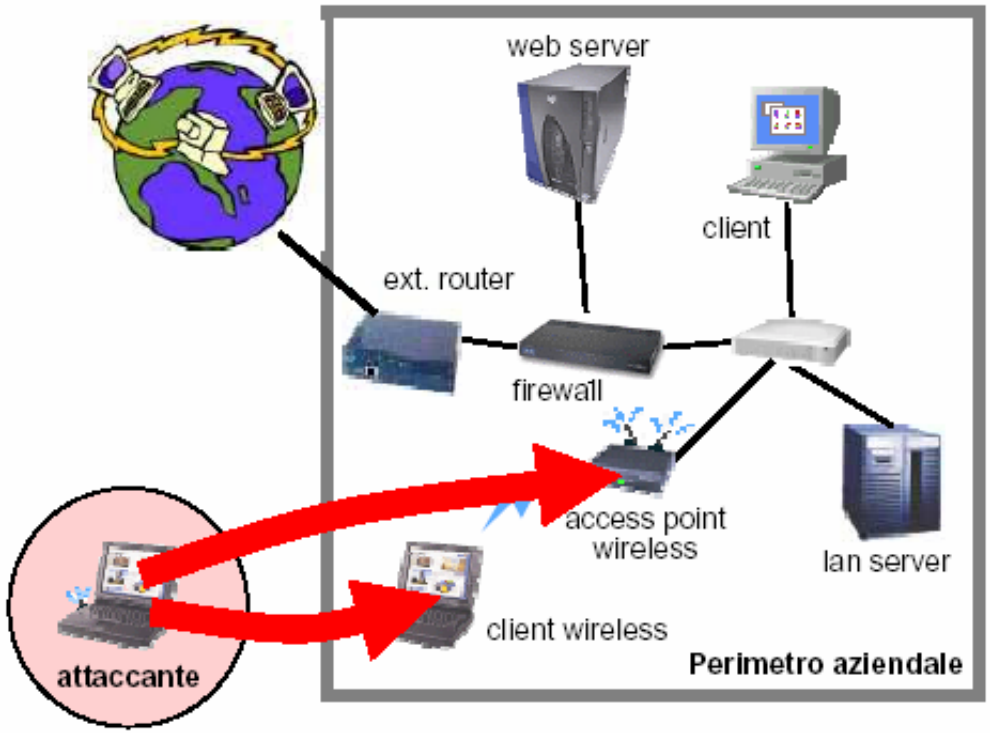
- se il traffico in transito non è cifrato, è possibile analizzarlo, in modalità "passiva" (semplicemente analizzando i pacchetti ricevuti senza inviarne)

```
Terminal
arsenale$ telnet 192.168.1.6
Trying 192.168.1.6...
Connected to 192.168.1.6.
Escape character is '^]'.
Debian GNU/Linux testing/unstable kppc
kppc login: utente
Password:
Last login: Thu Apr  5 15:34:06 2001 from 192.168.1.101 on pts/16
Linux kppc 2.4.3-pre3 #2 Tue Mar 13 10:12:58 CET 2001 ppc unknown

Most of the programs included with the Debian GNU/Linux system are
freely redistributable; the exact distribution terms for each program
are described in the individual files in /usr/share/doc/*/copyright

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
kppc:~$ su -
Password:
kppc:~# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
kppc:~#
```

Dati viaggiano in chiaro

- se il traffico in transito non è cifrato, è possibile analizzarlo, in modalità "passiva" (semplicemente analizzando i pacchetti ricevuti senza inviarne)

Open System Authentication



"NULL Authentication"

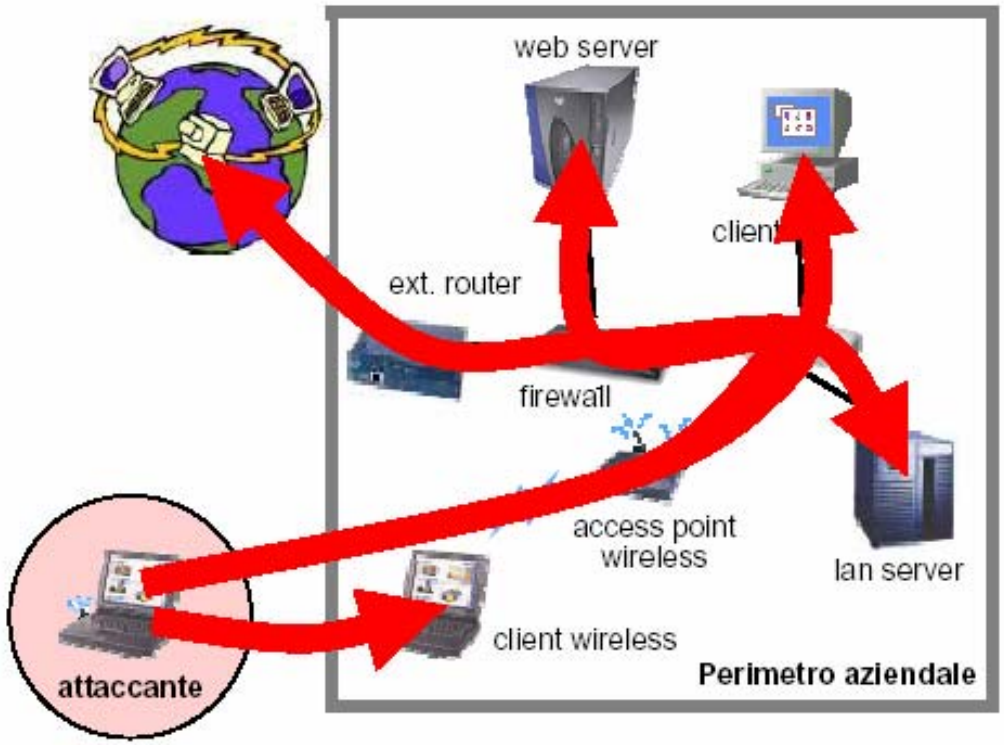
"infrastructure"

- raggiungere l'Access Point per entrare in rete
- simulare un AP e accettare connessioni dalle stazioni wireless

"ad hoc"

- attaccare direttamente altre stazioni

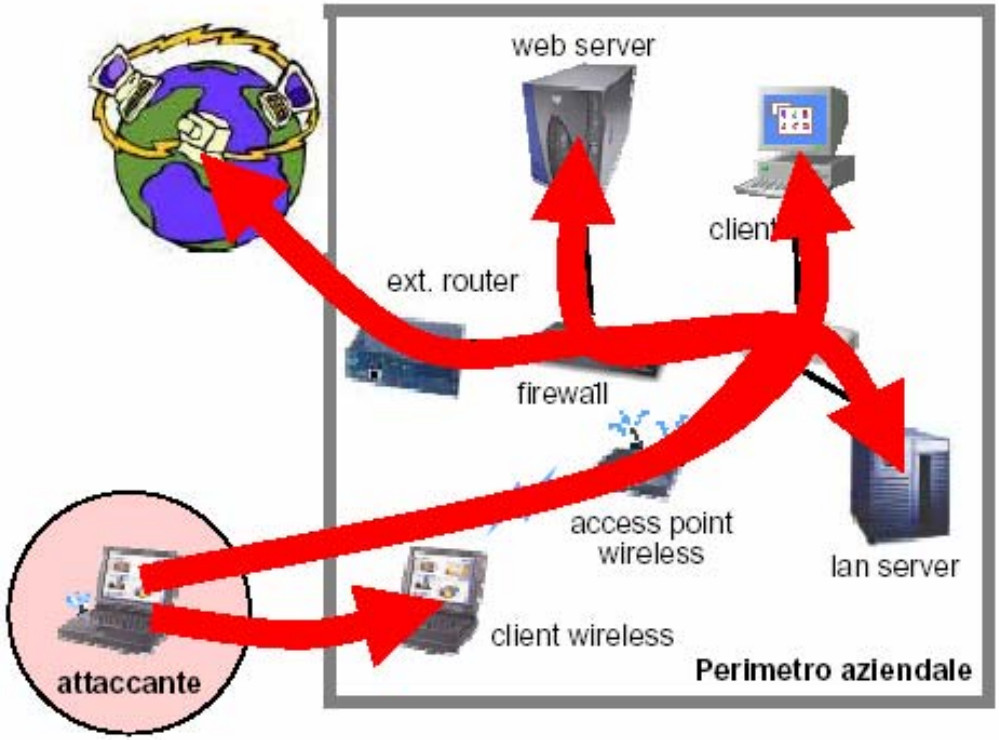
AP posizionati sulla rete interna



- attacco diretto ai server della rete interna
- attacco diretto alle stazioni sulla LAN
- attacco alle DMZ o altre stazioni da posizione privilegiata
- accesso ad Internet (attacco ad altri server, nascondendo la propria identità)

Le stesse possibilità di accesso di una stazione sulla LAN

Rete „wireless"

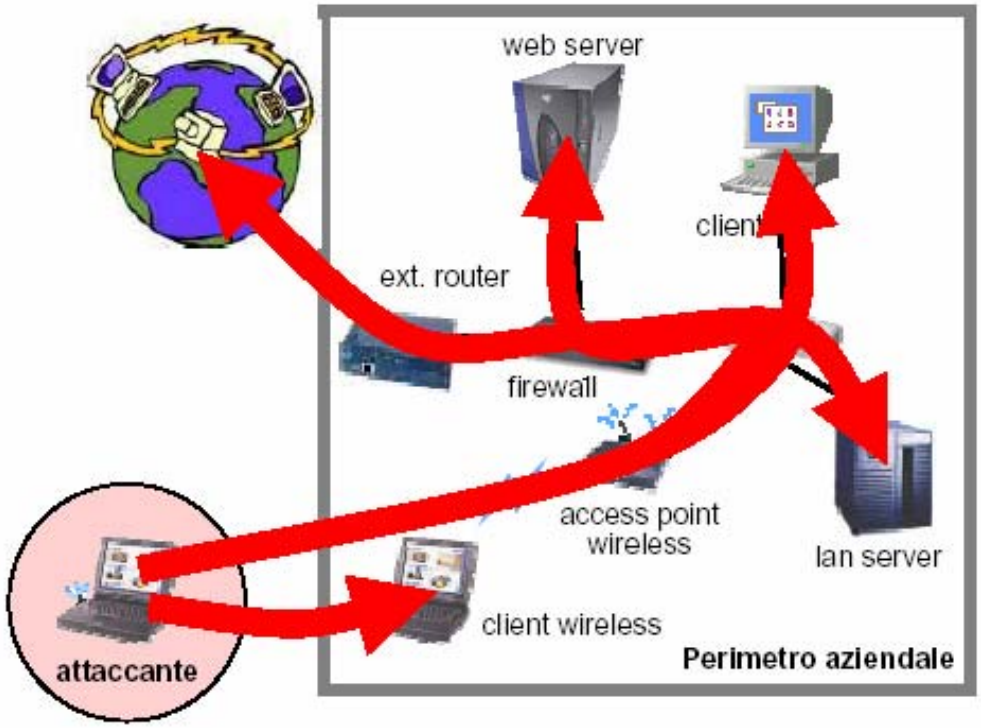


Cattive misure di sicurezza...

Perché insicure?

- conoscenza SSID
- filtro su MAC
- Wired Equivalency Privacy (WEP)
- Shared Key Authentication
- Varie estensioni proprietarie

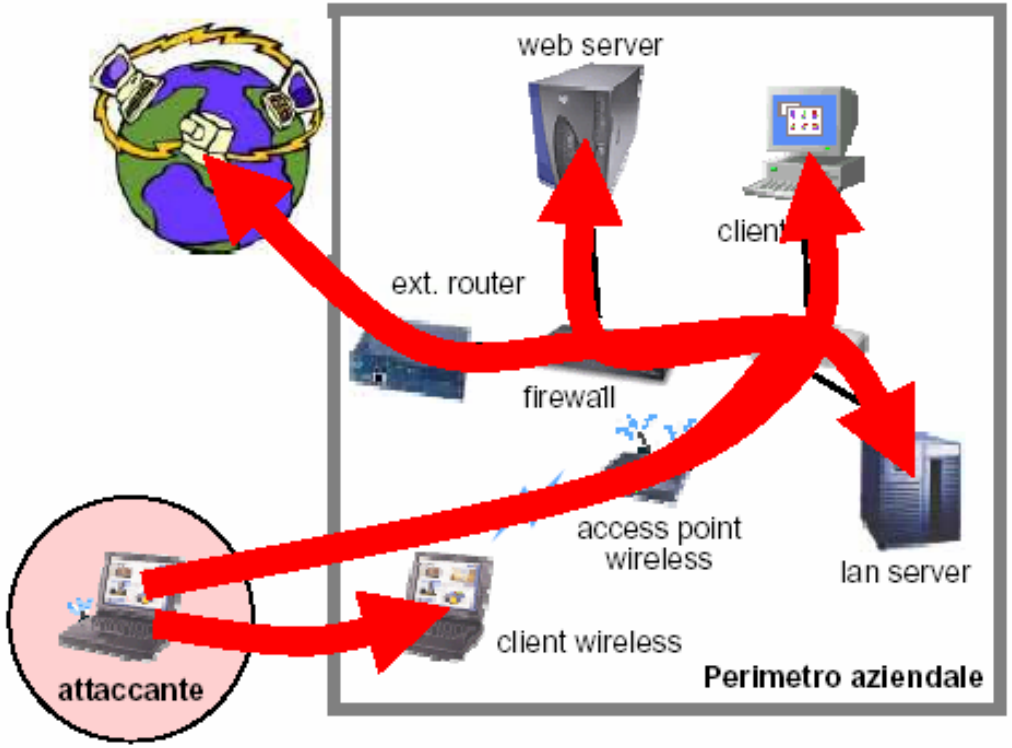
Conoscenza SSID



SSID: service set identifier

- per associarsi ad un AP è spesso sufficiente conoscere il SSID della rete
- SSID pre-impostati di default e non modificati
- il SSID viene inviato direttamente da molti AP nei "beacon" frame
- SSID trasmesso nei frame
- "probe" frame per verificare a quale AP corrisponda un SSID

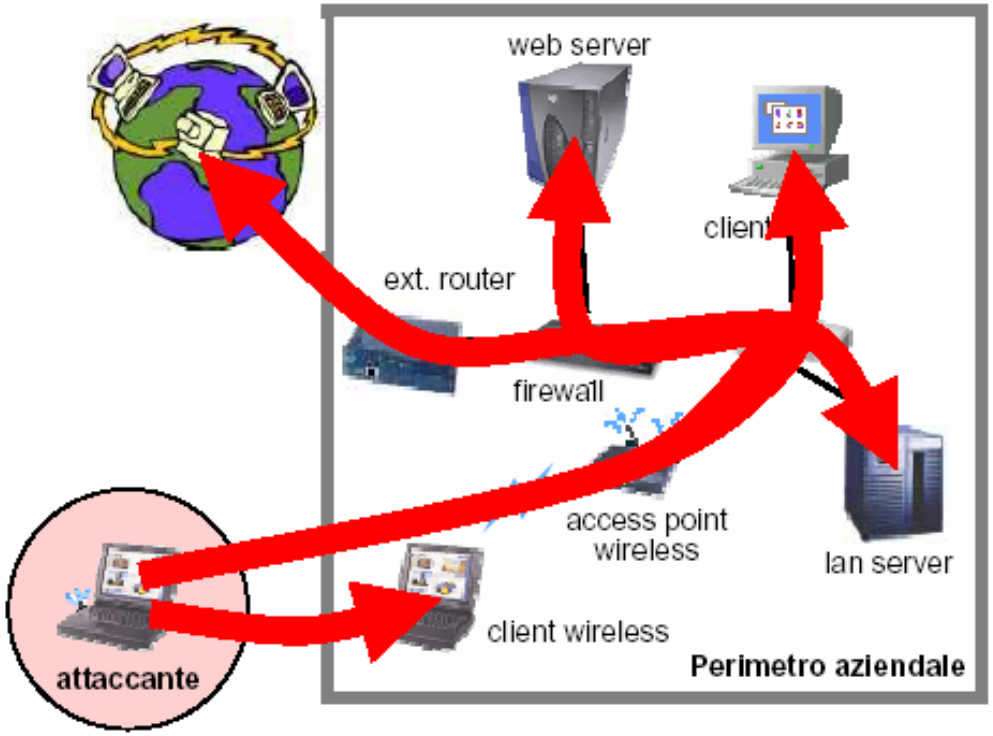
Filtro su MAC Address



- difficoltà di management per reti grandi
- MAC Address trasmesso nei frame dalle altre schede
- possibilità di cambiare con facilità il MAC Address della scheda

MAC: indirizzo hardware della eth

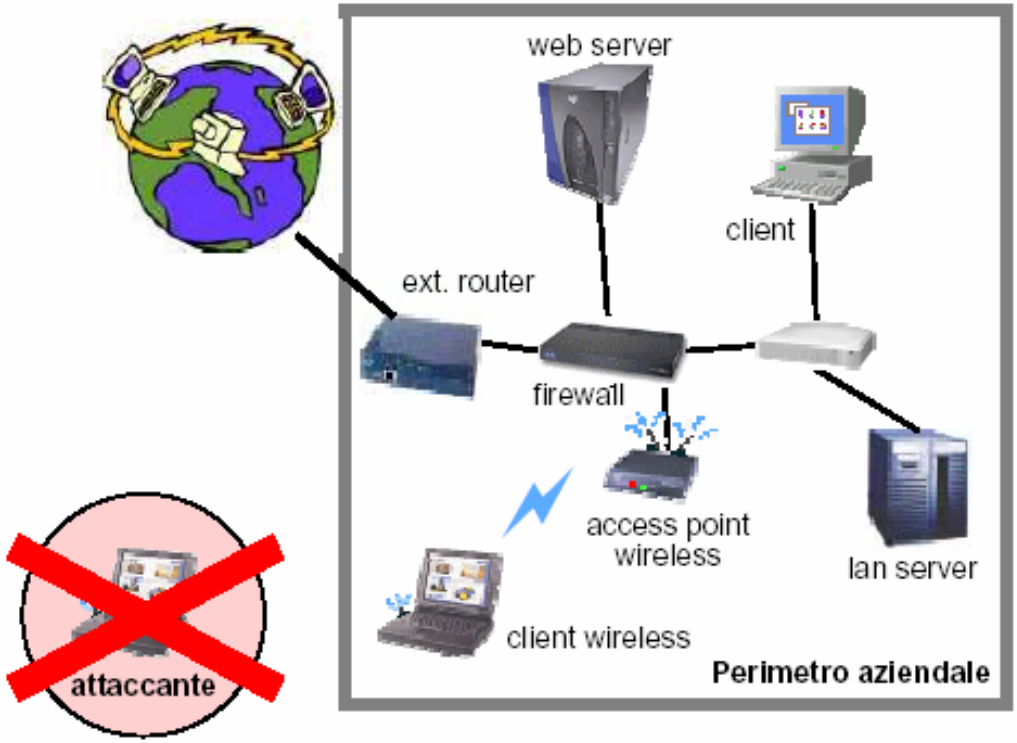
Wired Equivalency Privacy



cattiva implementazione di un buon algoritmo crittografico

- protocollo crittografico studiato per garantire la confidenzialità del traffico wireless da "sniffing" (Layer 2)
- chiave/i condivisa/e tra AP e client
- "Analysis of 802.11 Security *or Wired Equivalency* Privacy **Isn't**" Nikita Borisov, Ian Goldberg, David Wagner:
- possibilità di scoprire le chiavi analizzando quantità sufficiente di traffico

Sicurezza nelle reti wireless



- WEP 128bit con chiavi diverse per ogni client, e rigenerazione delle chiavi frequente ed automatica
- partizionamento della rete wireless dalla LAN (FW)
- IPSec/VPN
- Corretta configurazione Access Point
- Corretta configurazione stazioni wireless

Ulteriori consigli

- WEP è disabilitato per default
- Cambiare SSID di default
- Non utilizzare SSID banali (via, azienda, ecc.)
- Disabilitare il SSID broadcast
- Cambiare la password di accesso all'AP di default
- Posizionamento dell'AP lontano dal perimetro dell'edificio
- Analisi periodica della sicurezza (NetStumbler)
- Evitare installazioni WLAN da parte di terzi non autorizzati
- Analisi del segnale dall'esterno dell'edificio
- Utilizzare il filtro sui MAC address
- Protocolli di autenticazione per l'associazione con l'AP (RADIUS, LEAP, EAP-TLS, ecc.)

Ulteriori consigli

- Uso di IP statici, disabilitare DHCP
- Non utilizzare la subnet di default dell'AP
- Solo AP e schede con WEP (driver)
- AP con firmware aggiornabile
- Hardware proprietario ("closed network, "MIC", dynamic WEP keys, ecc.)
- Posizionamento dell'AP fuori dal firewall
- Uso di VPN (IPsec, SSL) sulle tratte Wireless
- Limitazioni temporali
- Policy aziendali

Link utili

- NetStumbler: www.netstumbler.com
- AirSnort: airsnort.shmoo.com
- Bsd-airtools: www.dachb0den.com/projects/bsd-airtools.html
- Raptor Wireless network stumbler for PRISM2 cards: www.0xdeadbeef.eu.org/code/p2s.c
- Wellenreiter: www.remote-exploit.org/modules.php?name=Downloads&d_op=viewdownload&cid=13

Link utili

- Boingo: www.boingo.com
- Kismet: www.kismetwireless.net
- Mognet: www.chocobospore.org/projects/mognet
- ETSI: www.etsi.fr
- WECA: www.wi-fi.org
- UFCOM (FAQ): http://www.ufcom.ch/en/telekommunikation/forschung/wlan/faq/index.html

Documentazione

- The Working Group for Wireless LANs: grouper.ieee.org/groups/802/11/
- Security for WEP algorithm: www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- Practical Exploitation of RC4 Weakness in WEP Environments: www.dachb0den.com/projects/bsd-airtools/wepexp.txt
- Wireless LAN Security FAQ: www.iss.net/wireless/WLAN_FAQ.php

Documentazione

- List of Vendor Access Point MAC addresses: caff.openbeer.it/wireless/mac_list.txt
- Security for WEP algorithm: www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- Default SSID's for several common Access Point and PCMCIA card Products: www.wi2600.org/mediawhore/nf0/wireless/ssid_defaults/
- Wardriving: www.wardriving.com