Introduzione alle nuove tecnologie Wireless per il Networking

Ing. Cristian Randieri

Università degli Studi di Catania

Istituto Nazionale di Fisica Nucleare (INFN)

Intellisystem TECHNOLOGIES

INFN Istituto Nazionale di Fisica Nucleare

Introduzione

- L'aumento dei dispositivi da collegare localmente in rete e dei collegamenti della rete stessa con altre reti locali all'esterno dell'edificio, ha portato alla necessità di cablare in modo "intelligente" gli edifici.
- Il criterio al quale ci si ispira è quindi quello di creare una struttura che debba tener conto sia del tipo di rete all'interno dell'edificio (rete dorsale di collegamento, reti di distribuzione sul piano, concentratori ...), sia del tipo di portante (fibra ottica per reti "verticali", cioè dorsali di edificio o tra edifici, oppure doppino o cavo coassiale per reti orizzontali o di piano).
- Tale tipo di cablaggio prende nome di ***cablaggio strutturato.***

Cablaggio strutturato

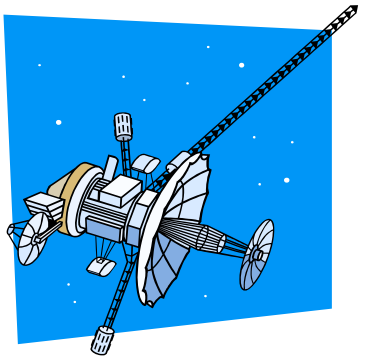
- La scelta del cablaggio, se effettuata con criteri tradizionali, in futuro creerà non pochi problemi, soprattutto perché ***ricablare un edificio già esistente presenta alti costi***, sia per caratteristiche infrastrutturali dell'edificio che per costi di istallazione e di gestione.
- Con le tecniche di cablaggio strutturato su tali edifici, si supererebbero in parte parecchi problemi legati al riammodernamento della struttura cablata dell'edificio, che risulterebbe intrinsecamente modulare e quindi, come si usa dire, ***"future proof",*** ma inevitabilmente la necessità di avere nel tempo collegamenti a velocità sempre maggiori, porterebbe a riconfigurare se non il cablaggio verticale, almeno quello orizzontale.

Cablaggio di nuovi edific

- Per quel che riguarda invece il cablaggio di nuovi edifici, ovviamente i problemi tendono a diminuire (grandi industrie, campus ...), ma talvolta avviene che non sempre lo studio architettonico dell'edificio è legato in maniera biunivoca alle esigenze tecniche dello stesso (edifici delle zone periferiche delle grandi città, piccoli edifici "cottage" per uffici di piccole e medie dimensioni).
- A questo si aggiunga che per tutti gli edifici in ambiente affari, vale il discorso che oltre alle reti dati, voce e video, si vanno a sovrapporre reti di controllo degli impianti che in futuro si prevede che saranno sempre più automatizzate, e che garantiranno il funzionamento a distanza degli stessi con cospicui margini di sicurezza.

Wireless Networks

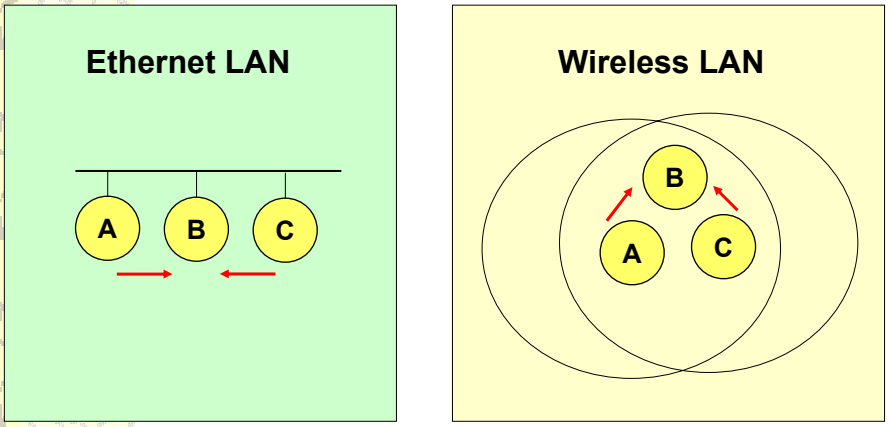
- Sono delle reti la cui interconnessione avviene mediante etere.
- Tipicamente il loro raggio d'azione è ristretto al campus o ad un ambiente confinato.
- La comunicazione tra I vari dispositivi può avvenire mediante:
  - ***link a raggi infrarossi*** (*Infrared IrDA*);
  - ***link radio*** (*Wavelan*).



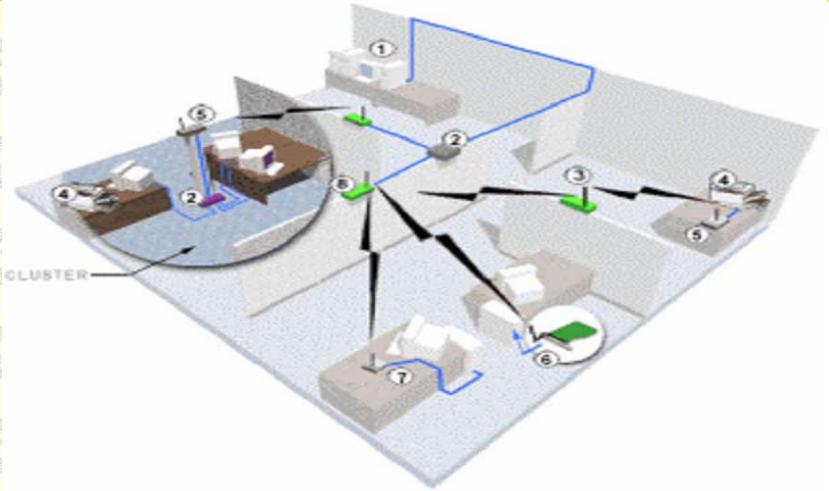
Le Wireless LAN (WLAN)

- Una **Wireless LAN (WLAN)** è un sistema flessibile di comunicazione da inquadrare come estensione di una LAN cablata (o come una sua alternativa). Poiché tale tecnologia usa frequenze radio, le WLAN trasmettono e ricevono dati via etere, minimizzando il bisogno di collegamenti cablati, combinando così la connettività con la mobilità dell'utente.
- Oggi le WLAN sono riconosciute più estesamente come un'alternativa di ***connettività general purpose*** per un gran numero di utenti.

Tecnologie a confronto



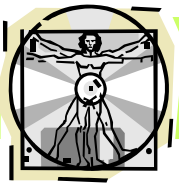
Tipica Wireless LAN



Il mercato

- Il ***Business Research Group***, una ditta americana specializzata in ricerche di mercato, ha previsto, nel marzo 1998, un'espansione del 600% del mercato mondiale delle WLAN entro l'anno 2002.

Perché wireless?



- Il vasto sviluppo del networking nel mondo degli affari e la crescita enorme dei servizi Internet online sono testimonianze forti dei benefici portati dalla condivisione dei dati e delle risorse.
- Con le WLAN, gli utenti possono accedere ad informazioni condivise senza cercare un luogo per collegarsi in rete, e gli amministratori di rete possono implementare o ingrandire una rete senza installare o trasportare fili.
- Le WLAN offrono vantaggi di ***produttività, convenienza e costi contenuti***, rispetto alle reti cablate tradizionali.

Proprietà di mobilità

- Le WLAN possono fornire agli utenti un modo per accedere dovunque, nella loro organizzazione, alle informazioni.
- Queste opportunità di mobilità e di servizio non sono possibili con reti cablate.

Velocità di installazione e semplicità

- Installare una WLAN può essere veloce e facile e può eliminare (o, nella peggiore delle ipotesi, limitare) la necessità di stendere cavi attraverso pareti e soffitti.

Costi di gestione ridotti

- Mentre ***l'investimento iniziale*** richiesto per l'hardware delle WLAN può essere più alto del costo dell'hardware delle LAN cablate, le spese di gestione complessive e le spese nel ciclo di vita della rete possono essere significativamente più basse.
- I ***benefici del costo a lungo termine*** sono maggiori in ambienti dinamici, che richiedono, cioè, spostamenti e cambiamenti frequenti della topologia della rete.

Scalabilità

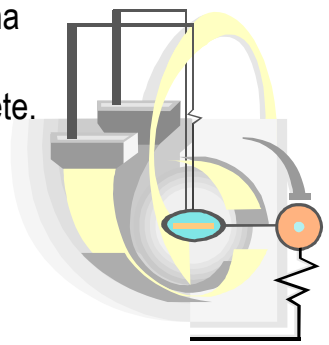
- Le WLAN possono essere configurate in una grande varietà di topologie per soddisfare alle necessità di applicazioni specifiche e di particolari installazioni.
- Le configurazioni possono essere cambiate facilmente e variano da reti peer to peer, appropriate per un numero piccolo di utenti, a reti di migliaia di utenti che possono operare su vaste aree grazie al roaming.

Applicazioni pratiche delle Wireless LAN

- Medici ed infermieri negli ospedali possono cooperare in maniera più produttiva perché mediante handheld computers o notebooks collegati mediante WLAN possono scambiare informazioni sui pazienti in tempo reale.
- Studenti possono accedere ad Internet o all'Intranet della facoltà per consultare i cataloghi delle biblioteche da qualsiasi punto nel campus universitario.
- Gli amministratori di rete in ambienti dinamici minimizzano gli overhead di gestione causati da spostamenti, estensioni di rete e da cambiamenti in generale; inoltre possono installare reti di computer in vecchi edifici senza il bisogno di creare infrastrutture costose.

Tecnologia delle WLAN

- I produttori di WLAN dispongono di una serie di tecnologie per scegliere la soluzione ottima per progettare una rete.
- Ciascuna di queste tecnologie ha una serie di vantaggi e di limitazioni:



Tecnologia Narrowband (banda stretta)

Tecnologia Spread Spectrum

Tecnologia Narrowband (banda stretta)

- Un sistema radio narrowband trasmette e riceve informazioni su una frequenza radio specifica.
- Tali dispositivi cercano di mantenere la banda del segnale radio quanto più stretta possibile, occupando solo le frequenze strettamente necessarie per l'interscambio di informazioni.
- I crosstalk tra canali di comunicazione sono evitati coordinando attentamente gli utenti su frequenze diverse.
- Una linea telefonica privata è molto simile ad una frequenza radio: poiché ogni appartamento ha la sua linea telefonica privata, gli abitanti di un appartamento non possono ascoltare le chiamate relative agli altri appartamenti.

Tecnologia Narrowband (banda stretta)

- In un sistema radio, privacy e affidabilità sono permessi dall'uso di frequenze radio separate.
- Un ricevitore filtra tutti i segnali radio trasmessi su frequenze diverse da quella assegnatagli.
- Un inconveniente della tecnologia narrowband è che l'utente deve ottenere una licenza (e quindi l'assegnazione di una frequenza) per ogni luogo da cui prevede di collegarsi in rete.

Tecnologia Spread Spectrum

- E' una tecnica di trasmissione radio sviluppata dal Ministero della Difesa USA per consentire comunicazioni affidabili e sicure.
- Lo Spread Spectrum utilizza una porzione di banda maggiore rispetto a trasmissioni narrowband;
- Ciò implica che il segnale trasmesso sia più forte e, quindi, di più facile ricezione, purché il ricevitore conosca i parametri del segnale trasmesso.
- Se un ricevitore non è sincronizzato alla frequenza giusta, il segnale Spread Spectrum viene visto come un rumore di fondo.

Tipi di trasmissione Spread Spectrum

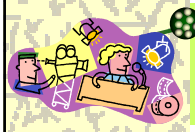
- *Frequency Hopping Spread Spectrum (FHSS)*
- *Direct Sequence Spread Spectrum (DSSS)*
- *Tecnologia infrarossa (IR)*

Frequency Hopping Spread Spectrum (FHSS)

- Tale tecnologia usa una portante che cambia frequenza secondo una sequenza nota solo al trasmettitore e al ricevitore.
- Se entrambi sono opportunamente sincronizzati, l'effetto globale che si ottiene è l'identificazione di un singolo canale logico.
- A un ricevitore non sincronizzato, il FHSS appare essere rumore di tipo impulsivo.

Direct Sequence Spread Spectrum (DSSS)

- Tale tecnica genera dei pattern di bit ridondanti per ogni bit che deve essere trasmesso. Questo pattern è chiamato "***chip***".
- Maggiore è la durata del chip, maggiore è la probabilità che i dati originali possano essere recuperati (e, chiaramente, maggiore è la banda utilizzata).
- Anche se uno o più elementi del chip si corrompono durante la trasmissione, mediante tecniche statistiche si possono recuperare i dati originali senza il bisogno di ritrasmissione.
- A un ricevitore non sincronizzato, il DSSS appare come un rumore di bassa potenza e larga banda, e quindi ignorato dalla maggior parte dei ricevitori narrowband;



Tecnologia infrarossa (IR)

- Tecnologia, poco usata negli usi commerciali.
- I sistemi ad infrarosso usano frequenze molto alte, appena al disotto della luce visibile, per trasmettere i dati.
- Come la luce, l'IR non può penetrare oggetti opachi; può essere diretta (a vista) o diffusa.
- I sistemi poco costosi possono lavorare a distanze molto limitate (circa 1 metro) mediante l'allineamento del trasmettitore e del ricevitore e tipicamente sono usati per reti di tipo personale, ma talvolta sono usati in applicazioni specifiche per le WLAN.

Tecnologia infrarossa (IR)

- Sistemi IR ad alte prestazioni non sono efficienti per utenti mobili e perciò sono usati solo per implementare sottoreti fisse.
- I sistemi IR diffusi (o riflessivi) non richiedono l'allineamento tra trasmettitore e ricevitore, ma le celle sono limitate a piccoli ambienti.

Problematiche introdotte dalle WLAN

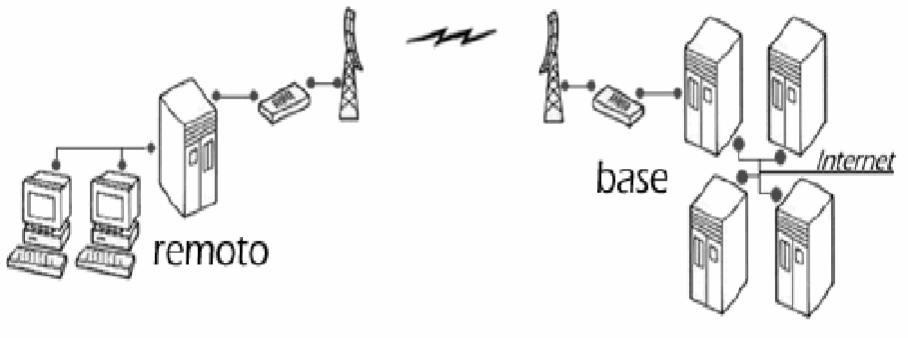
- L'uso di una frequenza radio alta (2.4 MHz) permette di raggiungere distanze considerevoli anche usando potenze di trasmissione minime (limitate per legge).

- A questo vantaggio si contrappone però uno svantaggio: nel caso di collegamenti punto–punto, condizione essenziale per l'utilizzo di questi apparati è che i due terminali remoti da collegare siano perfettamente "***a vista***", ovvero che sulla traiettoria di una linea immaginaria che li unisce non vi siano ostacoli fisici (palazzi, case, alberi …).

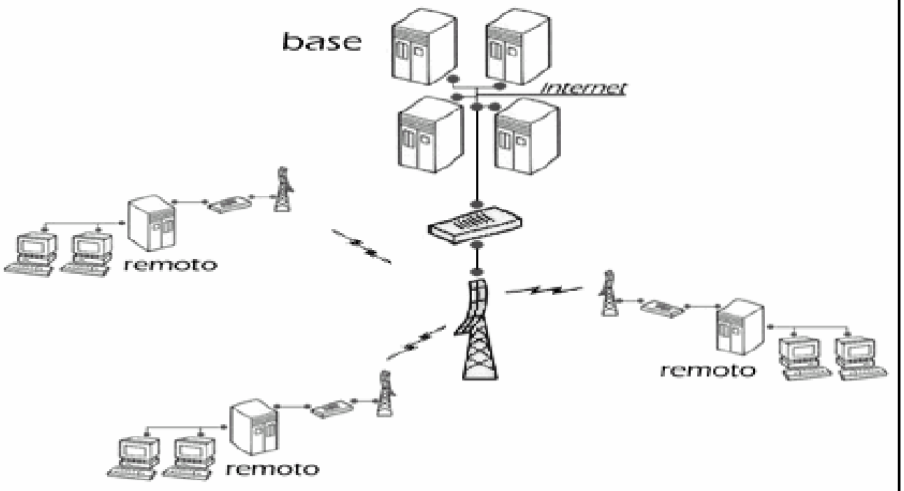
Problematiche introdotte dalle WLAN

- Inoltre, le distanze che si riescono a coprire con questo tipo di apparati sono molto variabili e strettamente legate al contesto ambientale in cui si opera.
- Presupponendo che i due punti da collegare siano perfettamente "a vista", le uniche cose che limitano il raggio di azione dell'apparato sono la presenza o meno di un'area densamente popolata.
- Se per esempio operiamo in una grande città allora il segnale di trasmissione può venire disturbato da interferenze dovute ad "***inquinamento radioelettrico***" (televisioni, radio, telefoni cellulari ...) oppure da riflessi dello stesso segnale causati da palazzi o case.

Collegamento punto punto



Collegamento punto multipunto

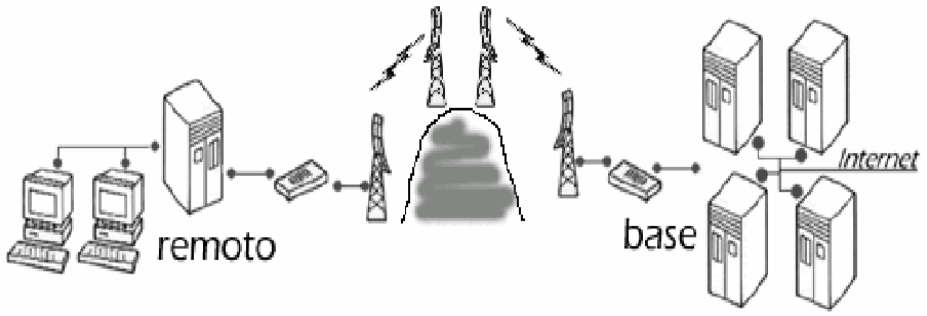


Ponti Radio

- Se per un motivo, dovuto o a distanza troppo elevata oppure a disturbi di trasmissione, non si riesce a stabilire un collegamento, si può ovviare installando in una zona intermedia tra i due punti un "***ponte radio***" che svolge la funzione di "***rilanciare***" il segnale ricevuto verso la destinazione finale.

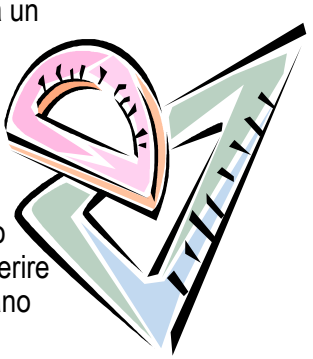
- Con questo sistema non ci sono praticamente limiti riguardo alla distanza che si può coprire; d'altro canto più "***ponti***" vengono installati più il costo della rete di collegamento aumenta in quanto il numero degli apparati da utilizzare praticamente raddoppia per ogni ponte radio utilizzato.

Ponti Radio



Come lavora una WLAN?

- Le WLAN usano ***onde elettromagnetiche*** (radio o infrarosso) per comunicare informazioni da un punto ad un altro senza sfruttare nessun collegamento fisico.
- I dati trasmessi sono sovrapposti ad una ***portante*** così che possano essere ricevuti correttamente da un opportuno ricevitore.
- Portanti radio multiple possono esistere nello stesso spazio allo stesso tempo senza interferire l'una con l'altra, a patto che le onde radio siano emesse su frequenze radio diverse.
- Un ricevitore si accorda su una frequenza per estrarre dati, mentre rigetta tutte le frequenze estranee.

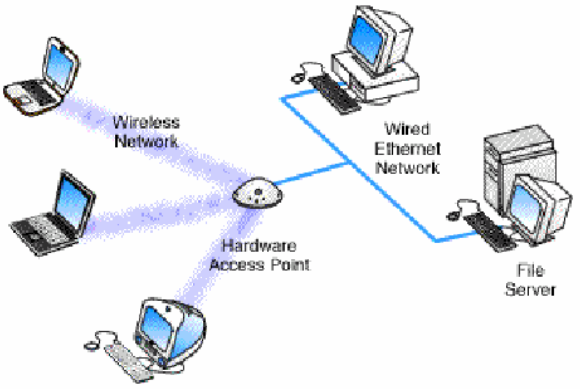


Access Point (AP)

- In una tipica configurazione di WLAN, un trasmettitore/ricevitore (il transceiver), chiamato **Access Point (AP)**, si connette ad una rete cablata mediante cablaggi standard: esso deve poter ricevere, bufferizzare, e trasmettere dati tra la WLAN e l'infrastruttura della rete cablata.
- Esistono due tipi di AP:
  - *Dedicated Hardware Access Points (HAP)*
  - *Software Access Point (SAP)*

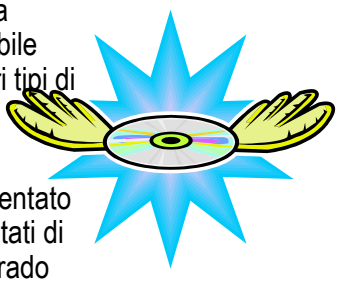
Dedicated Hardware Access Points (HAP)

- Sono dei dispositivi stand alone che si connettono direttamente alla rete cablata e fungono da interfaccia tra questa e i dispositivi wireless nella propria area di copertura.



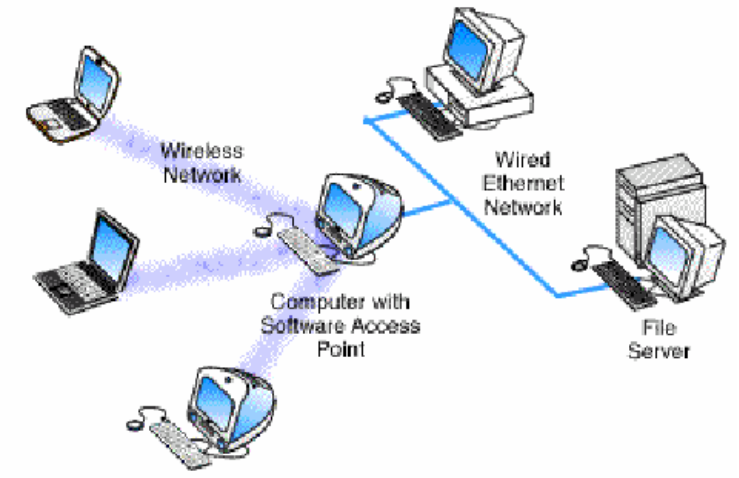
Software Access Point (SAP)

- Poiché lo standard utilizzato prevede soltanto la possibilità di collegare reti Ethernet alla WLAN, con un HAP risulterebbe impossibile implementare estensioni wireless per altri tipi di rete (Token Bus, Token Ring, …).



- Pertanto, alcuni produttori hanno implementato dei software, da far girare su terminali dotati di tutte le interfacce di rete necessarie, in grado di estrapolare i dati dalle frames dei protocolli di rete non supportati e trasformarli in frames per il protocollo wireless.

Software Access Point (SAP)



Operativamente….

- Un singolo AP può gestire un piccolo gruppo di utenti e può funzionare su ***un'area che va dai 30 ai 300 metri circa***.
- L'AP (o l'antenna connessa ad esso) è montato solitamente in alto, ma può essere montato in qualsiasi posizione, fino al raggiungimento della copertura radio desiderata.
- Gli utenti accedono alla WLAN mediante appositi adattatori che possono essere implementati come schede PCMCIA per notebooks o computer palmtop, oppure come schede in computer desktop o integrati in computer handheld.
- Tali adattatori forniscono un'interfaccia tra il sistema operativo di rete (NOS) e le onde elettromagnetiche mediante l'antenna.
- Il tipo di collegamento senza fili è del tutto trasparente al NOS.

Configurazione di Wireless LAN

- Nella configurazione più elementare, due PC, equipaggiati con schede apposite, possono implementare una rete indipendente fino a quando un PC è nell'area di copertura dell'altro.
- Questo tipo di rete è detto "***peer to peer***" o anche "***on demand***". Le reti di questo tipo non richiedono nessuna amministrazione o configurazione.
- In questo caso ciascun utente avrà accesso solamente alle risorse dell'altro utente e non ad un sistema di centrale.

Rete Wireless Peer to Peer

Configurare una Wireless LAN

- Installare un AP può estendere l'area di copertura di una rete; poiché l'AP è connesso ad una rete cablata, ogni utente avrà accesso a risorse di un sistema di servizio così come gli utenti collegati alla porzione cablata della rete.
- Ciascun AP può servire molti clienti, in base all'implementazione del singolo produttore.
- Esistono molte applicazioni reali dove un singolo AP serve dai 15 ai 50 utenti contemporaneamente.
- Gli AP hanno un'area di copertura limitata, sull'ordine dei 150 metri al coperto e 300 metri all'esterno.

Comunicazione tra utente singolo ed AP

ROAMING

- In reti molto estese, come quelle che è possibile realizzare in un supermercato o in una università, sarà probabilmente necessario installare più di un AP.
- Il posizionamento di tali AP deve essere effettuato mediante un accurato studio del luogo in cui si deve implementare la rete.
- Lo scopo è quello di ricoprire uniformemente un'area assegnata, facendo in modo che un utente in movimento non incontri mai delle zone non coperte dal segnale.
- La possibilità degli utenti di potersi muovere tra celle relative ad AP diversi è detta **roaming** e l'handoff tra celle adiacenti deve essere del tutto trasparente all'utente.

Access Point multipli e Roaming

Extension Points (EP)

- L'amministratore di rete potrebbe scegliere di usare degli ***Extension Points (EP)*** per ingrandire la rete degli AP.
- Gli EP sono molto simili agli AP, ma non sono collegati alla rete cablata come gli AP: il loro compito è quello di estendere l'area di copertura della rete, replicando i segnali trasmessi da un utente verso un AP o verso un altro EP.
- Tale dispositivo è in genere usato per passare un segnale da un AP ad un utente remoto (in modo simile ad una catena umana che si passa un secchio d'acqua da una sorgente all'incendio).

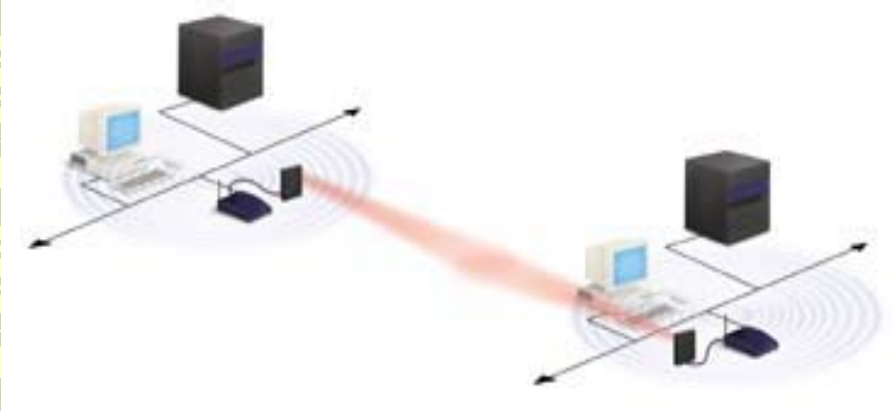
Uso di Extension Points (EP)

Uso di antenne direzionali

- Supponiamo di avere una LAN (sia essa wired o wireless) in un edificio A e di voler estendere la rete ad un altro edificio B distante anche alcuni chilometri dal primo e nel quale è stata implementata un'altra rete, distinta dalla prima.

- Una soluzione potrebbe consistere nel collegare, mediante un AP collegato alla rete preesistente, un'antenna direzionale su ciascun edificio, facendo in modo che ogni antenna sia puntata sull'altra.

Uso di antenne direzionali

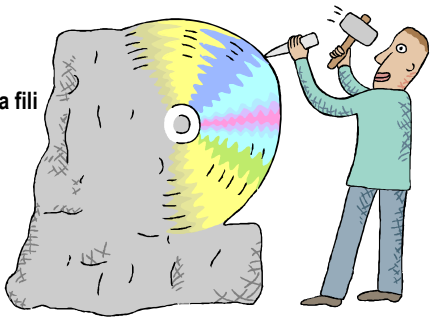


Elementi fisici di una WLAN

Considerazioni per l'installazione

Considerazioni per l'installazione

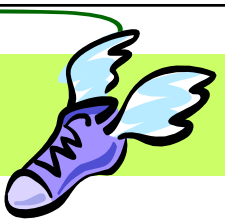
- Nonostante le WLAN offrano facilità di installazione, flessibilità di configurazione e libertà di movimento, bisogna elencare alcuni fattori tipici di tale tipo di rete:
- **Area di copertura**
- **Throughput**
- **Integrità e affidabilità**
- **Compatibilità con la rete esistente**
- **Interoperabilità di apparecchiature senza fili**
- **Interferenza e coesistenza**
- **Problemi di concessione**
- **Semplicità d'uso**
- **Sicurezza**
- **Costo**
- **Scalabilità**
- **Gestione del consumo energetico per stazioni mobili**
- **Incolumità**



Area di copertura

- La distanza alla quale possono comunicare onde RF e raggi IR è funzione del progetto del prodotto (potenza di trasmissione ed efficienza del ricevitore) e del percorso di propagazione del segnale, specialmente in ambienti chiusi.
- Le tipiche interazioni con gli oggetti interni all'edificio, inclusi arredamenti, pareti e persone, possono alterare la modalità di propagazione dei segnali, e quindi l'area di copertura del prodotto.
- Gli oggetti opachi bloccano i segnali infrarossi, che pertanto impongono limitazioni supplementari.
- La maggior parte delle WLAN usa segnali RF perché le onde radio possono penetrare gli ostacoli. I raggi di copertura tipici per le WLAN variano dai 30 metri ai 300 metri.
- Tale area di copertura può essere estesa attraverso una struttura di celle.

Throughput



- **C**ome le LAN cablate, il throughput attuale delle WLAN è dipendente dal prodotto e dalla configurazione usata.
- I fattori che influenzano il througput sono il numero di utenti, fattori di propagazione come il multipath, il tipo di WLAN usata, la latenza e colli di bottiglia sulle porzioni cablate delle LAN.
- I flussi dati tipici per le applicazioni commerciali sono dell'ordine dei 1.6 Mbps.
- Gli utenti di reti Ethernet tradizionali o Token Ring generalmente avvertono solo piccole differenze nelle prestazioni usando una WLAN che fornisce un livello di produttività sufficiente per le applicazioni da ufficio più comuni, includendo lo scambio della posta elettronica, accesso ad unità periferiche condivise, accesso ad Internet e accesso a database multi-utente. Per effettuare un paragone, si considerino i flussi dati tipici di connessioni via modem a 56.6 Kbps: in termini di throughput, una WLAN che opera a 1.6 Mbps è all'incirca trenta volte più veloce.

Integrità e affidabilità

- **L**e tecnologie wireless sono state perfezionate in più di cinquanta anni di applicazioni in sistemi commerciali e militari.
- Anche se le interferenze radio possono causare un degrado del throughput, tali interferenze sono rare nei posti di lavoro.
- La progettazione robusta delle tecnologie WLAN e la distanza limitata sulla quale i segnali viaggiano rendono i collegamenti tra utenti remoti più robusti di collegamenti telefonici cellulari e forniscono prestazioni di integrità di dati uguale o migliori rispetto a trasmissioni cablate.

Compatibilità

- Un grande numero di WLAN si interconnettono con reti cablate come Ethernet o Token Ring.
- I nodi delle WLAN sono visti dai sistemi operativi di rete alla stessa maniera di qualsiasi altro nodo di una LAN mediante l'uso di appositi drivers che, una volta installati, li rendono equivalenti a qualsiasi altro componente di una rete cablata.

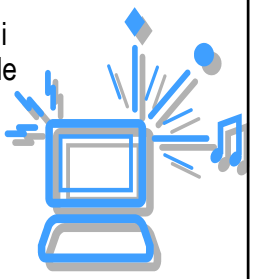
Interoperabilità di apparecchiature senza fili

Gli utenti dovrebbero essere consapevoli che WLAN di produttoridiversi potrebbero non essere interoperabili per tre ragioni.

- ***La prima ragione*** è che tecnologie diverse non possono interoperare: un sistema basato su tecnologia FHSS non potrà comunicare con un altro basato su tecnologia DSSS.
- ***La seconda regione*** è che i sistemi che usano bande di frequenza diverse non possono interoperare anche se usano la stessa tecnologia.
- ***La terza ragione*** è che sistemi di produttori diversi non possono interoperare, anche se impiegano la stessa tecnologia e la stessa banda di frequenza, per differenze nella realizzazione di ciascun venditore.

Interferenza e coesistenza

- La particolare tecnologia RF utilizzata può essere fonte di una notevole quantità di problemi che derivano dalla coesistenza nello stesso ambiente di altri dispositivi funzionanti a frequenze simili a quelle delle WLAN: i forni a microonde, ad esempio, sono una preoccupazione potenziale ma, conoscendo il problema, i produttori di dispositivi per WLAN progettano i loro prodotti in modo tale da evitare, o minimizzare, gli effetti di tale tipo di interferenza.



- Un'altra preoccupazione è la coesistenza di più WLAN nello stesso ambiente.

Normative sulle frequenze:USA

- Negli USA, la Federal Communication Commissions (FCC) regolamenta le trasmissioni radio, incluse quelle effettuate tramite WLAN.
- Le WLAN sono progettate tipicamente per operare in porzioni di banda dove la FCC non richiede all'utente finale di acquistare una licenza per l'uso dell'etere.
- Nei Stati Uniti molte WLAN trasmettono su una delle bande dell'ISM (Instrumentation, Scientific and Medical):
  - tali bande sono localizzate a 902-928 MHz, 2.4-2.483 GHz, 5.15-5.35 GHz, e 5.725-5.875 GHz.
- Per le WLAN da vendere in paesi stranieri, il produttore si deve assicurare che la sua certificazione sia adatta a quella del paese dove deve essere venduto il dispositivo.

Normative sulle frequenze:Europa

- La situazione europea è differente: per i sistemi radio in tecnica Spread Spectrum, la normativa tecnica ETS 300-328 impone di non irradiare con una potenza E.I.R.P. (Effectively Isotropic Radiated Power) superiore ai 100 mW (equivalente a 20 dBm);
- In linea di principio inoltre impone agli apparati radio Spread Spectrum, certificati ETS 300-328, di non trasmettere con una potenza elettrica effettiva superiore ai 50 mW (equivalente a 17 dBm), perché l'antenna a dipolo più semplice, che di solito li accompagna, ha generalmente un guadagno in trasmissione pari a circa 2.2 dB, che fa sì che la potenza E.I.R.P. trasmessa salga a circa 80 mW (per la precisione 19.2 dBm).

Normative sulle frequenze:Europa

- Per questo motivo su tutto il territorio dell'Unione Europea, ed anche in Italia, è assolutamente vietato utilizzare antenne che abbiano un guadagno in trasmissione elevato (in linea di massima diciamo superiore ai 3 dBi), tale da portare la potenza trasmessa E.I.R.P. oltre i 100 mW (equivalente a 20 dBm).

Ing. Cristian Randieri – Intellisystem Technologies
Introduzione alle nuove tecnologie Wireless per il Networking –
www.intellisystem.it

Availability of the 2.4 GHz band

US
Canada

Australia
China (*)
Hong Kong
Indonesia (*)
Japan
Korea
Malaysia
New Zealand
Philippines (*)
Singapore
Taiwan (*)
Thailand

(*) Certification in progress

Abu Dhabi (*)
Cyprus
Israel
Morocco (*)
Saudi Arabia
South Africa
Turkey (*)

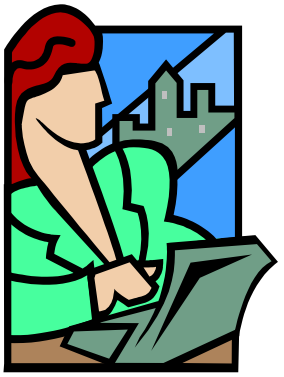
Austria
Belgium
Denmark
Finland
France
Germany
Iceland
Ireland
Italy
Netherlands
Norway
Portugal
Spain
Sweden
Switzerland
UK
Czech Republic (*)
Estonia
Hungary
Latvia (*)
Lithuania (*)
Poland (*)
Russia
Ukraine (*)

D.M. del 18.12.96

- In Italia, per l'utilizzo di apparati "Spread Spectrum" è necessario il pagamento di un canone come specificato da DM del 18.12.96 di seguito citato:" *n) per radiocollegamenti denominati radio L.A.N. (Local Area Network), realizzati a mezzo di apparecchiature con tecnica di modulazione a spettro diffuso (Spread Spectrum) o con tecnologia DECT (Digital European Cordless Telecommunication), relativi a impianti nell'ambito di ambienti confinati e con l'esclusione di impianti interconnessi a rete pubblica: L. 500.000 per canone base annuo e L. 50.000 per ogni terminale collegato*".
- Per i sistemi ottici, invece, sia in Europa che negli USA non è richiesto alcun tipo di canone.

Semplicità d'uso

- Gli utenti hanno bisogno di poche informazioni tecniche per trarre i massimi vantaggi dalle WLAN. Poiché la natura di una WLAN è trasparente al NOS dell'utente, le applicazioni lavorano allo stesso modo di come lavorano nelle LAN cablate.
- Le WLAN semplificano molti dei problemi di installazione e di configurazione che affliggono gli amministratori di rete.
- Poiché solo gli AP di una WLAN richiedono connessioni via cavo, gli amministratori di rete sono liberi dal posare cavi negli ambienti dove è necessario realizzare la rete, fornendo una notevole dinamicità alla rete stessa.

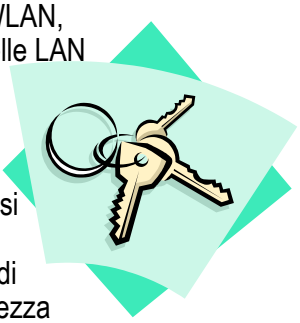


Semplicità d'uso

- Inoltre, la natura portabile delle WLAN consente agli amministratori di rete di risolvere i problemi di configurazione di reti intere prima di installarle nella posizione di utilizzo abituale.
- Una volta configurate, le WLAN possono essere spostate da un luogo all'altro con pochissime modifiche.

Sicurezza

- La sicurezza è stata per molto tempo il criterio fondamentale nel progetto dei dispositivi wireless.
- Meccanismi di sicurezza sono inclusi nelle WLAN, rendendole più sicure della maggior parte delle LAN cablate.
- È estremamente difficile, per ricevitori non autorizzati, ascoltare un traffico di WLAN.
- Tecniche di codifica complesse rendono quasi impossibile l'accesso non autorizzato alla trasmissione o alla ricezione del traffico: i nodi principali della rete devono garantire la sicurezza della trasmissione prima che sia permesso loro di partecipare allo smistamento di traffico nella rete.



Costi

- **U**na realizzazione di WLAN include entrambi i costi di infrastruttura per gli AP, e costi per l'utente per gli adattatori WLAN. Le spese per l'infrastruttura dipendono essenzialmente dal numero di AP usati; il loro prezzo oscilla tra i 1000 e i 2000 dollari.

- Il numero di AP dipende tipicamente dalla regione di copertura richiesta e dal numero e dal tipo di utenti che deve essere servito.

Costi

- Gli adattatori per WLAN sono necessari per computer standard e il loro prezzo varia dai 300 ai 1000 dollari.
- Il costo di installazione e di manutenzione per una WLAN è più basso del costo di installazione e manutenzione per una LAN cablata per due ragioni:
  - la prima è che una WLAN elimina le spese di posa e di manutenzione dei cavi.
  - la seconda è che le WLAN semplificano gli spostamenti, le aggiunte e il cambio degli utenti.

Scalabilità

- Le WLAN possono essere progettate per essere estremamente semplici o piuttosto complesse.
- Possono sostenere un grande numero di nodi su grandi aree fisiche aggiungendo un numero opportuno di AP per estendere l'area di copertura.

Gestione del consumo energetico per stazioni mobili

- I prodotti wireless per utenti finali sono progettati per funzionare, nel caso di notebooks o di handhelds, con batterie.
- I produttori di WLAN tipicamente impiegano tecniche di progetto speciali per minimizzare l'uso di energia degli hosts e la vita della batteria.

Incolumità

- La potenza trasmessa da sistemi WLAN è molto bassa, molto minore di quella di un telefono cellulare.
- Poiché le onde radio si attenuano rapidamente con la distanza, l'esposizione ad energia RF nell'area della WLAN è esigua. Le WLAN devono soddisfare a normative molto severe e a regolamentazioni per incolumità degli utilizzatori.
- Nessun danno alla salute è stato mai attribuito all'uso di WLAN.

Interoperabilità tra dispositivi wireless

Concetto di interoperabilità

- E' la possibilità di far lavorare insieme dispositivi realizzati da produttori diversi.
- Da quando ci si è resi conto che un singolo produttore non potrà mai provvedere alla fornitura di ogni elemento di una qualsiasi rete, il concetto di interoperabilità è diventato essenziale nel permettere agli amministratori di rete di evitare una serie incredibile di problemi per l'utente.
- Nonostante ciò, l'interoperabilità rimane un grosso problema nella pratica perché la configurazione di molti dispositivi, cavi e opzioni software può portare svariati problemi e perdite di tempo e di denaro.

Gli Standard

- A questo problema, fortunatamente, c'è una soluzione largamente accettata: gli standard industriali.
- Questi sono descrizioni formali di interfacce tra apparecchiature, ognuna delle quali considerata con le proprie caratteristiche.
- Ad esempio, una ditta potrebbe costruire una scheda di rete Ethernet 10BaseT, mentre un'altra ditta potrebbe costruire un hub 10BaseT.
- I due prodotti dovrebbero essere interoperabili, in quanto sono stati costruiti secondo le stesse specifiche contenute nello standard 802.3 10BaseT e, come vedremo, ci sono tecniche per verificare l'interoperabilità attraverso una serie di funzioni definite nelle moderne architetture di rete.

L'interoperabilità e la stesura degli standard sono elementi di importanza critica per le ragioni seguenti

1° Ragione

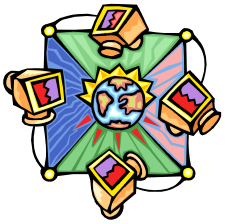
- Gli utenti hanno una grande varietà di prodotti tra cui scegliere e, inoltre, sono liberi di utilizzare un mix di prodotti per andare incontro alle proprie esigenze.
- Gli utenti possono anche ridurre il rischio di usare prodotti di un unico produttore, specialmente se quest'ultimo è una piccola ditta o una ditta nuova sul mercato.
- Gli standard incoraggiano lo sviluppo di una varietà di prodotti nuovi, aumentando il numero delle scelte disponibili.

2° Ragione

- Tutti questi prodotti favoriscono la competizione, portando come conseguenza un abbassamento dei prezzi, e una maggiore possibilità di scelta tra prodottidalle diverse caratteristiche.
- Estensioni degli standard, a patto che non creino incompatibilità, possono essere usate come elementi di differenziazione di prodotti simili

3° Ragione

- Gli standard rappresentano la legittimazione che le nuove tecnologie richiedono per stabilire un punto di partenza sul mercato.
- Ad esempio, le WLAN potrebbero essere viste solamente come adatte per applicazioni specialistiche e di nicchia.
- Grazie a standard come IEEE 802.11, le WLAN stanno godendo di una crescita rapida, permettendo l'espansione di opportunità e colmando le necessità di utenti che diventano consapevoli del fatto che la tecnologia delle LAN senza fili è dovuta all'esistenza di standard industriali.

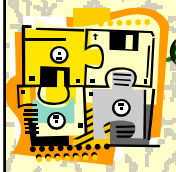


Conformità agli Standard

- Una preoccupazione di base, comunque, è come determinare se un qualsiasi prodotto realmente è conforme ad un standard dato.
- Potrebbe essere davvero frustrante comprare un prodotto che si pensa essere conforme, per poi scoprire che un suo (apparente) malfunzionamento, spesso è dovuto ad una leggera incompatibilità con l'infrastruttura esistente.
- Per questa ragione sono seguite procedure specializzate per verificare le funzionalità di un prodotto a vari livelli.

Verificata la conformità allo standard

- Poiché gli standard definiscono interoperabilità al livello di interfaccia, ***vengono svolte prove che verificano la funzionalità dell'interfaccia stessa*** (sia essa aria o filo).

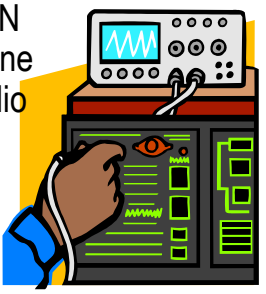


Esame dell'interoperabilità tra due componenti specifici

- Esame dell'interoperabilità tra due componenti specifici; questo di solito è effettuato con software specializzati che testano i due componenti che lavorano insieme.
- Si fa esplicitamente notare che, specialmente con standard complessi, possono essere realizzate interoperabilità solamente parziali: ad esempio, delle caratteristiche di un standard potrebbero non essere supportate, e questa situazione potrebbe essere anche accettabile in alcuni casi.
- Una volta che l'interoperabilità tra due dispositivi è accertata, possono essere compiute prove con un numero maggiore di dispositivi per la valutazione di carichi realistici di lavoro e per testare la robustezza del protocollo.

Valutazione delle prestazioni

- Sfortunatamente, mentre possono essere usati benchmarks per misurare le prestazioni di LAN wired, per le WLAN bisogna prestare attenzione alla natura fortemente dinamica dei canali radio durante l'esecuzione del ***benchmark***, specialmente quando si opera su bande di frequenza senza licenza.
- Possono essere richiesti dispositivi di misura specializzati, come ***analizzatori di spettro o di rete***, in unione ad ***analizzatori di protocollo***, per determinare situazioni patologiche.



Accertare l'interoperabilità delle Wireless LAN

- In linea di principio, il processo per determinare l'interoperabilità nelle LAN senza fili è identico a quello usato nel caso di LAN cablate.
- La maggior parte delle volte, questo processo coinvolge l'uso di procedure attentamente documentate incorporate in suites software che verificano gli aspetti specifici dell'interoperabilità per controllare la compatibilità con altri dispositivi.
- Nel caso di LAN senza fili, l'interoperabilità deve essere verificata mediante un gran numero di fattori……

Operativamente….

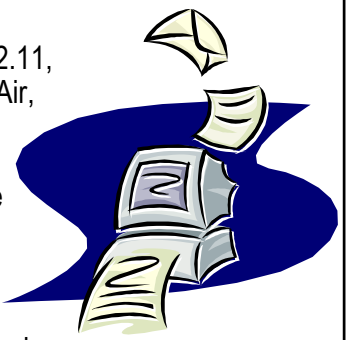
- Le realizzazioni e le specifiche dello strato PHY devono combaciare; questo include la coincidenza delle regolamentazioni locali (diverse per ogni nazione) per la particolare banda usata (tipicamente coinvolgendo larghezza di banda, antenne e limitazioni sull'energia di trasmissione).
- Per esempio, due sistemi potrebbero essere potenzialmente interoperabili, se entrambi operano alla frequenza di 2.4 GHz e usano protocolli FHSS.

Operativamente….

- Ci possono essere molte caratteristiche specifiche dello strato MAC per le LAN senza fili.
- Questo può includere il supporto per la sicurezza, gestione del risparmio energetico, ritrasmissione automatica nel caso di un errore (anche noto come ARQ), e molte altre caratteristiche.
- È possibile che non tutti i fabbricanti supportino ogni caratteristica disponibile in una specificazione di strato MAC e, come detto sopra, le differenti interpretazioni di uno standard, possono creare una grande varietà di non interoperabilità patologiche.

Wireless Standard

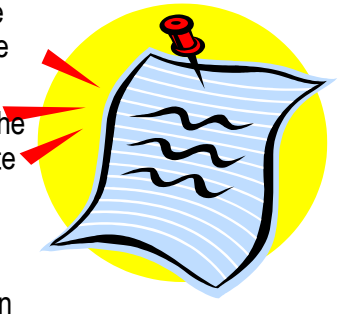
- Si fa notare esplicitamente che esistono molti standard di WLAN, inclusi la famiglia IEEE 802.11, il Wireless LAN Interoperability Forum's OpenAir, la European Telecommunications Standards Association's (ETSI) HYPERLAN, gli standard emergenti HomeRF e Bluetooth, e una grande varietà di realizzazioni proprietarie.



- Ma suites di prova opportunamente realizzate possono identificare anche incompatibilità minori, indicando problemi in un ambiente controllato.

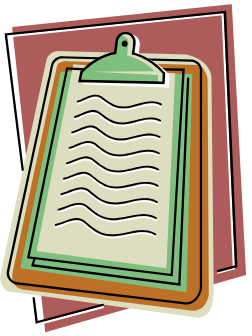
Osservazioni

- Ciascun prodotto deve supportare un insieme di driver per specifici sistemi operativi di rete inclusi Windows 9x, Windows NT, Netware e potenzialmente molti altri.
- Si dovrebbe fare attenzione anche al fatto che possono esistere prodotti che semplicemente non possono essere esaminati perché non sono parte di un standard.
- Per esempio, interoperabilità tra AP non è parte dello standard 802.11, e quindi ciascun produttore di AP definisce i suoi propri protocolli per l'handoff e il bilanciamento del carico.



Osservazioni….

- Funzioni di rete di alto livello (ad esempio allo strato della rete o superiori) possono essere verificate con mezzi che non sono specifici dello strato fisico.
- È importante tenere presente, inoltre, che l'interoperabilità deve essere realizzata attraverso tutta la pila del protocollo.
- Dato il livello di complessità, dovrebbe essere evidente che le suites software per i test dell'interoperabilità possono essere molto complesse.



UNH - IOL

- È stato sviluppato un certo numero di suites software per testare l'interoperabilità fra LAN senza fili.
- Le suites più note sono state sviluppate **nell'InterOperability Lab (IOL) dell'Università del New Hampshire (UNH**), noto per le sue ricerche nel verificare le interoperabilità in molte classi di dispositivi di trasmissione.
- UNH ha definito un numero di prove per lo strato PHY sia nel caso di trasmissione diretta che nel caso di Frequency Hopping.

Test imposti dall' UNH - IOL

- Test di interoperabilità punto a punto che verifichi che un AP possa comunicare con un terminale mobile.
- Test per verificare il tasso di errore che generi traffico multicast tra un AP e un certo numero di terminali.
- Test di accesso remoto che generi traffico tra un AP e vari terminali, verificando che tutti ricevono lo stesso traffico.
- Test di failover che si assicuri che sia possibile associare un gruppo di terminali con un altro AP nel caso di un malfunzionamento dell'AP al quale erano precedentemente connessi.
- Test di configurazione di reti di grandi dimensioni che esamini il tasso di errore in configurazioni di LAN senza fili tipiche di vere installazioni (punti dell'accesso multipli e terminali multipli).

Osservazioni

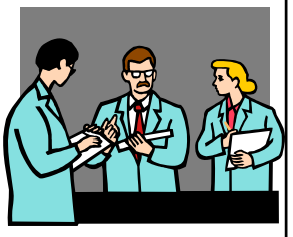
- UNH ha definito anche una serie di prove disegnate per indirizzare caratteristiche specifiche del livello MAC.
- Mentre UNH progetta procedure di test e installazione per produttori per favorire l'interoperabilità, non è certificata l'interoperabilità del prodotto individuale.

Wireless LAN Interoperability Forum (WLI)

- Ha definito una serie di prove procedurali per verificare l'interoperabilità con un minimo di software speciale.
- Tale collaudo, quando effettuato sotto condizioni molto precise, può verificare rapidamente che un dato prodotto sia interoperabile.
- Il Forum WLI pubblica le informazioni sui prodotti interoperabili e le correda di certificati per aiutare i clienti a prendere decisioni sull'acquisto.

Wireless LAN Interoperability Forum (WLI)

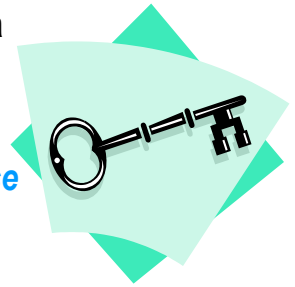
- Appena è stata accertata l'interoperabilità di base, possono essere eseguite prove supplementari per la verifica del throughput, dell'area di copertura effettiva e delle caratteristiche prestazionali.
- Questi possono includere benchmarks di LAN orientate alle prestazioni, o programmi che generano un carico di lavoro sintetico tipico di una classe di applicazioni.
- Utility diagnostiche incluse nei prodotti possono essere utili nell'isolare problemi di interoperabilità più piccoli, al fine di ottenere il massimo della produttività, dell'affidabilità, e della gestione operativa.



Caratteristiche di sicurezza nelle Wireless LAN

Caratteristiche di sicurezza nelle Wireless LAN

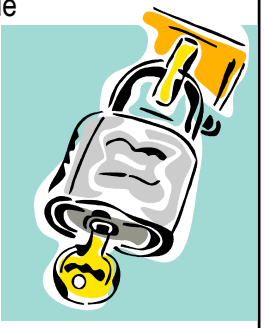
Le problematiche fondamentali relative alla sicurezza nelle WLAN comprendono:



- *L'accesso non autorizzato alle risorse di rete mediante dispositivi wireless.*
- *L'intercettazione delle trasmissioni.*

Tecniche per garantire la sicurezza

- A seconda dell'implementazione del protocollo 802.11 da parte di un costruttore, è possibile identificare varie tecniche per garantire la sicurezza:
  - Il **Pattern Chipping**;
  - Il **Frequency Hopping**;
  - L'**Identificativo di sicurezza (ID)**;
  - L'uso delle **Virtual Private Networks (VPN).**



- Questi meccanismi operano in stretto legame con i meccanismi di sicurezza implementati per le normali reti cablate.

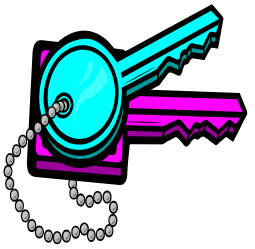
Caratteristiche di sicurezza nel Pattern Chipping

- E' una tecnica di codifica, effettuata dal livello fisico, che consiste nella rappresentazione di un singolo bit di informazione mediante un pattern complesso di bit, chiamato **Chip**.

- Il punto forte di questa tecnica è che essa è facilmente implementabile ed altamente efficace (si può raggiungere un enorme grado di affidabilità se, al momento della connessione, si determinano aleatoriamente i pattern per la rappresentazione dei bit).

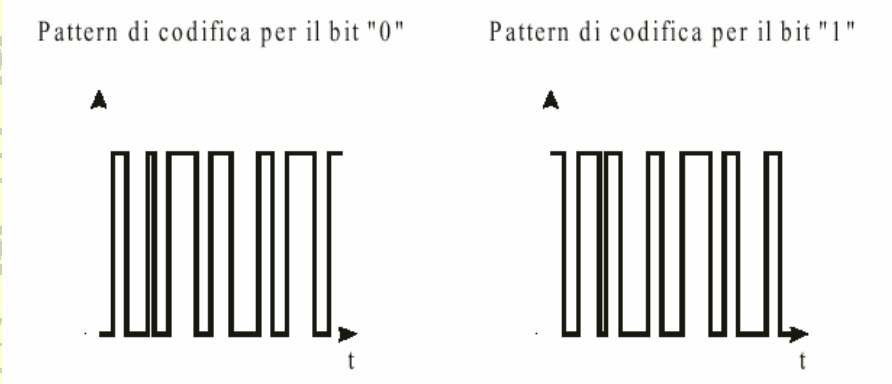
Caratteristiche di sicurezza nel Pattern Chipping

- Un altro grosso vantaggio di questa tecnologia consiste nell'elevato grado di recupero dei dati nel caso di corruzione durante la trasmissione: infatti, come è noto dalla teoria dell'informazione, aumentando il numero di bit necessari alla trasmissione (aumentando la ridondanza), mediante tecniche statistiche, aumenta la probabilità di poter recuperare dati contenenti errori.



- D'altronde, l'utilizzo di questa tecnica comporta un notevole spreco di banda.

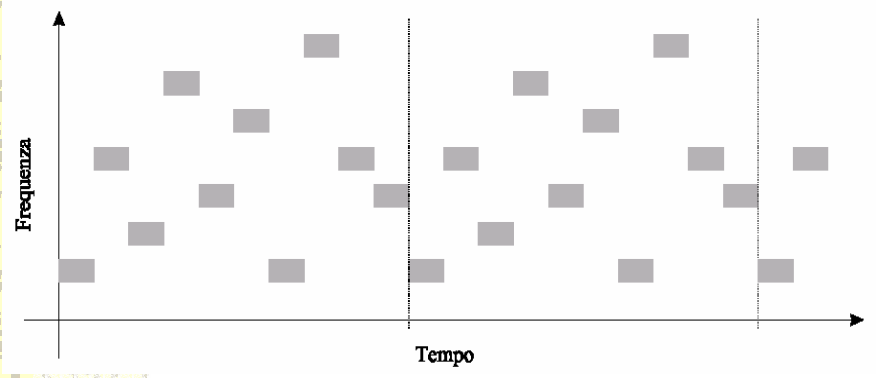
Caratteristiche di sicurezza nel Pattern Chipping



Caratteristiche di sicurezza del Frequency Hopping

- Una della ragioni chiave per cui si utilizza il Frequency Hopping è la qualità della sicurezza che deriva da questa tecnica: infatti, essa è stata originariamente elaborata ed usata dall'Esercito degli Stati Uniti per rendere sicure le proprie comunicazioni. Infatti, il segnale salta da frequenza a frequenza mediante una sequenza casuale e ripetitiva.
- Per comunicare correttamente, quindi, sia il trasmittente che ricevitore devono essere sincronizzati sulla stessa sequenza.
- Per complicare maggiormente la decodifica, questo tipo di segnalazione ha una durata temporale molto breve nel periodo in cui si è fissata una certa frequenza di trasmissione.
- Queste impostazioni non possono essere variate dall'utente.

Caratteristiche di sicurezza del Frequency Hopping



Ing. Cristian Randieri – Intellisystem Technologies
Introduzione alle nuove tecnologie Wireless per il Networking –
www.intellisystem.it

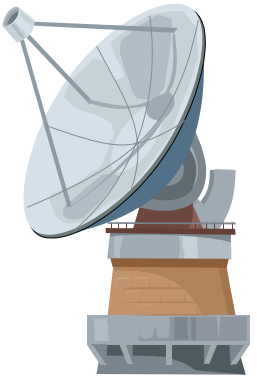
Identificativo di Sicurezza: come lavora l'ID

- L'ID è una stringa di caratteri unica, costituita da una sequenza di venti caratteri alfanumerici definita e configurata dall'utente; ogni dispositivo radio facente parte della stessa rete deve essere configurato allo stesso modo.
- Una volta configurato, l'ID è ridotto a 20 bit mediante algoritmi proprietari della casa costruttrice.
- Esso è trasmesso con l'indirizzo radio MAC (un campo di dodici caratteri, unico per ogni stazione), che lo nasconde mediante un altro algoritmo anch'esso proprietario.
- Questi dati "mescolati" sono memorizzati nella EEPROM della trasmittente mediante uno schema di memorizzazione segreto: con questa tecnica, l'ID non può essere violato da nessun mezzo esistente, neanche dalla casa costruttrice.

Accesso all'ID via etere

I passi dovrebbero essere i seguenti:

1. Determinare e seguire il pattern del FH;
2. Demodulare il flusso dei dati;
3. Decodificare il flusso dei dati (codificato con un algoritmo proprietario a monte della trasmissione);
4. Determinare quali, tra i 1500 byte del pacchetto, sono i 20 bit dell'ID;
5. Ricavare, a partire dai 20 bit così ricavati, la sequenza di 20 caratteri che costituisce l'ID.



Accesso all'ID via etere

- Con questo sistema sono possibili oltre 15 milioni di codici ID.
- Così, anche se qualcuno volesse cercare di violare il codice, impiegherebbe un tempo superiore ai 2 anni. Inoltre, data la potenza RF di trasmissione relativamente bassa, la persona che vorrebbe violare il codice dovrebbe trovarsi nel raggio di circa 150 m (o meno, se si lavora in interni).
- Se si dimentica il codice ID, deve essere selezionato un nuovo codice ID e devono essere resettati tutti i dispositivi nella rete.

Accesso all'ID via etere

- Per aumentare ulteriormente il grado di sicurezza della rete, esistono delle tabelle di autorizzazione contenenti gli indirizzi MAC legali.
- È pertanto possibile utilizzare queste tabelle per consentire l'accesso alla rete solo agli utenti regolarmente registrati. Inoltre, se un utente con un indirizzo di MAC non autorizzato tenta di accedere in rete, questo evento sarà registrato e riportato all'amministratore di rete.

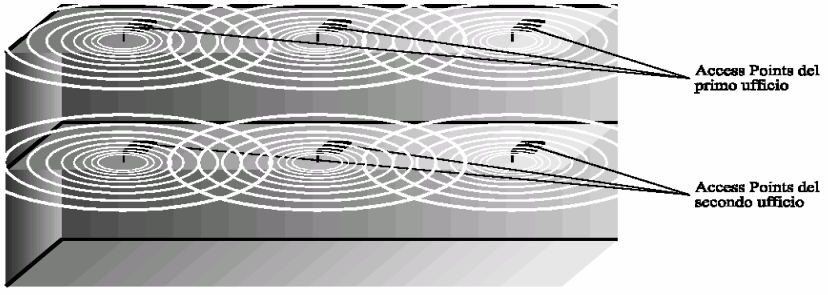
Ing. Cristian Randieri – Intellisystem Technologies
Introduzione alle nuove tecnologie Wireless per il Networking –
www.intellisystem.it

Rendere sicura la coesistenza di reti Wireless

- Un altro aspetto molto importante relativo alla sicurezza è quello della coesistenza, in ambienti confinanti, di WLAN diverse.
- Per garantire tale coesistenza, si deve definire un ID diverso per ogni dominio, ad esempio, definendo un “Dominio 1” per un gruppo di utenti che condivide un ID comune, e un “Dominio 2” per un altro gruppo di utenti che condivide un ID diverso.
- Data questa configurazione, non potrà mai verificarsi che un utente del dominio 1 possa accedere al dominio 2 rete e viceversa.

Esempio

- Supponiamo che in un edificio, in due piani adiacenti esistano due uffici, che chiameremo per convenzione “Ufficio 1” e “Ufficio 2” e ognuno dei due uffici abbia definito un proprio ID diverso dall’altro.
- Allora, un utente dell’Ufficio 1 non potrà accedere alla rete dell’Ufficio 2, e viceversa.
- Tutto questo è dovuto semplicemente alla differenza di ID tra i due uffici.



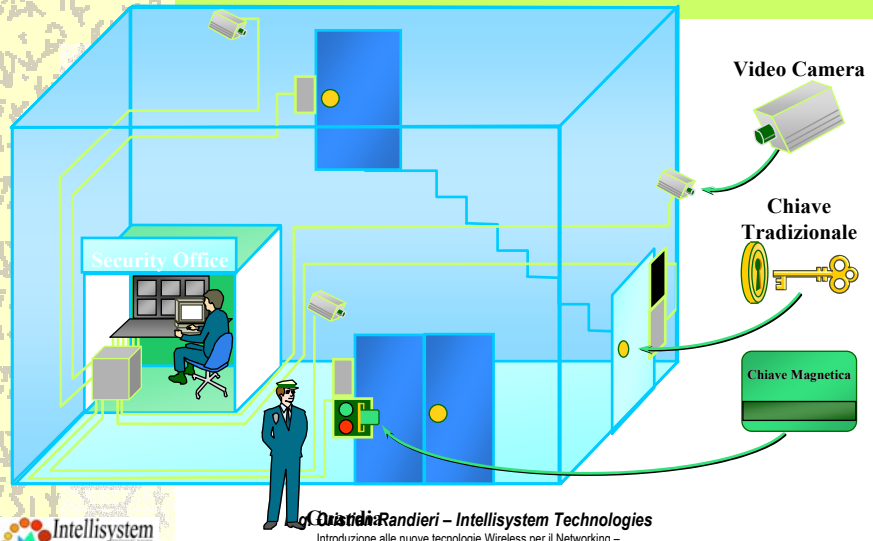
Quando è richiesta maggiore sicurezza: VPN

- Un metodo per garantire questa maggiore sicurezza si basa sull'uso delle **Virtual Private Networks (VPN)** e della crittografia.
- Le VPN sono state sviluppate per fornire un elevato livello di sicurezza per trasmissioni dei dati riservati su reti pubbliche come Internet.
- Questo metodo di sicurezza ha guadagnato grandi consensi ed è stato usato estensivamente da società che desiderano fornire un accesso ai loro dati sociali per trasmetterli ad impiegati in uffici remoti senza usare linee dedicate e costose.
- Questa tecnica si presta bene anche per trasmettere sulle LAN.

Cosa è una VPN?

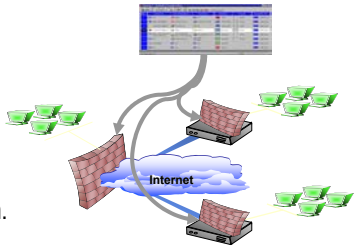
- Virtual Private Network
- Usa Internet (quindi a rete pubblica network) al fine di creare una Rete Virtuale Privata.
- Elementi chiave di una VPN sono:
  - ***Authentication***
  - ***Encryption***

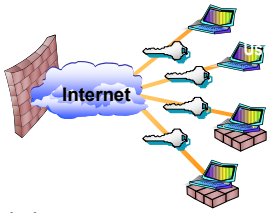
Sicurezza: Analogia Fisica



Tipi di VPN

- ***Site to Site:***
  - Riduce I costi WAN/Telecomm.
  - Migliora la ridondanza.
  - Gestisce la bandwidth.
- ***Client to Site*** (accesso remoto):
  - Accesso Remoto per sostituire i pools modem.
  - Abilita gli utenti DSL e Cable Modem.
  - Riduce I costi comuni (local dial access).
- ***Partner/Client Extranet***:
  - Abilita possibili servizi Business.

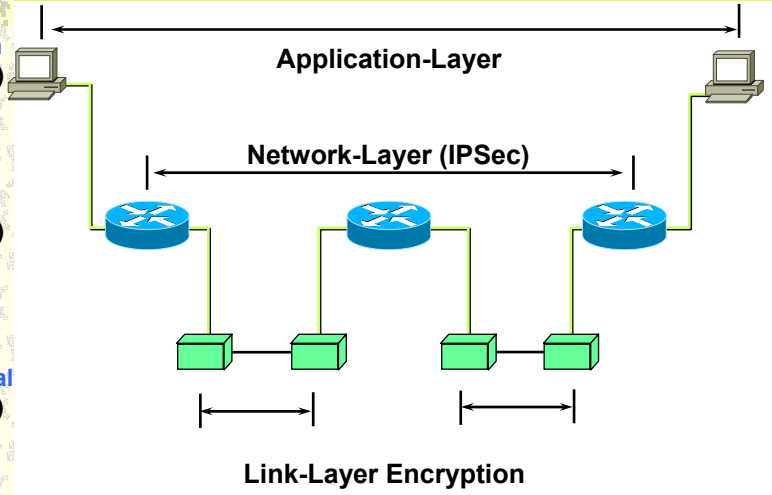




Internet Prototol Security (IPSec)

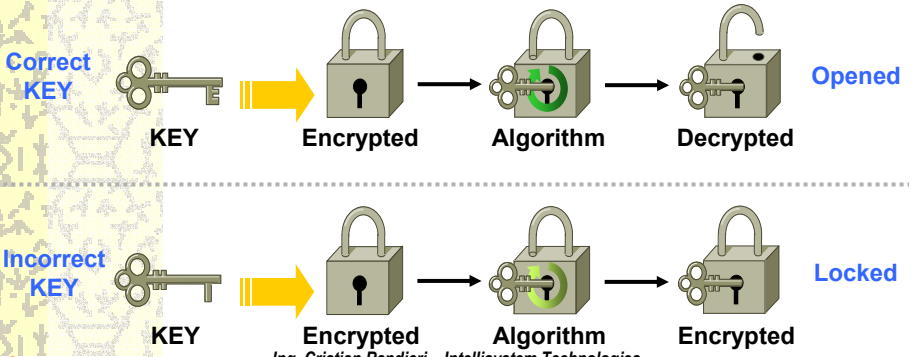
- Si adoperano un set di protocolli ed algoritmi per garantire la sicurezza dei dati a livello network.
- IPSec garantisce una protezione dei dati (encryption), integrità (hash), autenticazione (signature/certificate) dei pacchetti IP pur mantenendo l'abilità di fare I routing attraverso reti IP.
- IPSec si compone dei seguenti protocolli:
  - ***3DES (Data Encryption Standard) Encryption (DES).***
  - ***IKE (Internet Key Exchange).***
  - ***Si possono anche adoperare RSA/DSS, X.509v3 or MD5/SHA per la Gestione/Scambio delle chiavi.***

Livelli di Crittografia



Autenticazione

Chiave – Valore da porre in ingresso ad un algoritmo che deve produrre un unico risultato in uscita.



Processo di crittografia

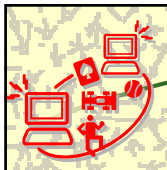
Chiave (numerica) | **Messagio (convertito numericamente)** | **Encryption Algorithm** | **Encrypted Output**

Protocollo 802.11

Protocollo 802.11

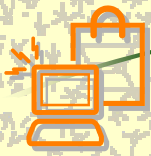
- Una 802.11 LAN è basata su una architettura cellulare in cui l'area in cui deve essere distribuito il servizio viene suddivisa in celle proprio come accade nei sistemi di distribuzione per servizi di telefonia GSM.

- Ciascuna cella (chiamata ***Basic Service Set*** o *BSS* nella nomenclatura) è controllata da una stazione base denominata ***Access Point*** o più semplicemente *A*P.



Standard 802.11

- Sebbene una wireless LAN possa essere formata da una singola cella, con un singolo ***Access Point*** (e come sarà descritto successivamente, esiste un modo di funzionamento privo di Access Point), la maggior parte delle installazioni sarà formata da una molteplicità di celle dove i singoli Access Point sono interconnessi attraverso un qualche tipo di rete di distribuzione (che normalmente viene definita ***Distribution System* o *DS***);

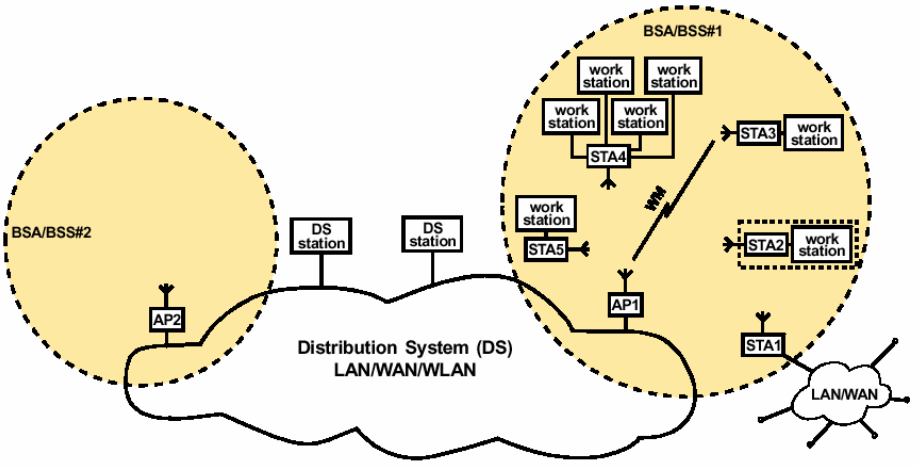


Standard 802.11

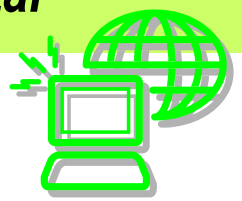
- La rete di distribuzione è normalmente costituita da una dorsale Ethernet e in certi casi è wireless essa stessa.

- Il complesso delle diverse wireless LAN interconnesse, comprendenti differenti celle, i relativi Access Point e il sistema di distribuzione, viene visto come una singola rete 802 dai livelli superiori del modello OSI ed è noto nello standard come ***Extended Service Set (ESS).***

Schema di una tipica rete LAN basata sul protocollo 802.11



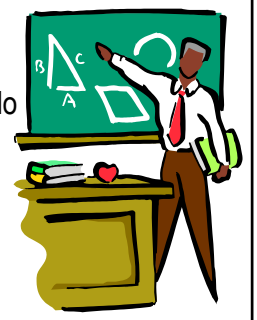
Concetto di Portal



- Lo standard definisce anche il concetto di *Portal*.
- Un ***Portal*** è un dispositivo che permette l'interconnessione tra una rete LAN 802.11 e un'altra rete 802. Questo concetto rappresenta una descrizione astratta di una parte delle funzionalità di un ***translation bridge***. Anche se lo standard non lo richiede espressamente, la maggior parte delle installazioni riuniscono l'Access Point e il Portal in un'unica entità fisica.

Descrizione degli strati dell'IEEE 802.11

Come tutti gli altri protocolli 802.x, anche il protocollo 802.11 prende in considerazione i due livelli di MAC e livello fisico.



Lo standard attualmente disponibile definisce un singolo livello MAC che può interagire con i seguenti tre livelli fisici, operanti a velocità variabili tra 1 e 3 Mbit/s:

- ***Frequency Hopping Spread Spectrum (FHSS) nella banda ISM 2,4 GHz.***
- ***Direct Sequence Spread Spectrum (DSSS) nella banda ISM 2,4 GHz.***
- ***Trasmissione infrarossa.***

Descrizione degli strati dell'IEEE 802.11

- Oltre alle funzionalità standard usualmente fornite dai livelli MAC dei protocolli 802.x, il MAC 802.11 supporta delle funzionalità aggiuntive, tipiche dei livelli superiori dello stack protocollare, come gestione della frammentazione, la ritrasmissione dei pacchetti e gestione dell'acknowledgements.

802.2			Data Link Layer
802.11 MAC			
FH	DS	IR	PHY Layer

Livello MAC

- Il livello MAC definisce come metodo di accesso il **Distributed Coordination Functio**n.
- Questo è un meccanismo di tipo **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)** che lavora in questo modo: una stazione che vuole trasmettere, ascolta il mezzo.
- Se il mezzo è occupato, allora sposta la trasmissione ad un altro momento mentre, se il mezzo è libero, trasmette subito.
- Questo tipo di protocollo è abbastanza efficiente quando il mezzo non è molto utilizzato, permettendo alle stazioni di trasmettere con piccoli ritardi; nonostante ciò, la probabilità che due o più stazioni decidano di trasmettere contemporaneamente, generando una collisione, non è nulla.

Livello MAC

- Queste collisioni devono essere identificate in modo tale che lo strato MAC possa ritrasmettere il pacchetto da solo senza nessun intervento da parte degli strati superiori, cosa che evita ritardi inutili.
- Mentre questi meccanismi di Collision Detection sono facilmente implementabili per reti cablate, per reti wireless non possono essere usati per due motivi:

Livello MAC

1. L'implementazione di un meccanismo di collision detection richiederebbe la progettazione di ricetrasmettitori full duplex, capaci cioè di trasmettere e di ricevere contemporaneamente, facendo lievitare i costi di produzione.
2. In un ambiente wireless, non si può fare l'ipotesi che tutte le stazioni si ascoltino tra loro (cosa che invece è richiesta nel meccanismo di collision detection), perché anche se il trasmettitore sente libero il mezzo intorno a sé, non è detto che intorno al ricevitore il mezzo sia altrettanto libero.

Collision Avoidance

Per prevenire questi problemi, lo standard usa un meccanismo di **Collision Avoidanc**e:

- Una stazione che vuole trasmettere ascolta il mezzo. Se il mezzo è occupato, allora sposta la trasmissione ad un altro momento. Se in un certo istante di tempo (chiamato **Distributed Inter Frame Space (DIFS))** il mezzo è libero, la stazione può trasmettere.
- La stazione destinataria controlla il CRC del pacchetto ricevuto e manda un ACK. La ricezione dell'ACK indica che non è avvenuta nessuna collisione in trasmissione. Se il mittente non riceve l'ACK allora ritrasmette il frammento fino a quando non riceve l'ACK o fino a quando non ha esaurito i tentativi a sua disposizione.

Virtual Carrier Sense

- **Per ridurre la probabilità che due stazioni collidano, lo standard definisce un meccanismo di Virtual Carrier Sense.**
- **La stazione che vuole trasmettere, prima invia un piccolo pacchetto broadcast, chiamato RTS (Request To Send), che include informazioni sulla sorgente, sulla destinazione e sulla durata della transazione seguente (ad esempio la durata della trasmissione del pacchetto e dell'ACK conseguente); la stazione che deve ricevere risponde (se il mezzo è libero) con un pacchetto broadcast di controllo chiamato CTS (Clear To Send) che include la stessa informazione circa la durata della trasmissione.**
- **Tutte le stazioni che ricevono i pacchetti RTS e CTS modificano l'indicatore Virtual Carrier Sense (chiamato Network Allocation Vector (NAV)) per la durata indicata, in**

Livello MAC

- Il meccanismo di accesso base è denominato ***Distributed Coordination Function***, basato sul meccanismo di accesso multiplo con rilevamento della portate e prevenzione delle collisioni *(**Carrier Sense Multiple Access con Collision Avoidence*** o in forma più compatta *CSMA/CA*).

Livello MAC

- Nel caso dell'Ethernet questa situazione di collisione è rilevata dalla stazione trasmittente la quale entra in una fase di ritrasmissione basata su algoritmo di posticipo della trasmissione denominato ***Exponential Random Backoff algorithm***, il quale fissa arbitrariamente un tempo di ritrasmissione al termine del quale viene nuovamente testato il mezzo trasmissivo, e se è ancora occupato il tempo di ritrasmissione viene aumentato con logica esponenziale.
- Mentre questo meccanismo di rilevamento della collisione è un'ottima idea nel caso di wired LAN, è assolutamente esclusa la sua adozione nel caso in cui il mezzo trasmissivo sia il canale radio per due ragioni principali…..

Livello MAC

- L'implementazione di un meccanismo di rilevamento della collisione richiederebbe l'immediata implementazione di capacità di trasmissione e ricezione Full Duplex. Questo approccio porterebbe ad un significativo incremento del prezzo degli apparati.
- In un ambiente wireless non è possibile assumere che una stazione sia in grado di sentire l'attività di tutte le altre (questa ipotesi è alla base dello schema di rilevamento della collisione). In quest'ottica se una stazione che vuole trasmettere rileva la non occupazione del mezzo, non necessariamente significa che il mezzo sia libero attorno all'area di ricezione.

Livello MAC: Collision avoidance & Positive acknowledge

Allo scopo di superare questi problemi, l'802.11 utilizza un meccanismo di collision avoidance unito ad uno schema di *positive acknowledg*e, il cui funzionamento è il seguente:

- Una stazione che vuole trasmettere testa il mezzo trasmissivo. Se il mezzo è occupato la trasmissione verrà deferita. Se il mezzo è libero per un certo tempo, denominato ***Distributed Inter Frame Space (DIFS)*** nello standard, la stazione effettua la trasmissione.
- La stazione destinataria controlla il CRC del pacchetto ricevuto e manda un ACK. La ricezione dell'ACK indica che non è avvenuta nessuna collisione in trasmissione. Se il mittente non riceve l'ACK allora ritrasmette il frammento fino a quando non riceve l'ACK o fino a quando non ha esaurito i tentativi a sua disposizione.

Livello MAC: metodi d'accesso

Il livello di MAC definisce due differenti metodi di accesso quali:

- **CSMA/CA**
- **Virtual Carrier Sense**
- **Acknowledgment a livello di MAC**
- **Fragmentation e Reassembly**
- **Inter Frame Spaces**
- **Exponential Backoff Algorithm**

Distributed Coordination Function

- Il meccanismo di accesso base è denominato *Distributed Coordination Function*, basato sul ben noto meccanismo di accesso multiplo con rilevamento della portate e prevenzione delle collisioni *(Carrier Sense Multiple Access con Collision Avoidence* o o *C*D).
- Questi tipi di protocolli sono molto efficienti se il mezzo di trasmissione non è pesantemente caricato in quanto le stazioni possono trasmettere con il minimo ritardo.
- Nel caso dell'Ethernet una situazione di collisione è rilevata dalla stazione trasmittente la quale entra in una fase di ritrasmissione basata su algoritmo di posticipo della trasmissione denominato *Exponential Random Backoff algorithm* [WLAN1], il quale fissa arbitrariamente un tempo di ritrasmissione al termine del quale viene nuovamente testato il mezzo trasmissivo e se è ancora occupato il tempo di ritrasmissione viene aumentato con logica esponenziale.

Distributed Coordination Function

- Mentre questo meccanismo di rilevamento della collisione è un'ottima idea nel caso di wired LAN, è assolutamente esclusa la sua adozione nel caso in cui il mezzo trasmissivo sia il canale radio per due ragioni principali:

1) L'implementazione di un meccanismo di rilevamento della collisione richiederebbe l'immediata implementazione di capacità di trasmissione e ricezione Full Duplex. Questo approccio porterebbe ad un significativo incremento del prezzo degli apparati.

2) In un ambiente wireless non è possibile assumere che una stazione sia in grado di sentire l'attività di tutte le altre (questa ipotesi è alla base dello schema di rilevamento della collisione). In quest'ottica se una stazione che vuole trasmettere rileva la non occupazione del mezzo, non necessariamente significa che il mezzo sia libero attorno all'area di ricezione.

Distributed Coordination Function

- Allo scopo di superare questi problemi, l'802.11 utilizza un meccanismo di collision avoidance unito ad uno schema di *positive acknowledg*e, il cui funzionamento è il seguente:

1) Una stazione che vuole trasmettere testa il mezzo trasmissivo. Se il mezzo è occupato la trasmissione verrà deferita. Se il mezzo è libero per un certo tempo, denominato Distributed Inter Frame Space (DIFS) [WLAN1] nello standard, la stazione effettua la trasmissione:

2) La stazione ricevente controlla il CRC del pacchetto ricevuto e invia un pacchetto di acknowledgement (ACK). La ricezione di questo pacchetto indica alla stazione trasmittente che non si è verificata nessuna situazione di collisione. Se la stazione che ha iniziato la trasmissione non riceve l'acknowledgement allora ritrasmetterà il pacchetto fintanto che non riceve un pacchetto di acknowledge. E' comunque fissato un numero massimo di ritrasmissioni oltre il quale il pacchetto viene buttato via.

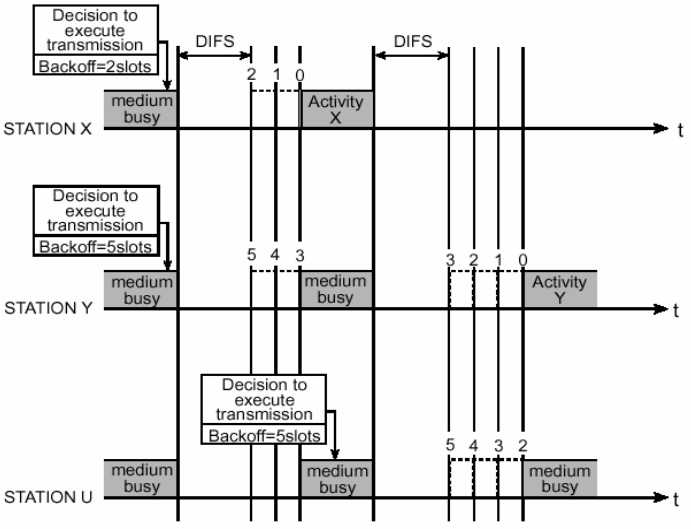
Virtual Carrier Sense

- Allo scopo di ridurre la probabilità che si verifichi una situazione di collisione tra due stazioni a causa della impossibilità di ciascuna stazione di sentire tutte le altre, lo standard definisce un meccanismo denominato *Virtual Carrier Sense* [WLAN1]:
- Una stazione che vuole trasmettere innanzitutto procede alla trasmissione di un breve pacchetto di controllo denominato *RTS (Request To Send*) che contiene l'identificativo della sorgente e della destinazione oltre alla durata della successiva trasmissione relativa al pacchetto RTS e al rispettivo *ACK*.
- La stazione di destinazione risponde (se il mezzo è libero) con un pacchetto di controllo denominato *CTS (Clear To Send*) con la stessa informazione relativa alla durata di trasmissione. Tutte le stazioni ricevendo sia un RTS sia un CTS, settano l'indicatore *Virtual Carrier Sense* (chiamato *NAV* che sta per *Network Allocation Vector*), per un certo tempo ed utilizzano questa informazione insieme con il Phisical Carrier Sense al momento in cui vanno a effettuare la rilevazione di occupazione del mezzo.
- Questo meccanismo riduce la probabilità di collisione su un'area di ricezione che è nascosta all'interno dell'intervallo di tempo necessario alla trasmissione dell'RTS poiché la stazione sente il CTS e definisce il mezzo come occupato fino alla fine della trasmissione.
- L'informazione relativa al tempo di trasmissione protegge inoltre l'area del trasmettitore dalle collisioni durante l'ACK da parte di quelle stazioni che sono fuori dall'area di visibilità della stazione che deve fornire l'acknowledge.

Osservazioni

- A causa delle ridotte dimensioni dei pacchetti RTS e CTS, il meccanismo riduce anche l'overhead dovuto alla collisione, poiché non è necessaria la ritrasmissione dell'intero pacchetto dati. Questo è vero se il pacchetto dati è significativamente maggiore rispetto all'RTS. Per questo motivo lo standard prevede una variante in cui se il pacchetto è breve può essere ritrasmesso senza la transazione RTS/CTS. Tutto ciò è controllato in ogni stazione da un parametro detto *RTS Threshold*.

Transazione tra due stazioni A e B con relativo settaggio del NAV nelle stazioni vicine



Acknowledgment a livello di MAC

- Il livello di MAC realizza il rilevamento della collisione aspettando la ricezione di un acknowledge per ogni frammento trasmesso.
- I pacchetti che hanno più di una destinazione, come i pacchetti multicast, non sono soggetti al meccanismo di acknowledge.

Fragmentation e Reassembly

- Tipicamente i protocolli per reti locali utilizzano pacchetti aventi dimensioni di diverse centinaia di bytes. Ci sono però molte ragioni che spingono all'utilizzo di pacchetti di dimensioni minori in un contesto wireless LAN:
- A causa della elevata Bit Error Rate di un collegamento radio, la probabilità che un pacchetto sia corrotto durante la fase di trasmissione aumenta all'aumentare della dimensione del pacchetto.
- Nel caso in cui un pacchetto ricevuto debba essere ritrasmesso, l'overhead introdotto dal processo di trasmissione decresce con la dimensione del pacchetto.
- In un sistema Frequency Hopping non è garantita la continuità del mezzo trasmissivo a causa dei salti di frequenza (nel nostro caso questi salti avvengono ogni 20 ms.). Riducendo la dimensione del pacchetto diminuisce la probabilità che la trasmissione sia posticipata dopo il tempo di pausa (dwell time).

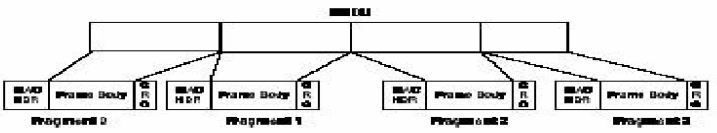
Fragmentation e Reassembly

- Di conseguenza è impensabile introdurre un nuovo protocollo che non possa trattare pacchetti di dimensione di 1518 bytes come quelli utilizzati nell'Ethernet, così l'organismo di standardizzazione ha deciso di aggiungere un semplice meccanismo di frammentazione e riassemblaggio al livello di MAC.
- Il meccanismo è costituito da un semplice algoritmo Send-and-Wait che non consente ad una stazione di trasmettere un nuovo frammento finché non sia verificata una delle seguenti situazioni:
  - § Ricezione di un ACK per il frammento precedentemente trasmesso.
  - § Decide che il frammento è stato ritrasmesso troppe volte ed elimina tutto il frame.

Bisogna notare che lo standard permette alla stazione di trasmettere a un differente indirizzo tra la ritrasmissione di un dato frammento. Questo è particolarmente utile quando un AP ha parecchi pacchetti arretrati riferiti a differenti destinazioni e uno di questi non risponde.

Fragmentation e Reassembly

Frame (MSDU) suddiviso in diversi frammenti (MPDUs).



Inter Frame Spaces

- Lo standard definisce quattro tipi di spazi tra i frame (Inter Frame Spaces) [WLAN1], che sono utilizzati per fornire differenti priorità:

§ *SIFS – Short Inter Frame Spac*e, è utilizzato per separare trasmissioni che appartengono ad un singolo dialogo (Fragment-Ack) ed è il più piccolo spazio tra i frame possibile. C'è sempre al più una stazione che trasmette ad un dato istante di tempo, prendendosi dunque la priorità sulle altre. Questo valore è fissato per il livello fisico ed è calcolato in modo tale che la stazione trasmittente possa essere in grado di commutare il suo modo di funzionamento alla ricezione e decodificare il pacchetto entrante. Sul livello fisico dell'802.11 questo valore è settato a 28 ms.

§ *PIFS – Point Coordination IF*S, è usato dall'Access Point (o dal Point Coordinator, come è chiamato in questo caso) per guadagnare l'accesso al mezzo prima di ogni altra stazione. Questo valore è pari al SIFS più uno slot time (definito nel prossimo paragrafo) e vale 78 ms.

Inter Frame Spaces

§ *DIFS – Distributed IF*S, è l'Inter Space Frame utilizzato per una stazione che vuole iniziare una nuova trasmissione. E' calcolato come PIFS più uno slot time e vale quindi 128 ms.

§ *EIFS – Extended IF*S. E' il più lungo IFS ed è usato da una stazione che ha ricevuto un pacchetto di cui non è stata in grado di comprendere il contenuto.

Questo è necessario per proteggere la stazione (la quale non comprende l'informazione di durata necessaria per il virtual carrier sense) da collisioni con i futuri pacchetti appartenenti al dialogo corrente.

Exponential Backoff Algorithm

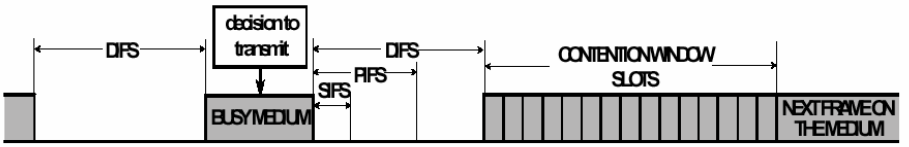
- Il *backoff* è un metodo ben noto per risolvere il contenzioso tra differenti stazioni che vogliono accedere contemporaneamente al mezzo trasmissivo. Il metodo richiede che ciascuna stazione scelga un numero casuale (n) compreso tra 0 e un dato numero e aspetti per questo numero di slot prima di accedere al mezzo, effettuando comunque il controllo sulla portante per vedere se qualche altra stazione ha acceduto al mezzo in precedenza.
- Lo *Slot time* è definito in modo tale che la stazione sia sempre capace di determinare se un'altra stazione ha acceduto al mezzo al inizio del precedente slot. Questo consente di ridurre notevolmente la probabilità di collisione.
- Backoff esponenziale ha il seguente significato: ogni volta che la stazione sceglie uno slot per la trasmissione e si verifica una collisione, sarà esponenzialmente aumentato il massimo valore per la selezione casuale dello slot di trasmissione.

Exponential Backoff Algorithm

- L'802.11 definisce un *algoritmo di backoff esponenziale* [WLAN1] che deve essere eseguito nei seguenti casi:
  - § Quando la stazione testa il mezzo prima della prima trasmissione del pacchetto e il mezzo è occupato
  - § Dopo ciascuna ritrasmissione
  - § Dopo una trasmissione che ha avuto successo.

  Il solo caso in cui il meccanismo non è utilizzato è quando la stazione decide di trasmettere un nuovo pacchetto e il mezzo viene rilevato libero per un tempo maggiore di DIFS.

Schematizzazione del meccanismo di accesso al mezzo



Metodi di accesso ad una BSS

- Una volta che una stazione ha localizzato un Access Point e ha deciso di unirsi alla corrispondente BSS, viene eseguito il Processo di Autenticazione. In questa fase la stazione e l'Access Point effettuano uno scambio di informazioni in modo da verificare la relativa conoscenza di una data Password.
- Non appena le stazioni si sono autenticate inizia il processo di Associazione. In questa fase le informazioni scambiate hanno lo scopo di definire le caratteristiche della stazione e le capacità offerte dalla BSS. Tutto ciò consente al DSS, ovvero all'insieme degli AP, di ottenere informazioni circa l'attuale posizione della stazione espressa come appartenenza ad una particolare BSS ovvero come associazione ad un determinato Access Point.
- Osserviamo che una stazione è in grado di trasmettere o ricevere informazioni solo dopo che il processo di associazione si è positivamente concluso.

Roaming

- Il Roaming è il processo che consente lo spostamento di una stazione da una cella (o BSS) ad un'altra senza perdita di connessione. Questa funzione è simile a quella che viene realizzata nei sistemi di telefonia cellulare, con due differenze fondamentali:
  - § Su un sistema LAN basato su un sistema di trasmissione a pacchetti, la transizione da una cella ad un'altra deve essere realizzata tra la trasmissione di un pacchetto e quella del successivo, al contrario di quanto accade in un sistema per telefonia in cui il processo deve avvenire durante lo svolgimento di una comunicazione. In una LAN quindi il processo risulta sicuramente di più semplice implementazione.
  - § Su un sistema per il trasferimento della voce una temporanea disconnessione può non avere un effetto significativo, mentre in un ambiente basato sul pacchetto questa momentanea interruzione della connessione porta ad una significativa riduzione delle prestazioni, in quanto è necessario operare delle ritrasmissioni gestite però dai livelli superiori dello stack protocollare.