

# Riassunto RIM

## Introduzione

### Cosa è la rete

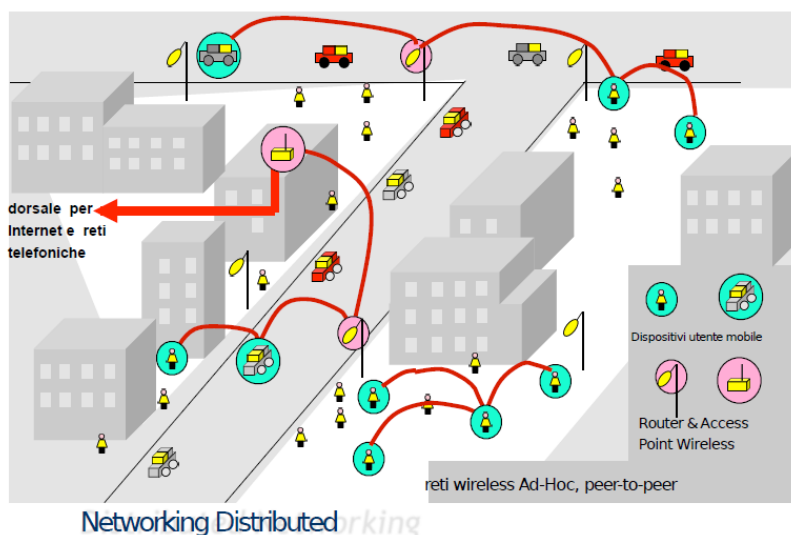
- Internet: milioni di computer collegati (Hosts). Le applicazioni sono in esecuzione sugli host, ed essi sono collegati con fibre, cavi, wireless o satelliti. Esistono altri dispositivi come i router che sono dispositivi di rete. Internet è un'infrastruttura di comunicazione che consente alle applicazioni di parlare e utilizza dei protocolli di comunicazione per inviare o ricevere messaggi. Ai bordi di internet possiamo trovare i terminali che eseguono il software applicativo secondo il paradigma client server o attraverso peer to peer. La rete fornisce un servizio di comunicazione per trasportare le informazioni tra processi remote e il trasferimento può essere di vari tipi. Posso essere usati messaggi brevi e poco affidabili o uno streaming affidabile di byte.
- Il core della rete è un insieme di router interconnessi e le informazioni sono trasferite con una comunicazione a commutazione di circuito (a ogni chiamata assegnato un circuito) o a commutazione di pacchetto (informazioni divise in messaggi).
- Nella commutazione di circuito le risorse di comunicazione sono riservate sulla base di una chiamata. In esse le risorse di rete sono divise in circuiti e ciascun circuito è assegnato staticamente alle comunicazioni. Il circuito rimane fermo se non usato (mancanza di condivisione). Vari tipi di commutazione:
  - \* A divisione di tempo
  - \* A divisione di frequenza
  - \* A divisione di codice
- Nella commutazione di pacchetto il flusso di dati è diviso in pacchetto e i pacchetti di diversi flussi condividono le risorse di rete. Ciascun pacchetto utilizza completamente il canale. Le risorse di rete sono utilizzate in base alle esigenze attuali. Avviene un conflitto di risorse:
  - \* Store and forward: ciascun pacchetto deve essere completamente ricevuto prima di avviare la trasmissione sul link di uscita
  - \* Multiplexing statici: esiste una coda dei pacchetti e si formano dei tempi di attesa per usare il link.

### Architettura internet e tecnologie di accesso

- L'architettura è formata da vari ISP (Internet Service Provider) che forniscono la connettività e utilizzano una dorsale comune secondo una gerarchia (ISP internazionale -> ISP nazionale ->...).
- La rete IP gestita da una sola organizzazione si chiama Autonomous System (AS). Il TCP/IP viene spesso utilizzato anche in reti private col nome di intranet. I router appartenenti ad un dato AS sono detti Interior Gateway (IG), mentre i router di collegamento tra AS differenti sono detti Exterior Gateway (EG).
- L'accesso a internet può avvenire per dial-up (accesso diretto al router IP attraverso PSTN) o tramite ADSL (Asymmetric Digital Subscriber Line) (in cui è presente un UTP condiviso con PSTN fino al primo punto di commutazione a divisione di frequenza. L'accesso ai router di ISP avviene attraverso la rete dati veloce). Da ADSL il router esterno permette l'accesso a internet alle reti locali (LAN) di collegamento tra terminali e router e con Ethernet interno alla rete. L'accesso a internet avviene anche grazie a accessi wireless (wireless LAN e sistemi cellulari come GSM, GPRS, EDGE, UMTS e LTE attraverso una base station o tramite access point).

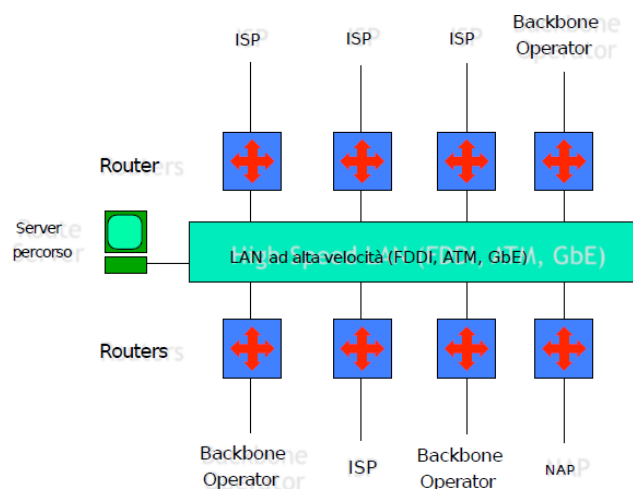
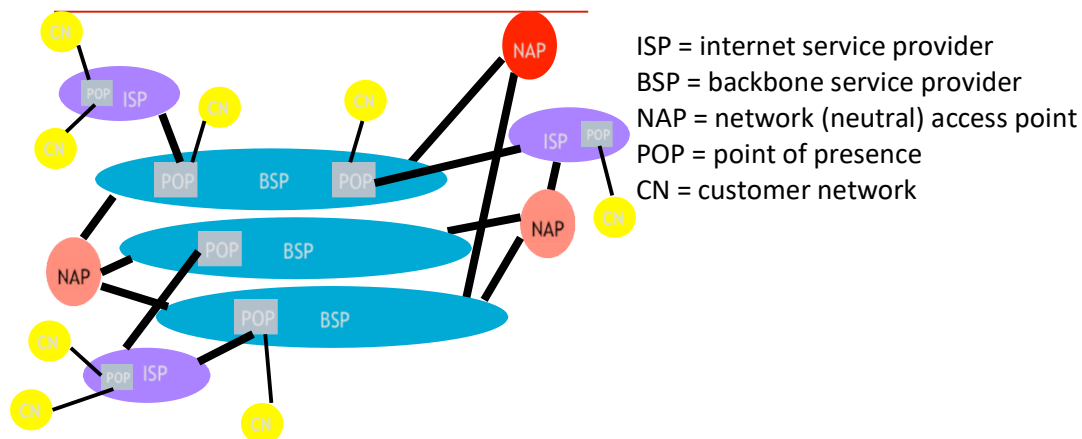
### Internet pervasiva

#### Mesh e reti ad hoc!



Il pervasive internet è una rete di sensori wireless: essi sono piccoli e leggeri nodi di rete a basso costo in grado di misurare, comunicare e attuare. Esempi di applicazioni di esse sono l'embedded computing, il wearable computing e l'intelligenza ambientale.

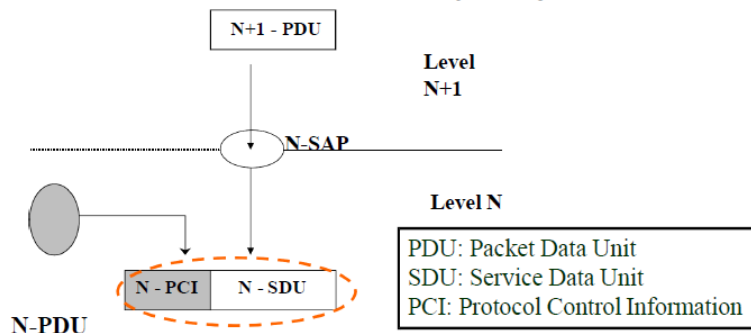
- La standardizzazione di internet avviene grazie a documenti pubblici chiamati RFC (Request For Comment) e l'ente che ne coordina la pubblicazione è l'Internet Engineering Task Force (IETF).
- L'architettura internet odierna è la seguente:



- Store & Forward:  $T_0$ =inizio trasm.,  $T_1$ = fine trasm.,  $T_2$ =arrivo primo bit,  $T_3$ =arrivo ultimo bit.  
 Tempo di trasmissione= $T=T_1-T_0=L/R$  con  $L$ =lunghezza pacchetto [bit] e  $R$ =rate trasmissivo [bit/s]  
 Tempo di propagazione= $\tau=T_2-T_0=l/C$  con  $l$ =lunghezza link [m] e  $C$ =velocità onda [m/s].
- Multiplexing statico: la trasmissione dei pacchetti non segue una sequenza fissa ma le risorse sono staticamente condivise.
- Ritardo di pacchetto (o nodale): è il ritardo sperimentato da ciascun pacchetto a causa di lavorazione, code, trasmissione e propagazione. Il nodo deve elaborare il pacchetto, verificando errori di bit e determinando il canale di uscita. Dopo deve mettere in coda il pacchetto (tempo di attesa al link di uscita per la trasmissione) (dipendenza dal livello di congestione del router). Il ritardo di trasmissione è il tempo per l'invio dei bit nel link (lunghezza del pacchetto[bit]/banda di collegamento [bps]), mentre il ritardo di propagazione è la lunghezza del collegamento fisico/velocità di propagazione.  
 L'intensità del traffico è data da (lunghezza del pacchetto[bit] \* tasso medio di arrivo dei pacchetti) / banda del collegamento [bps] e se è circa 0 abbiamo un piccolo ritardo di accodamento, mentre se tende a 1 il ritardo è quasi infinito.
- Può avvenire una perdita di pacchetti: la coda precedente al link nel frame ha una lunghezza finita. Quando il pacchetto arriva ad una coda piena, il pacchetto viene scartato, ma esso può essere ritrasmesso dal nodo precedente, dal sistema terminale sorgente, o non ritrasmesso affatto.
- La comunicazione di pacchetto, rispetto a quella di circuito, fornisce ritardi di trasferimento inferiore e supporta un maggior numero di utenti. Esso è molto semplice da implementare (meno sulla segnalazione) e molto adatto per il traffico a raffica (condivisione di risorse) ma sono necessari protocolli per il trasferimento di dati affidabili (controllo della congestione e recupero dei pacchetti persi).

## Fondamenti di protocolli e servizi di comunicazione

- Date due o più entità remote un servizio di comunicazione fornisce informazioni sul trasferimento di entità, gestisce lo scambio di informazioni fra esse e trasferisce informazioni in unità di parole, bit, frame o pacchetti, file etc. Un servizio di comunicazione potrebbe essere descritto attraverso chiamate di servizio denominate primitive. Esse possono essere utilizzate per descrivere il servizio, richiedere il servizio e raccogliere informazioni su di esso. Esse sono caratterizzate dal tipo di informazioni trasferite, l'indirizzo destinatario, le caratteristiche del servizio richiesto etc.
- Il tipo di comunicazione può essere orientato alla connessione (impostazione della connessione -> trasferimento dati -> rilascio della connessione) oppure senza connessione (modalità tutto in uno, asincrona). In questa seconda modalità si forma una mancanza di creazione di coordinamento tra le unità. Inoltre, le sessioni di trasferimento differenti tra le stesse entità non possono essere relazionate e si formano problemi nell'implementazione dei tipici servizi orientati alla connessione.
- Due entità allo stesso livello possono offrire un servizio di comunicazione a entità di livello superiore. Il servizio di comunicazione fornito allo strato superiore è "più ricco" grazie a specifiche funzioni attuate a livello inferiore.
- Le entità di pari livello cooperano per fornire alle entità di livello superiore una comunicazione di servizio e scambiano tra loro messaggi. Il set di regole che gestiscono la comunicazione tra entità dello stesso livello, come il formato del messaggio, le informazioni sul servizio, la procedura di trasferimento etc, è definito protocollo. L'unità di informazione utilizzata da un protocollo per entità di pari livello è detta Packet Data Unit (PDU) e potrebbe comprendere le informazioni di segnalazione (intestazione) e i dati ricevuti dal livello superiore (carico utile). I servizi di comunicazione complessi possono essere organizzati a livelli (a partire dal livello di movimentazione dei bit e arrivando a movimentazione di file e/o oggetti più complessi tramite protocolli). Le reti sono complesse: sono composte da vari pezzi come hosts, router, link di vari contenuti, applicazioni, protocolli e HW e SW. L'architettura a strati riduce la complessità, ha interfacce standardizzate, sfrutta la modularità e l'interoperabilità di Fosters con un insegnamento alleviato. Ne è un esempio il modello OSI. Il modello a livelli o strati è applicabile anche nella realtà e ciascun strato realizza un servizio attraverso delle azioni interne a esso e gli strati sopra si basano su quelli sotto. Stratificare serve a rapportarsi con sistemi complessi: una struttura esplicita consente l'identificazione e il rapporto tra pezzi complessi del sistema (stratificazione di un modello di riferimento) e la modularizzazione facilita la manutenzione e l'aggiornamento del sistema. Per la comunicazione tra livelli della stessa entità si fa uso di interfacce layer-to-layer in cui i servizi offerti da un determinato strato sono caratterizzati da un Service Access Point (SAP).



Il più basso livello è il fisico, dove la PDU (Phy-PDU) è fatta da flussi di bit. Le funzioni dei vari livelli possono essere divise in funzioni di adattamento (multiplexing e segmentazione) e di aumento (controllo errore e sequencing). Esistono poi funzioni di networking affinché una data entità possa comunicare con più entità di pari livello, ma si ha bisogno di funzionalità di routing (SAP scelta), di solito elaborato sulla base di un indirizzo. La PDU viene passata al livello inferiore con il parametro indirizzo, che si usa per instradare la PDU (scelta del SAP) e viene inserito nella PDU per un ulteriore instradamento. L'indirizzo è un identificativo SAP unico tra quelli di pari livello e può essere di tipo unicast (singolo SAP), multicast (gruppi di SAP) o broadcast (tutti i SAP). Una volta scelto il SAP la PDU deve essere inoltrata: la SAP è scelta sulla base della tabella di routing e avviene una raccolta di informazione attraverso i protocolli di routing.

## Canali e multiplexing

I canali possono essere di diversi tipi:

- I canali point-to-point sono connessioni permanenti tra un mittente e un ricevitore. Il ricevitore può essere progettato e ottimizzato sulla base del (unico) segnale che deve ricevere. La trasmissione dati può essere continua o divisa in frame (ciò solleva problemi di sincronizzazione).

- I canali broadcast sono canali in cui molte stazioni/nodi possono accedere ad un canale di trasmissione in parallelo e il canale è condiviso tra tutte le stazioni. Le trasmissioni di una stazione raggiungono tutte le altre stazioni. Il ricevitore può ricevere varie trasmissioni che differiscono nel loro livello di potenza e sincronizzazione, e deve essere in grado di adattarsi a tali differenze, trovando la giusta trasmissione. Le trasmissioni di solito iniziano con un preambolo (carattere di sincronizzazione) per ottenere la sincronizzazione.
- La capacità fisica di un canale può essere suddivisa per avere più (sotto)canali con velocità inferiore. Questo metodo è chiamato multiplexing. Nella moltiplicazione fisica ciascun (sotto)canale è definito esclusivamente in base a parametri fisici, come frequenza, tempo, codice, lunghezza d'onda etc.
- Nella moltiplicazione a divisione di frequenza (Frequency Division Multiplexing-FDM) ciascun canale fisico può essere caratterizzato dalla sua lunghezza di banda disponibile (l'insieme delle frequenze disponibili per la trasmissione ( $f_{\min}-f_{\max}$ )) e tale larghezza di banda può essere suddivisa in sottocanali e possiamo associare una comunicazione per ogni sottocanale. Il segnale relativo ad una comunicazione è filtrato e poi modulato (quindi spostato in frequenza) in modo da adattarsi esattamente al sottocanale. Il numero di sottocanali è  $n=B(\text{banda totale disponibile})/(b_s (\text{banda di segnale}) + b_g (\text{banda di guardia}))$ . In passato, FDM è stato usato come tecnica di multiplexing per trasmettere le chiamate vocali tra centrali telefoniche (con una larghezza di banda delle chiamate vocali di circa 4 kHz e una suddivisione di 12 canali su larghezza di banda totale di 48 kHz e questa aggregazione è stata ulteriormente ampliata in aggregazioni ancora maggiori (schema di modulazione gerarchico)).
- La modulazione a divisione di tempo (Time Division Multiplexing-TDM) è una tecnica utilizzata per i segnali digitali/binari. Dato un canale con velocità/capacità  $C$  [bit/s] definiamo intervalli di tempo (slot) la cui durata è un multiplo della durata  $t_b=1/C$  [bit]. Ogni sorgente/mittente può utilizzare solo un singolo slot di tempo ogni  $N$ . Definiamo una struttura del frame, in cui esso è costituito da  $N$  time slot consecutivi e se diamo un numero a ogni slot, ogni sorgente è associato a un numero di slot e può trasmettere solo dentro tale slot. La capacità/velocità di ogni sottocanale è  $c=C/N$ , mentre la durata di slot è  $T_i=n_i/C$  e la durata del frame è  $N \cdot n_i/C$ . La scelta della durata dello slot è molto importante (parametro scelto durante la progettazione del sistema). Avendo il numero di bit per slot  $n_i$  e la durata dello slot  $T_i$ , la capacità del sottocanale  $c$  non dipende da  $T_i$  ma solo da  $N$ . Il tempo per raccogliere  $n_i$  bit è  $T_a=n_i/c$ . Ogni sorgente/ mittente produce bit esattamente con velocità  $c$ . Gli  $n_i$  bit che sono nello slot devono essere già pronti quando lo slot inizia. Chiaramente, alla sorgente servono  $n_i/c$  secondi per produrre e accumulare gli  $n_i$  bit.  
Se in ogni sottocanale è assegnato un singolo slot per frame, tutte le velocità di trasmissione sono uguali ma in molti casi è necessario multiplexare i flussi con velocità diverse. A questo scopo è possibile usare frame più complessi in cui ad un canale può essere assegnato più di uno slot. Per semplicità la suddivisione è solitamente ottenuta usando una gerarchia di frame, con frame e superframe. Questa metodologia è usata anche per TDMA.
- La tecnica CMD (Code Division Multiplexing) consiste nel miscelare (cioè aggiungere)  $N$  flussi di bit ( $N$  trasmissioni), dopo aver moltiplicato ciascuno di essi per una codeword  $C_i$  scelta tra le  $N$  codewords di un codice ortogonale. Le codewords sono costituite da  $N$  simboli binari, detti chips (al fine di poterli distinguere dai bit) la cui durata è  $N$  volte più corta.

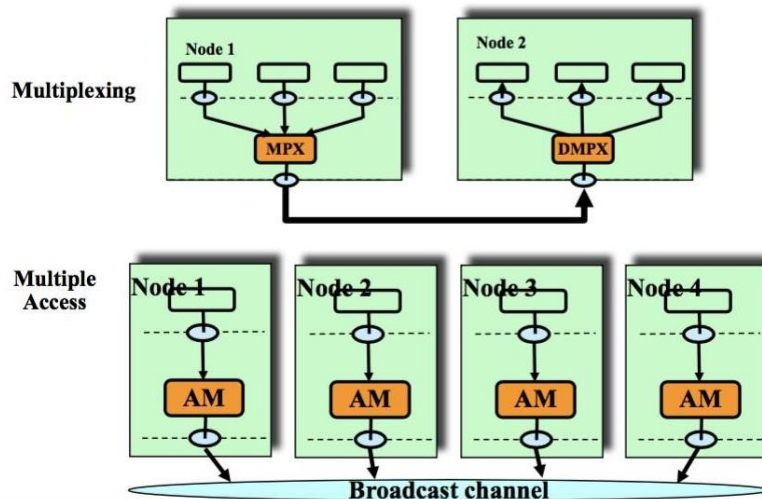
I segnali ortogonali sono  $\int s_1(t) \cdot s_2(t) dt = 0$ , mentre le sequenze ortogonali sono

$$\begin{array}{l}
 C_1(t) \rightarrow \int_0^T C_1(t) \cdot C_2(t) dt = 0 \\
 C_2(t) \rightarrow \sum_{i=1}^N c_{1i} \cdot c_{2i} = 0
 \end{array}$$

Si utilizzano inoltre le matrici di Hadamard. Sul ricevente si può estrarre il  $k$ -esimo segnale semplicemente moltiplicandolo per  $C_k$ :  $\int_T (\sum_{i=0}^{N-1} s_i C_i) \cdot C_k = s_k$ . Esiste inoltre, nella tecnica CDMA, una diffusione e una de-diffusione: il codice "espande" la larghezza di banda radio del segnale attraverso un fattore di spreading (SF-Spreading Factor) ( $n$ ). Diversi segnali usano la stessa banda di segnale e al ricevimento il segnale viene moltiplicato per il codice (de-diffusione) e l'interferenza degli altri segnali è ridotta di  $1/n$ .

- Il WDM (Wavelength Division Multiplexing) è lo stesso di FDM (per ragioni storiche relative allo sviluppo delle fibre ottiche). In esso diversi segnali sono modulati utilizzando diverse lunghezze d'onda su fibre ottiche e ogni lunghezza d'onda può trasportare enormi quantità di informazioni, ma è presente un limite tecnologico dovuto alla stabilità del led/laser utilizzato per modulare i segnali e alla precisione dei filtri ottici.

- L'accesso multiplo è simile al multiplexing ma è concettualmente molto diverso. Infatti, l'accesso multiplo è legato ai canali trasmessi. Quindi le stazioni/nodi che accedono al canale trasmissivo sono distanti e fisicamente in luoghi diversi (molto distanti tra loro) e devono quindi coordinarsi tra loro per accedere al canale senza collidere.

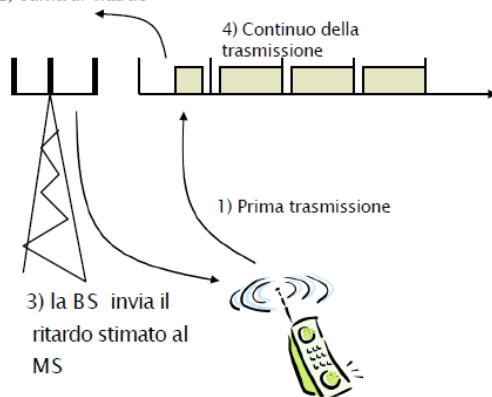


FDMA (Frequency Division Multiple Access) è analogo a FDM: diverse stazioni/nodi devono coordinarsi per accedere al canale, ma questo non è un problema per FDMA. Esempi di FDMA sono TV o stazioni radio e sistema cellulare TACS.

TDMA (Time Division Multiple Access) è simile a TDM ma in questo è necessario che le stazioni si coordinino tra loro per trovare un riferimento temporale comune (necessario sapere gli slot/fotogrammi di inizio e fine). La sincronizzazione non può essere perfetta: dei tempi di guardia sono necessari per evitare sovrapposizioni. In CDMA è impossibile avere la perfetta sincronia tra le diverse trasmissioni dei nodi: si perdono i codici di ortogonalità e quindi si è costretti a usare codici con bassissima correlazione per ogni possibile spostamento temporale  $\Delta$ . Questo sistema è usato nei sistemi di 3° generazione come UMTS.

- Il canale di trasmissione può essere un canale broadcast centralizzato oppure distribuito. Nel primo il punto di accesso è fisso (come nei sistemi cellulari, nelle WLAN e WMAN). Nella copertura cellulare la copertura del territorio è ottenuta dalle stazioni base BS (o AP-access point) che forniscono l'accesso alle stazioni radio mobili (MS) all'interno di un'area di servizio denominata CELL. Il canale trasmissivo distribuito è tipico delle reti wireless ad hoc (come le reti mesh o di sensori). Nel funzionamento multi-hop le stazioni mobili possono inoltrare le informazioni ad altre stazioni mobili.
- Le differenze principali tra le reti cablate e quelle wireless sono il mezzo di trasmissione: nelle reti wireless il mezzo è condiviso e si usano meccanismi di accesso multiplo e avviene un riutilizzo della risorsa radio. Il canale radio ha inoltre delle caratteristiche del canale variabili e si utilizza una modulazione avanzata e vari schemi di codifica.
- Nel canale centralizzato la stazione base è fondamentale per far rispettare la sincronizzazione tra i terminali mobili e le sue trasmissioni sono utilizzate per sincronizzare tutte le trasmissioni (ad esempio l'invio di un segnale per l'inizio del frame). L'inizio della trasmissione avviene dopo  $2\tau$ , con  $\tau$ =ritardo di propagazione=distanza delle stazioni/velocità della luce nel mezzo. Il massimo tempo di  $2\tau$  tra due delle stazioni è detto tempo di guardia (che viene adottato nel frame di tutte le trasmissioni) ed è dominato dal più lontano nodo dalla BS. Si sviluppa un meccanismo di Timing Advance: se ogni nodo conosce il ritardo di propagazione verso la BS, si può prevedere la trasmissione. Il ritardo di propagazione  $\tau$  deve essere stimato (può variare nel tempo) e un errore di stima è ancora possibile: il tempo di guardia è ridotto, ma non è nullo.

2) stima di ritardo





La tecnica di cui sopra è utilizzata nel GSM, che è stato progettato per celle con un raggio di massimo 37.8km. il tempo di guardia è quindi 233 m\*s che è equivalente a 68.25 bit su una velocità di 270.8 kbit/s.

$$\eta = \frac{T_i}{T_i + T_g} = \frac{1}{1 + \frac{T_g}{T_i}} = \frac{1}{1 + T_g \frac{C}{n_i}}$$

Si può calcolare l'efficienza  $\eta$  come quando aumentano le distanze dalla BS (aumento di  $T_g$ ), quando aumenta la velocità di canale o quando la durata della fessura diminuisce.

- Il problema di accesso radio è legato al modo in cui gli utenti delle risorse radio condividono le celle. Quindi in downlink (da BS a MS) si utilizza la moltiplicazione, mentre in uplink (da MS a BS) si utilizza l'accesso multiplo. Le frequenze disponibili non sono sufficienti per tutti gli utenti: una soluzione è data dal riutilizzo della stessa frequenza in celle diverse (riuso spaziale) che tuttavia causa interferenze di co-canale. Il riuso spaziale è reso possibile se le celle sono sufficientemente distanziate tra loro in modo tale che l'interferenza sia piccola/tollerabile (al fine di garantire una buona qualità del segnale trasmesso). L'interferenza è quindi una caratteristica fondamentale, intrinseca dei sistemi cellulari. si assume di solito che la qualità del sistema sia buona quando il rapporto tra la potenza del segnale e la potenza di interferenza, di nome SIR (Signal-to-Ratio Interference) è superiore a una soglia predefinita  $SIR_{min}$ . tradizionalmente, per descrivere in maniera semplificata la struttura dei sistemi cellulari, la forma delle celle è raffigurata come esagonale. A causa delle posizioni delle stazioni base e della propagazione non uniforme dei segnali dovuta a ostacoli, la forma delle celle è solitamente diversa. L'uso della forma esagonale regolare è comunque un buon approccio per fare un dimensionamento di massima del sistema e serve per comprendere i principi fondamentali del riuso.

Il dimensionamento esagonale è detto a cluster: in esso tutte le frequenze disponibili sono divise in K gruppi e assegniamo un gruppo per ogni cella al fine di massimizzare la distanza tra due celle che utilizzano lo stesso gruppo di frequenze. L'efficienza del riuso della frequenza sarà di  $1/K$ . K ha possibili valori 1,3,4,7,9,12,13....

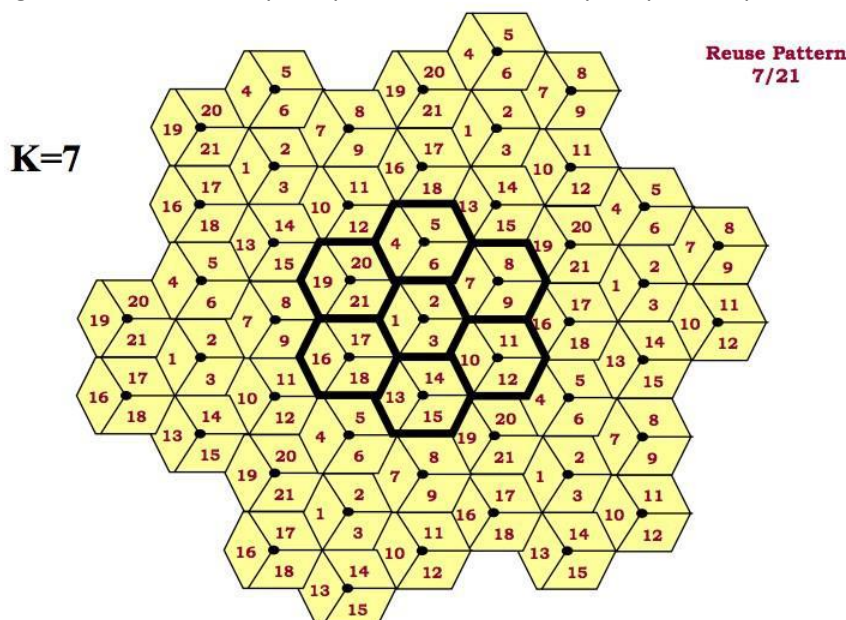
Se sappiamo o impostiamo il  $SIR_{min}$  come valore tollerato dal sistema, allora possiamo stimare la massima efficienza del sistema, ovvero il minimo K che deve essere usato. Consideriamo la potenza ricevuta come  $P_r = P_t * G * d^{-\eta}$ , con G numero antenne e d distanza tra due stazioni. Se ipotizziamo le stesse antenne (G) e la stessa  $P_t$  (potenza trasmissiva) avremo un  $SIR = \frac{d^{-n}}{\sum_{i=1}^{N-1} d_i^{-n}}$  e ci poniamo nel caso peggiore in cui  $d=r$ (raggio) e

approssimiamo  $d_i=D$  (distanza centri degli esagoni) avremo un SIR di circa  $(1/(N-1)) * (1/R)^{-\eta}$ , con  $R$ =rapporto di utilizzo= $D/r$ (raggio esagono). Il SIR dipende esclusivamente da R e da  $\eta$ , ma non dalla potenza trasmissiva assoluta o dalla dimensione delle celle. Se fissiamo  $SIR_{min}$  possiamo calcolare  $R_{min}$  e se  $R_{min}$  è noto, possiamo ottenere K poiché  $K=R^2/3$  ( $R=\sqrt{3K}$ ) e quindi  $K_{min}=((N-1)*SIR_{min})^{2/\eta}/3$ .

Ricordiamo che nel modello appena visto di cluster abbiamo fatto varie ipotesi semplificatrici (distanze, solo il primo anello di interferenti, nessun rumore termico e propagazione con solo perdita di percorso).

L'obiettivo del dimensionamento è quello di garantire una buona SIR a tutti gli utenti e dobbiamo considerare i casi più critici. Per includere una dissolvenza veloce e lo shadowing possiamo considerare un margine su  $SIR_{min}$  (come fatto nel dimensionamento delle celle).

Nei sistemi cellulari reali le antenne sono settoriali e si fa uso di antenne direttive che permette di modificare il layout cellulare e ridurre le interferenze ricevute. Nei sistemi cellulari le antenne direttive con angolo di 120° del lobo principale sono comuni. Si può quindi replicare il riuso spaziale nei settori:



Per il SIR riutilizziamo la stessa formula  $SIR \cong \frac{r^{-\eta}}{6D^{-\eta}} = \frac{1}{6} \left( \frac{1}{R} \right)^{-\eta}$ , con una piccola modifica dove M è il numero di interferenze (primo anello) visibile da un singolo settore (M=6/#settori) e quindi  $K_{min}$  è uguale a  $\frac{(M \cdot SIR)^{2/\eta}}{3}$ .

Una volta selezionata la dimensione del cluster, l'assegnazione dei canali alle celle è solitamente soggetta a vincoli aggiuntivi. Le frequenze adiacenti hanno spesso uno spettro leggermente sovrapposto e possono generare quindi mutue interferenze (interferenza del canale adiacente). Ma il problema può essere più complesso a causa di settori che solitamente hanno lobi secondari nel diagramma dell'antenna che generano interferenze nelle celle vicine. Quindi non è possibile, di solito, assegnare frequenze adiacenti a celle dello stesso sito.

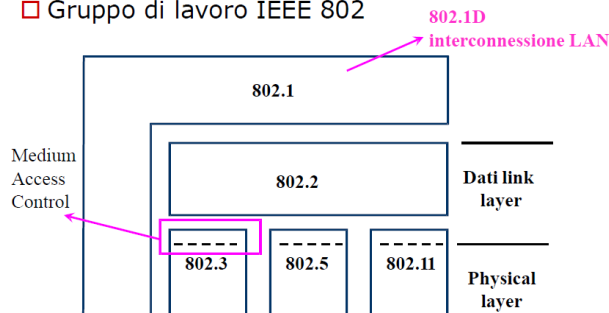
Una osservazione importante è che la formula semplificata per il dimensionamento del cluster non dipende dal raggio della cella ma solo dai rapporti di distanza. Variando il raggio della cella possiamo variare il numero di canali disponibili per unità di superficie e questo ci dà libertà di pianificare il layout cellulare (dimensioni delle celle) in base alla densità del traffico stimata in diverse aree.

- Ricordiamo che le potenze in dB sono rappresentate in scala logaritmica, quindi  $P_{dB} = 10 \log_{10} P$  e  $P = 10^{P_{dB}/10}$ . Inoltre, il prodotto in scala lineare corrisponde ad una somma utilizzando i dB e il rapporto corrisponde a una differenza in dB.

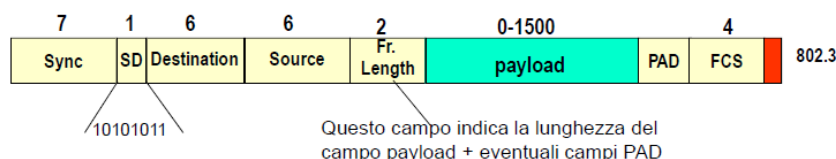
## Tecnologie di accesso

- La prima lan Ethernet aveva una capacità del Bus Broadcast di 10 Mb/s ed è stato standardizzato all'inizio degli anni 80 come IEEE 802.3, con grande successo e parecchie estensioni.

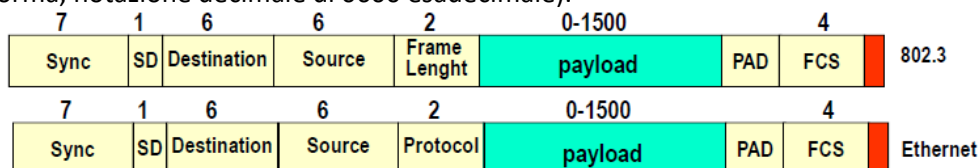
□ Gruppo di lavoro IEEE 802



La topologia storica di rete è stata la topologia a bus, mentre si è poi sviluppata la topologia a stella, in cui lo switch è come un repeater: ogni qualvolta un frame è ricevuto da una stazione, viene trasmesso in direzione di tutte le altre stazioni. La frame Ethernet ha una lunghezza minima di 512 bit (1 slot) che equivalgono a 51,2 us. Si propaga con una velocità di  $2 \cdot 10^8$  m/s e il massimo diametro della lan è di 2.5 km.



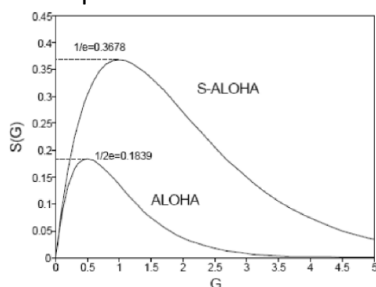
Analizziamo che 802.3 e Ethernet non sono lo stesso protocollo: 802.3 (MAC) ha un livello LLC (802.2) mentre ethernet è direttamente collegato al livello rete. Inoltre in Ethernet il campo protocollo è usato per identificare il network SAP. È anche vero che in molte LAN Ethernet e 802.3 coesistono: il campo frame length può essere nel range 0-1500 e il campo protocol è maggiore di 1500 (precisamente >1536 per la norma, notazione decimale di 0600 esadecimale).



Nota: in quest'ultimo caso, lo standard MAC dice che è il protocollo client MAC (ad esempio, IP o il livello superiore che utilizza Ethernet) che devono funzionare correttamente nel caso in cui l'imbottigliamento viene introdotto al livello MAC (in altre parole, il corretto funzionamento è demandato allo strato superiore)

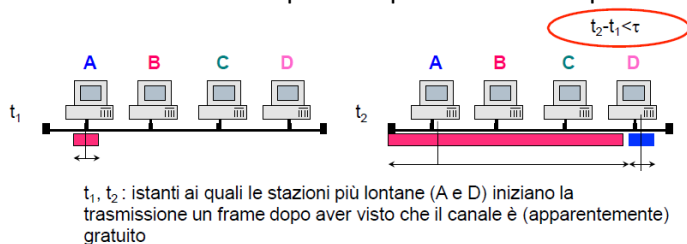
- Se due o più stazioni cercano di trasmettere allo stesso tempo, si ha una collisione => il segnale (o il frame) non viene ricevuto correttamente. Abbiamo bisogno di protocolli (regole) per controllare l'accesso al mezzo broadcast, per evitare (o almeno, limitare) le collisioni. Se si verifica una collisione, essa deve essere correttamente individuata da tutte le stazioni per reinviare nuovamente il frame colliso. Questa funzione è eseguita in Ethernet dal sottolivello MAC (Medium Access Control).

- Nel modello concettuale di accesso multiplo il Master non sa se e quanti pacchetti sono presenti in ciascuna coda (cioè, se e quanti pacchetti sono prodotti da ciascuna stazione). Ogni stazione non conosce lo stato delle code delle altre stazioni.  
Esistono due tipi di tecniche di accesso multiplo: l'accesso ordinato (TDMA, Round Robin, Polling (Roll Call e Hub)) oppure l'accesso casuale (CSMA/CD per ethernet e CSMA/CA per 802.11/Wi-Fi). Prendendo come esempio TDMA, nella LAN il traffico risulta intenso e abbiamo diverse stazioni. Quindi TDMA è inefficiente: ha elevati ritardi e basso throughput. In RR ogni stazione ha, in ogni turno, l'opportunità di trasmettere. Quando arriva il suo turno se non ha pacchetti da trasmettere rifiuta l'opportunità di trasmissione e la cede alla successiva, mentre se ha da trasmettere, trasmette i suoi pacchetti fino a un numero massimo  $K$  definito dal protocollo stesso. Infine, la possibilità di trasmissione è inviata alla successiva stazione. Nel Roll Call polling il token (pacchetto di controllo che garantisce l'opportunità di trasmissione) è sempre rimandato alla stazione Master. Nell' Hub Polling il token torna al Master solo alla fine del ciclo.
- I protocolli ad accesso casuale non hanno un coordinamento esplicito tra le stazioni quindi si possono verificare collisioni. Essi differiscono in come essi risolvono le collisioni e anche nella risposta dal canale (cioè l'informazione che deriva dall'ascolto del canale). Le collisioni sono superate con l'introduzione di un meccanismo casuale. Ad esempio, nello Slotted Aloha il canale è slotted (il tempo è diviso in slot) e quando un pacchetto arriva alla stazione, essa cerca di inviarlo nel primo slot disponibile. Se si verifica una collisione, la stazione tenta di inviare nuovamente il frame dopo un numero casuale di slot, dove il numero casuale è scelto in modo uniformemente casuale in un intervallo  $[0, r]$ . Se  $r=0$  la collisione si verifica infinite volte e il throughput è uguale a 0. Se il traffico offerto è alto, abbiamo bisogno di un alto valore di  $r$  per evitare instabilità. Riassumendo vorremmo avere un piccolo valore di  $r$  quando la rete è vuota e grandi valori di  $r$  quando la rete è congestionata. In Aloha il meccanismo di accesso è molto semplice: quando c'è un pacchetto da trasmettere lo trasmetti e, se la trasmissione non riesce, aspetta un tempo casuale e ritrasmetti. Assumendo che il tempo di inizio trasmissione sul canale sia un processo poissoniano con ritmo  $\lambda$  e consideriamo  $G=\lambda T$  il ritmo normalizzato. La probabilità di successo è data dalla probabilità che non ci siano altre trasmissioni nell'intervallo  $2T$ , quindi  $P_s=e^{-2G}$  e il throughput normalizzato  $S$  è quindi dato da  $S=Ge^{-2G}$ . Se la trasmissione è in qualche modo sincronizzata (slotted aloha) il periodo di vulnerabilità si riduce di  $T$  e quindi  $S=Ge^{-G}$ .



Purtroppo, il traffico sul canale è la combinazione di nuove trasmissioni e ritrasmissioni, ed esso può aumentare se il throughput si riduce. Per valutare il comportamento dinamico di Aloha è necessario prendere in considerazione maggiori modelli.

- CSMA (Carrier Sense Multiple Access) è stato creato per sistemi in cui la stazione può sentire il canale (carrier sense). La trasmissione è possibile solo se il canale è liberamente sensato (listening before talking) e le collisioni sono ancora possibili per il cosiddetto periodo di vulnerabilità.



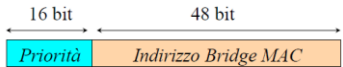
Il periodo vulnerabile è quindi di  $2\tau$  con  $\tau$  tempo di propagazione fra le due stazioni più lontane. La durata  $T$  della trama deve essere maggiore di  $2\tau$ .

In alcuni canali (come quelli cablati) è possibile per una stazione scoprire se si è verificata una collisione. Il tempo necessario che ci mettono tutte le stazioni per vedere che una collisione accada veramente dipende sul tempo di propagazione (che è inferiore al tempo di trasmissione dei frame in LAN). Ogni volta che la stazione conosce il verificarsi della collisione, essa arresta immediatamente l'invio del resto della frame => CSMA/CD. In CSMA/CD se il canale è libero, la trasmissione è eseguita e se il canale è occupato, la trasmissione viene fermata e avviene solo quando il canale ritorna libero. Se accade una collisione la



trasmissione viene interrotta dopo la trasmissione di 32 bit chiamata sequenza di jamming. Dopo una collisione, la prossima trasmissione è tentata dopo X time slot, dove X è scelta casualmente tra 0 e  $2^{\min(K,10)}$ K numeri di collisioni consecutive con  $K \leq 16$  (exponential binary backoff). Dopo 16 mancati tentativi il frame è buttato.

- Un problema rilevante nelle reti è che le topologie LAN sono di solito mischiate per tolleranza ai guasti. Bridging e Backward Learning lavorano su una topologia ad albero e Broadcast Storm avviene a causa dei cicli nel grafo topologico. Per evitare questo problema bisogna ottenere una topologia ad albero logico da uno a maglia fisica. La topologia ad albero è ottenuta bloccando alcune porte e una porta bloccata filtra i frame di dati e rilascia i frame di controllo (spanning tree). Lo spanning tree protocol funziona in questo modo: viene eletto un bridge root e ogni bridge individua la root port (individua la porta con la distanza minore dal root bridge). In ciascuna LAN un bridge designato viene scelto e la porta che interconnette il bridge designato con la sua LAN è chiamata designed port. La root port e le designed port sono attive, le altre sono messe in blocco. La topologia risultante è uno spanning tree. Per scegliere il root bridge ci si basa

sul Bridge ID (64 bit) . Il bridge con il minimo Bridge ID è il root bridge. Una volta che il root bridge viene eletto, ogni bridge seleziona la root port (seleziona la porta con distanza minore per la root bridge, in cui la distanza è espressa come un costo attraverso il parametro Root Path Cost che corrisponde spesso al numero di salti). Viene eletto un Designed Bridge per ogni segmento LAN. Esso porta i frame attraverso il Root Bridge. (tutte le porte di un root bridge sono designed bridge port).

### Gestione indirizzi in reti IP

- Le tabelle di inoltra (IP/indirizzo fisico) sono create e gestite in modo dinamico dagli hosts attraverso l'ARP (Address Resolution Protocol). Questo protocollo è basato sulla capacità di indirizzamento broadcast della sottostante tecnologia. Ogni volta che l'indirizzo MAC destinatario non è nella ARP-cache viene generato un messaggio ARP-request. Gli ARP-request sono inviati in broadcast (fisico) con l'indicazione dell'IP da risolvere. L'host che riconosce il proprio IP invia una ARP-reply in unicast (fisico) alla stazione indagatrice. Così come ARP, esiste anche il suo duale RARP (Reverse ARP) che assegna un indirizzo IP a un indirizzo MAC conosciuto. È utile per le macchine senza disco che devono effettuare un bootstrap di rete. È un protocollo scarsamente utilizzato.
- Le procedure statiche di assegnazione di un indirizzo IP hanno una flessibilità bassa. L'uso di un server centrale che memorizza la configurazione degli host può aiutare. In molti casi un accoppiamento statico tra indirizzi IP e MAC non è necessario (più host che IP disponibili). Assumendo di avere un server che gestisca le assegnazioni degli indirizzi IP su richiesta. Esistono diverse soluzioni fattibili: il Binding statico (il server tratta una tabella di corrispondenze statiche tra indirizzi IP e MAC) o il Binding dinamico (gli indirizzi IP impostati potrebbero essere meno rispetto a quelli che servono agli host- il binding cambia nel tempo). Quest'ultimo è utile se l'host ha vari cicli di attività. Il binding deve essere temporaneo e usato da timeout and/or e procedure esplicite di pubblicazione. La probabilità di rifiuto è non nulla e il problema di dimensionamento degli IP è simile a quello del dimensionamento dei circuiti telefonici.
- Una versione evoluta del BOOTP è il DHCP (Dynamic Host Configuration Protocol), che è un protocollo di livello applicativo basato sul paradigma client-server. In esso il client invia un messaggio DHCP Discover in broadcast IP contenente il proprio MAC e un ID sessione. Il server risponde con un DHCP Offer contenente l'IP proposto con la netmask, il tempo di affitto dell'IP e l'ID di sessione. Il client può accettare la proposta con un DHCP Request con ID sessione e parametri proposti e quindi il server lega i due indirizzi e risponde con un DHCP Ack confermando la configurazione. I parametri di configurazione sono l'indirizzo IP, la netmask, la porta e il server DNS. Il binding viene rotto con un messaggio DHCP Release da parte del client. Nelle reti reali abbiamo architetture multi-server e si fa uso di DHCP Relay. DHCP utilizza UDP come trasporto e durante la fase di costruzione (fino alla creazione del binding) i messaggi del client hanno IP mittente 0.0.0.0, IP destinatario 255.255.255.255, porta origine 68 e porta destinataria 67.

### Instradamento Unicast dei pacchetti

- Le funzionalità di routing sono fondamentali per la comunicazione di rete. Nelle reti TCP/IP il routing permette la comunicazione tra due nodi A e B non direttamente connessi. Le entità di livello 3 instradano i pacchetti (scelta del SAP di uscita) in base all'indirizzo destinatario. La corrispondenza SAP di uscita-indirizzo di destinazione è immagazzinata nella tabella di routing. Il protocollo di routing comprende due funzionalità: scambio di informazioni sulla topologia di rete, traffico e creazione e manutenzione della tabella di routing. La prima funzionalità è formalmente il protocollo di instradamento e nella pratica le due funzioni sono fasi unite. Il metodo con cui le tabelle di routing sono create dipende dai messaggi di routing scambiati e viceversa. Un algoritmo di routing definisce i criteri di come scegliere il cammino tra sorgente e destinazione e costruisce le tabelle di instradamento. Il criterio scelto dipende dal tipo di rete (datagram, circuito

virtuale,...). Nelle reti broadcast non c'è necessità di routing. Così il massimo traffico supportato dipende dalla capacità del canale. Nelle reti IP mischiate, i collegamenti multipli possono essere usati nello stesso momento ed essi hanno un impatto profondo sulla capacità della rete. Può esistere una pianificazione muta di routing dove sia la capacità di collegamento che il massimo traffico sono C o una pianificazione saggia di routing con capacità di collegamento C e traffico massimo 3C.

- Il tipo di invio impatta sulla politica di instradamento. L'invio IP è basato sulla destinazione e sul prossimo salto. Come conseguenza abbiamo che tutti i pacchetti destinati a D e arrivati al router R seguono lo stesso percorso dopo R. si creano quindi dei vincoli sul percorso: tutti i percorsi da tutte le sorgenti indirizzati alla destinazione D devono formare un albero, per ogni D, e le coppie sorgente-destinazione non possono essere instradate indipendentemente dalle altre coppie. Nel routing TCP/IP è scelto il percorso più breve per una destinazione. Il calcolo di esso è eseguito sul grafo che rappresenta la rete (dispositivo=vertice, collegamento=filo e peso\_filo=metriche). Le proprietà del percorso minimo sono che tutti i percorsi per una destinazione formano un albero e si usino facili e semplici algoritmi (complessità polinomiale, anche distribuiti).

### Algoritmi di routing

- Un grafo (o digrafo)  $G(N,A)$  ha N nodi e  $A=\{(i,j), i \in N, j \in N\}$  bordi (coppie ordinate di nodi).
- Un percorso  $(n_1, n_2, \dots, n_l)$  è un set di nodi con  $(n_i, n_{i+1}) \in A$ , senza ripetizioni di nodi.
- Un ciclo è un percorso con  $n_1 = n_l$ .
- In un digrafo connesso per ogni coppia i e j esiste almeno un percorso da i a j.
- Il digrafo pesato è un digrafo in cui assegno  $d_{ij}$  pesi al filo  $(i,j) \in A$ .
- La lunghezza del percorso  $(n_1, n_2, \dots, n_l)$  è  $d_{n_1, n_2} + d_{n_2, n_3} + \dots + d_{n_{l-1}, n_l}$ .
- Dato  $G(N,A)$  e due nodi i e j, la scoperta del sentiero con la lunghezza minima ha complessità polinomiale nel numero di nodi. Ricordiamo la seguente proprietà: se il nodo k è attraversato dal percorso più breve da i a j, anche il percorso da i a k è il più breve.
- Se assumiamo dei pesi positivi o negativi e che non ci siano cicli negativi, l'algoritmo di Bellman-Ford si pone come obiettivi quelli di trovare i percorsi minimi da una fonte a tutti gli altri nodi e di trovare i cammini minimi da tutti i nodi a una destinazione. Poniamo la variabile  $D_i^{(h)}$  come lunghezza del percorso più breve dalla fonte (ipotesi: nodo 1) al nodo i con un numero di salti  $\leq h$ . L'algoritmo inizia con  $D_1^{(h)} = 0 \forall h$  e  $D_i^{(0)} = \infty$

$\forall i \neq 1$ . L'iterazione dell'algoritmo è 
$$D_i^{(h+1)} = \min \left[ D_i^{(h)}, \min_j (D_j^{(h)} + d_{ji}) \right]$$
 L'algoritmo si arresta dopo N-1 iterazioni.

Si può dimostrare che l'algoritmo converge in un numero finito di iterazioni, anche nella forma distribuita. I nodi periodicamente inviano la loro stima del percorso più breve e aggiornano tale valutazione secondo la

regola 
$$D_i := \min \left[ D_i, \min_j (D_j + d_{ji}) \right]$$
. Nella pratica ad ogni nodo è assegnato un'etichetta (n,L) con n=prossimo salto sul percorso e L=lunghezza del sentiero. Ogni nodo aggiorna la sua etichetta guardando le etichette dei vicini. Quando le etichette non cambiano per molto tempo il cammino minimo può essere costruito.

- Se ipotizziamo solo collegamenti pesati positivi possiamo utilizzare l'algoritmo di Dijkstra, che si pone l'obiettivo di trovare il percorso minore tra un nodo sorgente (1) e tutti gli altri nodi. Inizia con  $P=\{1\}$  e  $D_1=0$ ,  $D_j^{(0)}=d_{1j} \forall j \neq 1$  e  $d_{ij}=\infty$  se il lato i-j non esiste. L'iterazione è formata da:

1. Trova  $i \in (N-P)$ :

$$D_i = \min_{j \in (N-P)} D_j$$

e imposta

$$P = P \cup \{i\}. \text{ Se } P = N, \text{ allora STOP.}$$

2. Per ogni  $j \in (N-P)$  vicino di ogni nodo in P imposta:

$$D_j = \min \left[ D_j, \min_k (D_k + d_{kj}) \right]$$

3. Vai a 1.

Nella pratica si usano gli stessi criteri di etichetta di Bellman-Ford e l'etichetta può essere temporanea o permanente. All'inizio, l'unica etichetta permanente è quella della fonte e, ad ogni iterazione, l'etichetta temporanea con il più basso costo del percorso è resa permanente.

- A livello di complessità Bellman-Ford ha N-1 iterazioni, N-1 nodi da controllare per ogni iterazione e N-1 confronti per nodo. Quindi la complessità è  $O(N^3)$ . Dijkstra ha N-1 iterazioni e N operazioni in media per iterazione. Quindi la complessità è  $O(N^2)$ . Dijkstra è generalmente più conveniente.
- Il routing IP invia pacchetti sul percorso più breve per la destinazione. La lunghezza del percorso è misurata secondo delle metriche date. Il più breve percorso calcolato è implementato in via distribuita attraverso un

protocollo di instradamento. Nella tabella di routing, solo il prossimo salto viene memorizzato, grazie alla proprietà che i sottopercorsi di un percorso sono a loro volta i minimi.

I protocolli di routing servono per gestire lo scambio di messaggi tra i router per calcolare i percorsi per una destinazione. Ne esistono due classi: DV (Distance Vector come RIP o IGRP) e LS (Link State come OSPF e IS-IS). Le differenze stanno nel tipo di metriche, nel tipo di messaggi scambiati e nel tipo di procedure utilizzate per lo scambio di messaggi.

### Protocolli di routing Distance Vector

- Nei protocolli di routing DV i router si scambiano informazioni sulle specifiche di connettività: i Distance Vector (che sono composti da [indirizzo di destinazione, distanza]). DV è inviato solo ai router direttamente connessi, è inviato periodicamente e/o ogni volta che avvengono modifiche alla topologia di rete e la stima della distanza è eseguita utilizzando Bellman-Ford.

Alla ricezione del DV:

1. Aumenta la distanza dalla destinazione specificata del costo sul collegamento corrente.
2. Per ogni destinazione specificata se la destinazione non è nella tabella di routing inserisci la destinazione/distanza, mentre se il prossimo salto nella tabella di routing è il DV mittente aggiorna le informazioni memorizzate con quelle nuove, sennò se la distanza memorizzata dalla destinazione è maggiore di quella specificata nel DV aggiorna le informazioni memorizzate con le nuove.

Il DV è inviato periodicamente e ogni volta che qualcosa cambia con la ricezione di un altro DV. I router calcolano le distanze se è ricevuto un nuovo DV o qualcosa cambia nella topologia della rete locale (caduta del collegamento).

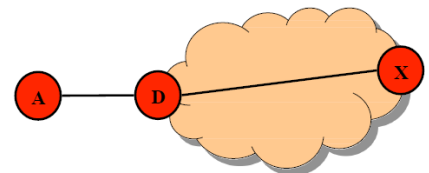
Un pro del DV è che è molto facile, ma per contro c'è un alto tempo di convergenza, è limitato dai nodi minori, ci sono possibili cicli e diventa instabile nelle grandi reti (counting to infinity). Il tempo di convergenza cresce proporzionalmente col numero di nodi (bassa scalabilità).

Un rimedio al counting to infinity è limitare il conteggio dei salti: il conteggio a infinito è rotto se l'infinito è rappresentato da un valore finito. Tale valore deve essere maggiore della lunghezza del percorso più lungo nella rete. Quando una qualsiasi distanza raggiunge tale valore il nodo corrispondente è dichiarato irraggiungibile. Durante il counting to infinity i pacchetti sono in ciclo, i link si congestionano e si forma una probabilità di perdita elevata dei pacchetti (compresi i pacchetti di routing). La convergenza potrebbe essere comunque molto lenta.

Un altro rimedio è lo split-horizon: se il nodo sorgente A invia a D intermedio i pacchetti indirizzati a X, è inutile che A annunci X nel proprio DV in D. il nodo A non fa pubblicità a D della destinazione X. Nello split horizon il nodo A invia diversi DV su diversi link locali.

Esistono due tipi di split horizon: la versione base dice che il nodo omette qualunque informazione sulla destinazione che raggiunge attraverso il collegamento che sta usando, mentre la versione Poisonous Reverse dice che il nodo include tutte le destinazioni, impostando all'infinito la distanza a quelli raggiungibili attraverso il collegamento che sta utilizzando. Split horizon non funziona con alcune topologie di rete.

Altri rimedi al counting to infinity sono l'utilizzo di contatori/timer (hold down) o l'aggiornamento da trigger, dove avviene una esplicita pubblicazione dei cambiamenti nella topologia, un aumento di velocità sulla convergenza e la scoperta di richieste di cadute.



### Protocolli di routing link state

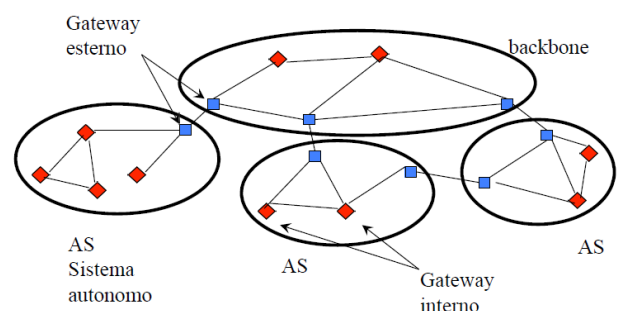
- Ogni nodo conosce i nodi vicini e i costi relativi a raggiungerli. Ogni nodo invia a tutti gli altri nodi tali informazioni (flooding) attraverso pacchetti Link State (LSP). Tutti i nodi conservano un database LSP e una mappa completa della topologia della rete (grafo). Sul grafo completo i cammini minimi sono elaborati con Dijkstra. I vantaggi del Link state sono la flessibilità e ottimalità nella definizione del cammino, le informazioni LSP non sono inviate periodicamente ma solo quando cambia qualcosa e tutti i nodi ricevono prontamente conoscenza di eventuali cambiamenti nella topologia della rete. Gli svantaggi sono che serve un protocollo di segnalazione per mantenere le informazioni topologiche (Hello), la necessità di Flooding, LSP deve essere riconosciuto e è difficile da implementare.
- Con la tecnica del flooding ciascun pacchetto inserito è trasmesso attraverso tutte le interfacce tranne quella di provenienza. Si possono creare cicli e conseguente congestione del traffico. Il numero di sequenza (SN) e la banca dati SN in ciascun nodo sono replicate per evitare trasmissioni multiple dello stesso pacchetto. Si inserisce inoltre un contatore dei salti (uguale a TTL in IP).
- Al ricevimento di un LSP se l'LSP non è ancora stato ricevuto o se il SN è maggiore di quello immagazzinato si conserva il nuovo LSP e si applica il flooding. Se il LSP ha lo stesso SN di quello immagazzinato non si fa nulla. Se il LSP è più vecchio di quello immagazzinato trasmetti il più nuovo al mittente.

## Multi Protocol Label Switching

- MPLS (Multi Protocol Label Switching) è una nuova tecnologia di livello 2 per prendere le migliori caratteristiche di IP e ATM (Asynchronous Transfer Mode) nelle reti a dorsale (backbone), ovvero l'indirizzamento IP e la commutazione ATM (commutazione di etichetta), con alcune funzioni avanzate che eliminano le inconvenienti dei classici protocolli IP al di sopra di ATM. L'architettura generale è composta da dei router di confine e dei router di nucleo e la gestione del flusso avviene attraverso circuiti virtuali (Forward Equivalence Class) che possono essere predefiniti dall'operatore, impostati su richiesta dell'utente, impostati da un meccanismo dinamico e tenendo conto anche della prenotazione delle risorse e della QoS (Quality of Service). In questa architettura è possibile ottimizzare l'instradamento basato su meccanismi statici o dinamici ed è possibile classificare il traffico (definizione di flusso) basandosi su un ricco set di parametri (inclusendo indirizzi sorgente, porte, applicazioni, ...). Quindi, MPLS è una politica di forwarding per reti ad alte prestazioni che rende facile creare link virtuali tra nodi collegati in maniera indiretta e può incapsulare pacchetti di qualunque tipo di protocollo.
- I pregi di MPLS sono che è indipendente dal livello data-link, che è estremamente scalabile (permette il controllo del traffico sul percorso) e qualunque tipo di traffico può essere canalizzato indipendentemente dal sistema di trasporto sottostante (è possibile trasportare un flusso di pacchetti IP attraverso una rete mista ATM, ethernet e frame relay).
- Ogni pacchetto in MPLS (di qualunque natura) viene preceduto da una sequenza di etichette (label stack), ogni etichetta del label stack è composta da un identificatore (20 bit), una classe di traffico (3 bit), un TTL (1 byte) e un flag di "ultima etichetta". Il forwarding viene effettuato basandosi sull'etichetta in cima allo stack. Se ho due flussi avviene una aggregazione di flusso (push and pop): i due flussi sono instradati sul percorso comune, il primo router del percorso aggrega i due flussi con una label aggiuntiva comune (push), i router intermedi inoltrano i pacchetti basati sulla label esterna e l'ultimo router del percorso disaggrega i flussi e li inoltra basandosi sulla label originale (pop).  
I pacchetti di controllo seguono un inoltro hop-to-hop come i tradizionali datagrammi IP, e questi pacchetti creano un nuovo percorso a commutazione di etichetta (circuiti virtuali). I pacchetti il cui percorso è stato creato, possono essere inoltrati direttamente dal livello LS.
- I percorsi dei pacchetti possono essere costituiti offline (ottimizzazione globale basata sulle informazioni di tutte le risorse di rete e di flusso) o online (instradamento basato su vincoli, considerando i vincoli di specifici utenti/flussi come larghezza di banda, inclusione o esclusione di nodi/collegamenti, richieste di specifiche amministrative e possibilità di riarrangiare i flussi già percorsi).
- Viene richiesto un meccanismo di segnalazione per coordinare la distribuzione delle etichette, inizializzare i circuiti virtuali sul percorso selezionati, prenotare delle risorse, riassegnare delle risorse e evitare i cicli.

## Internet routing

- In internet sono presenti vari componenti e vari protocolli: gli Autonomous System sono una porzione di rete gestita da una singola organizzazione, mentre i protocolli usati sono EGP (Exterior Gateway Protocol) e IGP (Interior Gateway Protocol).  
Il dominio di routing (RD) è la porzione di un AS che esegue un singolo protocollo di routing. Alcuni router appartenenti a più RD implementano protocolli di routing multiplo. Più router RD devono agire come protocolli di routing per gateway e la traduzione da un protocollo all'altro dipende dall'implementazione del protocollo, poiché uno potrebbe essere IGP e uno EGP. I più comuni protocolli di instradamento sono RIP (Routing Information Protocol) o IGRP (Interior Gateway Routing Protocol) (protocolli di tipo Distance Vector) e IS-IS (Intermediate System Intermediate System) o OSPF (Open Shortest Path First) (protocolli di tipo Link State) per IGP e BGP (Border Gateway Protocol) (protocollo di tipo Path Vector) per EGP.
- RIP (versione 1) è un protocollo IGP di tipo DV, che usa Bellman-Ford per calcolare i percorsi più brevi. Le metriche usate sono il numero di salti ed è limitato a 16 hops. I messaggi RIP sono incapsulati in segmenti UDP (porta 520) ed inviati con indirizzo IP di destinazione 255.255.255.255. I messaggi RIPv1 possono essere richieste (di invio di un DV) o risposte (stimolate/non stimulate). Se il campo Command è uguale a 1 si tratta di richiesta, se 2 di risposta. La Version è la versione del protocollo RIP, la Family è la famiglia di indirizzi utilizzati (2=IP), il Net. address è l'indirizzo di rete di destinazione e la Distance rappresenta i costi (da 1 a 15, 16=inf). Le richieste possono



Repeated	Command	Version	Reserved
	Family		All 0s
	Network address		
	All 0s		
	All 0s		
	Distance		

di richiesta, se 2 di risposta. La Version è la versione del protocollo RIP, la Family è la famiglia di indirizzi utilizzati (2=IP), il Net. address è l'indirizzo di rete di destinazione e la Distance rappresenta i costi (da 1 a 15, 16=inf). Le richieste possono

provenire da router “appena accesi” o da router che hanno delle destinazioni non aggiornate. Le richieste potrebbero avere a che fare con tutte le destinazioni o una destinazione specifica. I messaggi di risposta possono contenere massimo 25 percorsi e se superiori devono essere mandati con più messaggi UDP. In RIPv1 la sincronizzazione del messaggio può essere svolta con timer di aggiornamento del routing (Periodo di tempo tra la trasmissione di 2 DV contigui), con un timer di percorso non valido o di durata (Se nessun DV viene ricevuto da un interfaccia in questo intervallo, i percorsi sono dichiarato non validi. Esso è ancora annunciato, ma con la distanza = 16 (inf)), con un timer di pulizia del percorso o di raccoglimento rifiuti (Intervallo di tempo dopo il quale un percorso invalido viene cancellato (se diversi DV arrivano da altre interfacce essi sono accettati) - esso è usato per annunciare ai vicini l’invalidità di destinazione prima di annullare il pacchetto). Si usa un meccanismo di aggiornamento innescato: se una metrica cambia in un itinerario, un DV viene immediatamente inviato con le sole entrate modificate.

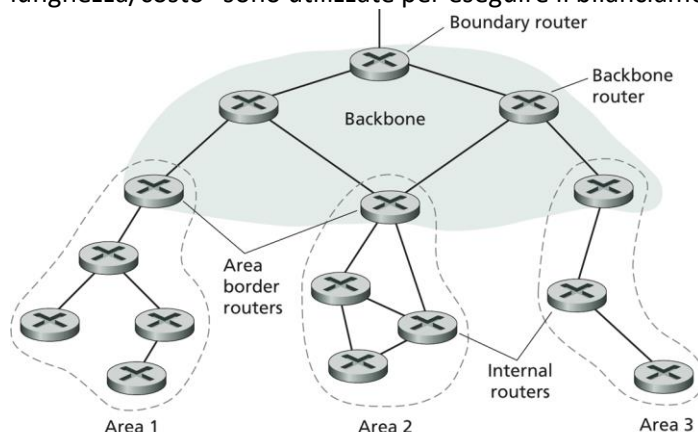
In RIPv1 il contatore di salti è una metrica molto semplicistica e si vorrebbero usare metriche più complesse come lunghezza della coda, ritardi o tasso di errore del pacchetto. RIPv1 funziona solo per piccole-medie reti (fino a 15 nodi come diametro della rete) e il tempo di convergenza è lento.

Con RIP versione 2 si aggiungono delle funzionalità: informazioni sulla connettività, autenticazione, routing senza classe (maschere di sottorete) e multicasting (utilizza l’indirizzo 224.0.0.9 come indirizzo destinatario).

Command	Version	Reserved
Family		Route tag
Network address		
Subnet mask		
Next-hop address		
Distance		

Per l’autenticazione in family si ha FFFF e il route tag è il tipo di autenticazione. Il network address, subnet mask, next-hop address e distance sono dati di autenticazione (16 byte).

- OSPF opera nello stato di collegamento (link state) con l’esecuzione di Dijkstra in ogni nodo. OSPF supporta il routing gerarchico (aree di routing e di backbone), utilizza metriche generiche (Il costo della traslazione di un interfaccia può essere impostato dal amministratore di rete) e utilizza il protocollo Hello per monitorare lo stato dei vicini. Utilizza anche LSA (annuncio dello stato di collegamento). OSPF è trasportato direttamente sopra IP (Protocol=89) e deve implementare funzioni di trasporto (messaggi ACK), vari tipi di messaggi, supportare l’autenticazione e supportare più percorsi verso la destinazione (rotte con la stessa lunghezza/costo” sono utilizzate per eseguire il bilanciamento del carico).



In rappresentazione OSPF il collegamento tra i nodi (reti token ring, point-to-point, transient) viene sostituita dal router designato. OSPF contiene moltissimi tipi di pacchetti e vengono riconosciuti i pacchetti di instradamento. Hello gestisce lo stato di collegamento dei vicini, descrizione DB scambia l’intero database della rete (per esempio durante la fase di inizializzazione), richiesta LS chiede informazioni su un percorso specifico, aggiornamento LS invia messaggi di stato dei collegamenti, sia per la topologia interna sia per le destinazioni esterne e LS ACK invia l’ACK per i messaggi LS. L’installazione comune di OSPF è:

1	4	8	16	19	32
Versione (1)		Genere		Lunghezza del messaggio	
Indirizzo IP gateway sorgente					
ID di area					
Checksum			Tipo di autenticazione		
Autenticazione					
Autenticazione					

campo Tipo: tipo di pacchetti OSPF

Indirizzo IP del gateway di origine: indirizzo IP del mittente

ID area: indica l’area



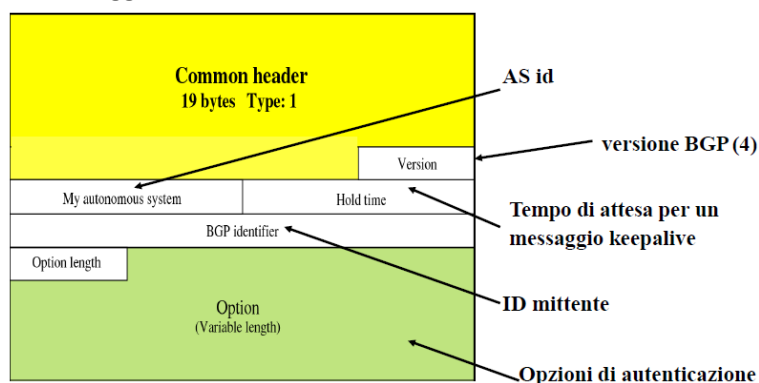
I tipi di LSA in OSPF sono annuncio collegamenti al router (all'interno della stessa zona), annuncio collegamento di rete (generato da un pseudo-nodo LAN), annuncio riassunto del link state (generato dai router del bordo dell'area per riassumere le informazioni riguardanti un'area), annuncio sintesi del collegamento dei router di bordo (generato dai router del bordo dell'area, indica la presenza di un AS router di confine nell'area e il costo associato) e annuncio collegamento di AS esterno (generato da router AS di confine e propagato a tutti i router di tutte le aree con informazioni sulle destinazioni esterne e i relativi costi associati).

I router al confine dell'area propagano in ogni area informazioni di routing per quanto riguarda tutte le altre zone connesse a essi (contaminazione del DV).

OSPF invia periodicamente messaggi HELLO per verificare se i vicini sono raggiungibili. I messaggi di descrizione del database sono utilizzati per inizializzare la base dati di topologia e i dati sulle metriche di collegamento sono trasmessi attraverso i messaggi di aggiornamento di stato del collegamento. Il pacchetto HELLO si occupa di scoprire i vicini e selezionare un router designato. I pacchetti LSU (Link state Update) hanno, oltre all'intestazione comune, anche l'intestazione di collegamento di stato comune e il payload. Il collegamento alla rete LSA è quindi usato per pubblicizzare le reti al di fuori dell'area di un AS e 1 messaggio per 1 rete (messaggi multipli necessari per indirizzare più reti).

- Il più utilizzato EGP è BGP che è la "colla" di internet, perché permette al AS di annunciare la loro presenza in internet e di raggiungerlo. I problemi di routing inter AS sono diversi da quelli intra AS: i criteri di decisione del percorso non sono basati sulla metrica, i gestori della backbone scelgono i router in base a una politica e le scelte di routing servono per esplodere la conoscenza completa del percorso per la destinazione. Così i DV non vanno bene dato che non sono a conoscenza di tutti i percorsi e i LS non vanno bene in quanto avranno bisogno di costruire una banca dati di tutta la rete internet. BGP è simile a DV ma i PV (path vector) non riportano una "distanza per la destinazione" ma l'intero percorso fino a destinazione. I messaggi scambiati tra due router in un path vector non contengono soltanto un percorso ma anche una sequenza di attributi che potrebbero essere obbligatori (che devono essere compresi da ogni implementazione BGP) e facoltativi. Gli attributi obbligatori sono l'ORIGINE (protocollo di origine IGP delle informazioni), l'AS\_PATH (sequenza di AS attraversati) e il NEXT\_HOP (router successivo). Ogni router BGP invia il suo vettore dei percorsi ai nodi vicini (colleghi), i messaggi BGP usano TCP e le connessioni TCP sono aperte dai router invianti e si utilizza numero di porta 179. I tipi di messaggi BGP sono OPEN (apre la connessione TCP e gestisce l'autenticazione reciproca dei due router), UPDATE (annuncia un nuovo percorso (o ne cancella uno vecchio)), KEEPALIVE (mantiene attivo un collegamento in mancanza di UPDATE (anche usato come ACK per i messaggi aperti)) e NOTIFICATION (notifica gli errori nei messaggi precedenti (o si utilizza per chiudere una connessione)). BGP permette la distribuzione di percorsi per specifiche destinazioni ma lascia la scelta del routing per l'amministrazione della rete (politica basata su instradamento): un router BGP riceve un path vector da un compagno e può decidere se aggiungere alla tabella di routing la destinazione specificata in PV e/o inoltrare il PV al suo vicinato. Esso è basato sulla politica di instradamento locale e a ogni AS è assegnato un ASN (Autonomous System Number) con senso globale da IANA (come gli indirizzi IP).

I messaggi BGP hanno un'intestazione comune.



I messaggi di apertura sono messaggi di configurazione dei compagni: i router rispondono con messaggi keepalive (solo intestazione comune).

I messaggi di aggiornamento contengono il vettore del percorso e sono utilizzati per pubblicizzare il percorso o per annullare i percorsi precedentemente annunciati.

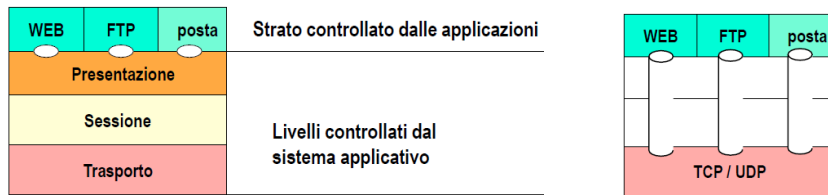
## Livello applicazione

### Client-server e paradigmi peer-to-peer

- Progettare le applicazioni di rete significa scrivere programmi che funzionino su diversi sistemi terminali e comunichino su una rete, come nel web dove i software web server comunicano con i software browser. Esiste poco software scritto per i dispositivi nel nucleo della rete: i dispositivi nel nucleo della rete non

eseguono codice di applicazioni utente e le applicazioni sui sistemi finali permettono sviluppo e propagazione di applicazioni rapide.

- I processi sono programmi in esecuzione all'interno di un terminale. Entro lo stesso Host due processi comunicano utilizzando comunicazioni tra processi (definite da OS) mentre i processi su host differenti comunicano attraverso lo scambio di messaggi. I processi in esecuzione su host remoti potrebbero scambiare messaggi e servizi attraverso la rete. I protocolli applicazione definiscono le regole e i formati di comunicazione tra processi remoti. Questi protocolli utilizzano i servizi forniti dagli strati inferiori attraverso i SAP (Service Access Point) e ogni processo di applicazione è associato a un SAP. Secondo la pila OSI:



I protocolli applicazione comunicano direttamente con lo strato trasporto. Un processo invia/riceve messaggi a/dai suoi socket. Il socket è analogo a una porta: il processo di invio spinge il messaggio fuori dalla porta e si basa su infrastrutture di trasporto sul lato opposto della porta che porta un messaggio per il socket al processo ricevente. Il socket equivale a un SAP tra il livello applicazione e trasporto.

- Per ricevere i messaggi, un processo deve avere un identificatore. Un dispositivo/host ha un unico indirizzo IP a 32 bit. L'indirizzo IP non è sufficiente a identificare il processo: l'identificatore comprende l'indirizzo IP e il numero di porta associato al processo sull'host. Il livello di trasporto multiplexa i diversi flussi provenienti dal livello applicazione.
- Il protocollo di livello applicazione definisce i tipi di messaggi scambiati, la sintassi del messaggio, la semantica del messaggio e le regole per quando e come un processo invia e risponde ai messaggi. I protocolli di dominio pubblico sono definiti in RFC e permettono l'interoperabilità ma esistono anche i protocolli proprietari. La decisione di quale servizio di trasporto serve a una applicazione dipende dalla perdita di dati (alcune applicazioni (audio ad esempio) tollerano delle perdite, mentre altre richiedono 100% di affidabilità), dalla sincronizzazione (alcune applicazioni richiedono poco ritardo per essere efficaci) e dalla larghezza di banda (le applicazioni multimediali richiedono quantità minime di larghezza di banda per essere efficaci, mentre altre applicazioni si adattano alla larghezza disponibile).
- L'obiettivo principale della comunicazione tra processi remoti è la fornitura di servizi. Due funzionalità possono essere realizzate da un processo: richiesta di servizi e fornitura di servizi. Se un dato processo realizza solo una delle funzionalità allora la comunicazione è solo client-server. I processi client fanno richieste e interpretano le risposte, i processi server interpretano le richieste e forniscono risposte. Se lo stesso host deve sia richiedere che fornire allora ha bisogno di due processi. Le possibili architetture dei protocolli applicativi sono client-server (terminali agenti come client o come server con possibilità di differenti caratteristiche) o peer-to-peer (P2P- dove tutti i terminali possono implementare il processo client e il processo server) o ibrido.
- Nell'architettura client-server il server è un terminale sempre acceso, gli indirizzi IP sono permanenti e i server si ridimensionano. Al contrario il client comunica con il server, può collegarsi a esso intermittenemente, può avere IP dinamici e non comunica direttamente con il server.
- Un'architettura P2P pura ha dei server non sempre accesi e i sistemi terminali comunicano direttamente e arbitrariamente. I colleghi (peer) si connettono intermittenemente e cambiano indirizzo IP. Un esempio è Gnutella. Questi protocolli sono altamente scalabili ma difficili da gestire.

## Navigazione web

- HTTP (HyperText Transfer Protocol) sfrutta l'architettura client-server. I clienti richiedono oggetti (File) identificati attraverso un URL (Uniform Resource Locator) mentre i server inviano i file ai clienti. HTTP svolge operazioni senza stato (nessuna memoria delle precedenti richieste). HTTP si basa su TCP per il trasferimento di messaggi. Generalmente una pagina web è composta da un documento principale (HTML) e multipli oggetti collegati. Un oggetto può includere immagini JPEG, JAVA applet, file audio e video, link a altre pagine.... Le richieste utilizzano l'URL che è caratterizzato da un tipo di protocollo, l'indirizzo simbolico del server e il documento sul server. TCP assegna il numero di porta 80 ai server HTTP. Il trasferimento di messaggi avviene con due modalità: connessione non persistente (modalità di default di HTTP 1.0) e persistente (HTTP 1.1 e HTTP/2).
- Nella connessione non persistente si instaura una connessione TCP per ogni ciclo di richiesta-risposta. Il server chiude la connessione TCP una volta che ha inviato l'oggetto richiesto. La stessa procedura viene adottata per tutti i documenti all'interno della pagina web richiesta. Possono essere aperte più connessioni

TCP in parallelo. Il numero massimo di connessioni può essere impostato nella configurazione delle opzioni del browser.

Nella connessione persistente il server non chiude la connessione dopo la risposta. La stessa connessione può essere utilizzata per trasferire altri oggetti all'interno della stessa pagina oppure anche altre pagine web. Il server chiude la connessione sulla base di un timeout. Ci sono due possibilità: senza pipelining (il cliente emette una nuova richiesta solo dopo la ricezione della precedente risposta) e con pipelining (più richieste possono essere emesse nello stesso tempo (Modalità predefinita HTTP v1.1)).

- La stima del tempo necessario per l'intero trasferimento è data da vari tempi: il Round Trip Time (RTT) è il tempo per il trasferimento di un messaggio da client a server e viceversa e quindi il tempo di risposta per http è un RTT per stabilire la connessione TCP + un RTT per inviare il primo byte della richiesta HTTP e ricevere il primo byte della risposta http + il tempo per trasmettere l'intero byte dell'oggetto (file HTML, immagini, eccetera...). alcuni metodi usati nelle richieste HTTP sono GET, HEAD, POST e PUT (oltre a PATCH, COPY, MOVE, DELETE, LINK, UNLINK e OPTION). Nelle risposte i messaggi nella linea degli stati sono identificati con un codice: 1xx è informativo, 2xx successo, 3xx reindirizzamento, 4xx errore del client e 5xx errore del server. Le intestazioni sono utilizzate per lo scambio di ulteriori info di servizio e un messaggio può trasportare intestazioni multiple.
- Il compito principale di un proxy è quello di fornire una memoria cache distribuita. Se un documento è memorizzato in un proxy presso il cliente il tempo di download viene ridotto. Un proxy è un gateway applicativo, ovvero è implementato fino a livello applicativo e deve lavorare sia come un client che come un Server. Il server finale parla con il cliente sul proxy (nascondiglio di utenti).
- Ricordiamo che HTTP è senza stato quindi le richieste consecutive dallo stesso utente non possono essere riconosciute. La procedura di autenticazione molto semplice è basata su UserID e password inserite nella richiesta. Il server può assegnare a ogni cliente un numero di cookie che identifica il cliente in future transazioni. Il numero di cookie viene memorizzato dal cliente e utilizzato in seguito alle richieste verso lo stesso server.
- Per ridurre la latenza (o tempo di caricamento) delle pagine web e per risolvere alcuni dei problemi di HTTP 1.1 è nato HTTP/2. Esso è in formato binario e trasferisce frames. Sfrutta il multiplexing (una connessione TCP per flussi multipli), comprime l'intestazione, svolge un servizio di server push, implementa a livello applicativo un controllo di flusso e usa TLS (ma esiste anche senza). La frame di HTTP/2 ha un campo type che può essere DATA, HEADERS, PRIORITY, SETTINGS, RST\_STREAM e altri. L'intestazione delle richieste HTTP può avere dimensioni non trascurabili, in quanto può contenere: diversi cookies, parecchie linee di intestazione per l'autenticazione, specifiche della transazione, ect. L'intestazione di HTTP consecutivi (verso lo stesso server) contengono informazioni ridondanti. Si può quindi usare la codifica di Huffman (dà stringhe binarie ai più comuni simboli), indicizzazione (consiste nel dare un indice per le più comuni linee di intestazione e poi inviare solo il tale index nei messaggi) e codifica differenziale (l'intestazione di richieste consecutive porta solo la differenza rispetto alla intestazione di richieste precedenti).

Come detto sopra, HTTP/2 svolge multiplexing: La frame scambiata tra client e server è organizzata in Flussi. Uno stream è una sequenza logica di frame e ogni stream ha una priorità (settata dal browser). Inoltre, è presente una funzione di server PUSH: Il server può inviare informazioni utili per il client prima che il client le richieda espressamente. Questa funzionalità viene chiesta dal client.

- Per migliorare la sicurezza di HTTP si è passati a HTTPS che sfrutta un sottolivello tra quello applicativo e TCP in cui si usa Secure Socket Layer (SSL) e Transport Layer Security (TLS) che inserisce riservatezza, integrità e autenticazione a connessioni TCP. Essi intervengono con una fase di handshake (fase in cui il server (e il client) si autenticano e accordano su quale tecnica usare per criptare i dati), di trasferimento TDATA (i dati sono divisi in record (PDU), ciascuno dei quali è cifrato con l'algoritmo scelto nella 1° fase) e chiusura della connessione (un messaggio speciale è usato per chiudere la connessione in maniera sicura). Nella fase di handshake, in particolare avviene uno scambio di certificato tra il server e il client (e viceversa) che certifica l'identità del server (client). Il certificato è generato da un Autorità di certificazione (CA) e contiene la chiave pubblica dell'entità certificata, ulteriori informazioni (indirizzo IP, nome, ect) e la firma digitale del CA. inoltre avviene la generazione e lo scambio di chiavi simmetriche per cifrare i dati trasferiti: tale scambio di chiavi simmetriche avviene su una connessione che è, a turno, cifrata con chiavi asimmetriche.
- HTTP gestisce il trasferimento di oggetti e non tiene conto del formato di esso. La visualizzazione dell'oggetto avviene attraverso programmi interprete (browser). Le pagine di testo formattato sono trasferite in file ASCII e sono interpretate secondo le istruzioni di formattazione scritte in HTML. Le pagine HTML potrebbero contenere riferimenti ad altri oggetti che devono essere interpretati dal browser come parte del documento da visualizzare o collegamenti ad altre pagine. Se una pagina HTML è memorizzata sul server e viene inviata

su richiesta, questa è una pagina statica. Esistono anche delle pagine dinamiche: Se una pagina viene creata in tempo reale al momento della ricezione di una richiesta, questa è una pagina dinamica. Il server esamina la richiesta, esegue un programma associato alla richiesta e genera la pagina HTML da inviare al client. Una pagina web potrebbe contenere un programma che va eseguito dal client. Il programma viene scaricato ed eseguito a livello locale dal client. Questo può essere utilizzato per impostare le pagine interattive, grafici in movimento, ect. Queste pagine sono dette pagine web attive.

### **File Transfer Protocol (FTP)**

- Questo protocollo è usato per trasferire i file tra due host remoti. L'applicazione funziona direttamente sul file system (sia dal server che dal client). FTP Utilizza TCP per il trasferimento. Due connessioni TCP sono usate per il trasferimento dei dati e controllo (dati=20 e controllo=21 sul server). La connessione di controllo è aperta nel solito modo: Il server emette una passive open con numero di porta 21 e attende le richieste, il client emette una active open con numero di porta dinamico ogni volta che serve trasferire files. La connessione di controllo è persistente e rimane aperta per tutto il trasferimento dei dati.
- Le connessioni dati sono non persistenti: una connessione per ogni trasferimento di file e la connessione è chiusa al termine del trasferimento file. Per aprire una connessione dati si son due modi:  
1 ° Modo: Il client emette una passive open con un numero porta dinamico, notifica il numero porta al server sulla connessione di controllo attraverso il comando PORT e il server emette una active open attraverso la specifica porta del client usando 20 come numero porta locale.  
2 ° Modo: Il client invia il comando PASV al server, esso sceglie un numero di porta dinamico, emette una passive open e comunica il numero di porta scelto per il client e il cliente emette un active open utilizzando il numero di porta ricevuto dal server.
- Il trasferimento dei dati può essere eseguito in diversi modi e utilizzando diversi formati in base ai tipi di file (ASCII o binario) e alla modalità di trasmissione (modalità stream: Il file viene inviato tramite TCP come un flusso di byte non strutturati, o modalità di blocco: Il file è strutturato in blocchi con un'intestazione ciascuno e inviato a TCP).

### **Servizio mail**

- Esiste un client/user agent e un server mail. Il servizio è offerto dal Simple Mail Transfer Protocol (SMTP) per il trasferimento di posta elettronica dal client al server di destinazione (destinatario) e da protocolli di accesso ai server di posta: per "scaricare" le e-mail dal proprio server di posta (POP3, IMAP). I server di posta contengono per ogni client controllato una coda di email in arrivo (mailbox) e una coda di posta in uscita. Il server di posta riceve tutte le mail in uscita dall'utente client e riceve dagli altri server tutte le mail destinate ai client controllati. I server usano SMTP con gli altri server di posta e con i clienti in caricamento e POP3/IMAP con i clienti in scaricamento.
- La E-mail è un servizio per inviare messaggi testuali in maniera asincrona. Essa viene attuata, mediante una rete di server di posta elettronica, utilizzando il protocollo SMTP. SMTP è un protocollo testuale. Anche il corpo dei messaggi deve essere ASCII (I Binary devono essere convertito in ASCII). Una volta che un server riceve un messaggio da un user agent, memorizza il messaggio in una coda, si apre una connessione TCP (porta 25) con il server di destinazione e viene inviato il messaggio. Il formato dei messaggi è specificato (comando DATA) e alcune intestazioni sono aggiunte al messaggio.
- Per consentire il trasferimento di messaggi non ASCII, vengono usate le Multipurpose Internet Mail Extensions (MIME), tramite tecniche di codifica Base64 (flusso di bit diviso in blocchi da 24 bit ognuno, ogni blocco diviso in 4 gruppi da 6 bit e viene interpretato come un carattere secondo una tabella di conversione) o Quoted-printable (flusso di bit suddiviso in blocchi da 8 bit ciascuno. Se una sequenza corrisponde a un carattere ASCII allora viene inviato immediatamente, in caso contrario, viene inviato come tre caratteri "=" seguito dalla rappresentazione esadecimale del byte. MIME consente il trasferimento di più oggetti all'interno dello stesso messaggio. Per accedere alla casella di posta si usa POP3 (Post Office Protocol) o IMAP (Internet Mail Access Protocol) e HTTP. Se si vuole più sicurezza si può utilizzare anche TLS/SSL.

### **Terminali remoti**

- TelNet (TERminal NETwork) è un'applicazione a terminale remoto con comandi trasferiti attraverso una connessione TCP. In telnet i caratteri trasferiti sono caratteri data e caratteri di controllo.

### **Domain Name System**

- Gli indirizzi IP non sono adatti per essere utilizzati dalle applicazioni. Sono più convenienti gli indirizzi simbolici gerarchici (via, città, stato) e indipendenti dal livello 3. È necessario il Binding. Le reti IP forniscono un servizio di indirizzi simbolici sostenuto da un servizio di database distribuito che gestisce il binding: DNS (Domain Name System). DNS è un protocollo sul livello applicazione che usa UDP/IP per il trasferimento dei messaggi. DNS è attualmente utilizzato anche per creare alias degli Host, creare alias dei server mail e

distribuire il carico. Questo DB è gerarchico e distribuito. Ogni livello nella gerarchia ha una diversa «profondità» di informazioni. Nell'indirizzamento gerarchico ogni gruppo è controllato da una autorità conosciuta. Per avere un indirizzo simbolico si deve passare attraverso queste autorità. I tipi di Name Server sono Local Name Servers (direttamente collegati agli host, ogni ISP (residenziale, universitario, industriale, ecc) ha un LNS e essi parlano con il NS Root), Root Name Servers (memorizza informazioni sull'indirizzamento dei grandi gruppi di host e domini, memorizza informazioni sui NS autorevoli per un dato dominio e colloquia con l'NS autorevole) e Authoritative Name Servers (NS responsabile per uno specifico hostname). Per risolvere un binding ogni host conosce l'indirizzo del LNS, ogni richiesta per la risoluzione di un legame viene inviata ai NS locali utilizzando UDP e l'LNS ottiene informazioni e risponde. Il tipo di informazioni memorizzate può essere A (name=nome host, value=ip), NS (name=dominio, value=nome simbolico server che sa come risolvere il nome), CNAME (name=alias, value=vero nome) e MX (name=dominio di posta elettronica o alias di posta elettronica, value=nome server mail).

- ARPANET utilizzava un db centrale, mentre Internet usa una struttura di database distribuito. Le filiali sono divise in zone e a ogni zona è associato un DNS. Il server di una zona è autorevole per quella zona. Si possono ottenere informazioni in modo ricorsivo (richieste viaggiano lungo gerarchia e le risposte percorrono direzione opposta) o iterativo (un server può notificare il nome di un altro server da cui prendere le informazioni).
- Un server può memorizzare nella cache le informazioni temporanee. Se una richiesta è emessa e riguarda le informazioni memorizzate nella cache del server, esso può rispondere anche se non è autorevole per quelle informazioni. TTL è impostato dal server autorevole per pubblicizzare la "freschezza" di un pezzo di informazioni. Il server non autorevole utilizza il TTL per impostare un Timer di validità per le informazioni della cache.

### Reti Content Delivery

- Per distribuire efficacemente diversi contenuti (video) contemporaneamente a più utenti (molto) lontani tra loro si è deciso di costruire una rete di server geograficamente distribuiti che ospitano copie del contenuto richiesto (similmente a una grande cache distribuita). Questa rete di server (Content Delivery Network, CDN) può essere costruita e di proprietà del fornitore di contenuti o di terzi. Per scegliere il miglior server si può trovare il più vicino (geograficamente) al client, quello col percorso più breve (minor numero di salti verso il client) o permettere all'utente di decidere

### Architetture peer-to-peer

- Nelle architetture peer-to-peer il file sharing è molto semplice. Siccome tutti i peer sono server l'applicazione è altamente scalabile. Si può anche realizzare una directory centralizzata (in origine con disegno "Napster") in cui quando i peer si connettono, informano il server centrale (indirizzo IP e file condiviso) e quando uno di essi richiede un file, la directory centralizzata fa inviare a chi l'ha già il file richiesto. Unico problema: se il server sbaglia, il sistema è bloccato. Le prestazioni sono a collo di bottiglia: il server è il collo di bottiglia. Inoltre, si può avere violazione del copyright: il server può essere responsabile. Il trasferimento di file è decentrato, ma la locazione del contenuto è fortemente centralizzata.
- Un P2P completamente distribuito è Gnutella. In esso non ci sono server centrali, è un protocollo pubblico e molti client Gnutella sono sparsi nel mondo. Gnutella si basa su una rete overlay: graph. Si crea un bordo tra pari X e Y se c'è una connessione TCP. La ricerca dei vicini è distribuita in natura, tutti gli altri peer attivi e i bordi sono reti coperte. Il bordo non è un collegamento fisico. I peer dati saranno tipicamente connessi con <10 vicini coperti. Gnutella è scalabile ma limitata in ambito flooding. L'unione di un peer alla rete avviene in questo modo:
  1. il peer X deve trovare qualche altro peer della rete Gnutella: per utilizzare la lista dei peer candidati
  2. X sequenzialmente tenta di fare TCP con i peer in lista fino alla configurazione della connessione con Y
  3. X invia un messaggio Ping a Y; Y invia Ping.
  4. Tutti i colleghi che ricevono un messaggio Ping rispondono con messaggio Pong.
  5. X riceve molti messaggi Pong. esso può poi configurare connessioni aggiuntive TCP.
- BitTorrent invia file divisi in pezzi di 256 kbyte. Il tracker tiene traccia dei peer che partecipano ad un torrent, il torrent è un gruppo di peer che si scambiano chunk di un file. Il peer che entra in un torrent registrato su un inseguitore ottiene un elenco di colleghi "attivi". L'inseguitore invia un elenco di coetanei attivi su un torrent (indirizzi IP). Il nuovo peer stabilisce connessioni TCP solo con un sottoinsieme di colleghi nella lista (colleghi vicini). I colleghi vicini inviano al nuovo peer la lista dei pezzi a disposizione ed esso sceglie quali pezzi scaricare e da quale peer in base a meccanismi euristici. Il meccanismo di richiesta dei pezzi sfrutta il principio del rarest first: il peer entrante, tra tutti i pezzi mancanti, scarica prima i pezzi rari nella lista dei pezzi inviati da parte di tutti i peer vicini. Il nuovo peer risponde alle richieste che vengono ai x peer che inviano pezzi al massimo rate. Tutti gli altri peer sono



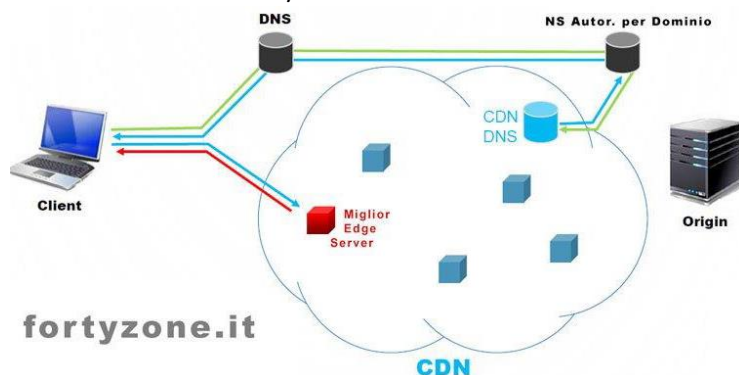
soffocati. I migliori peer X sono rideterminati periodicamente (10 [s]) e ogni 30 [s] un nuovo peer è scelto a caso per inviare un pezzo (soffocato ottimista).

### Modelli per distribuzione di contenuti tra passato, presente e futuro

- Nel passato erano presenti due modelli di rete: il modello telefonico (comunicazione host-to-host e a commutazione di circuito con attenzione rivolta al percorso che collega i due punti finali) e al protocollo internet (comunicazione host-to-host e a commutazione di pacchetto con attenzione rivolta ai due punti finali). Nella fine anni 60 è stato progettato IP per sfruttare le costose risorse di calcolo disponibili in remoto. La natura di "Internet TCP / IP" odierna è quella di una rete di comunicazione. Tuttavia, gli utenti sfruttano di più Internet come una infrastruttura di distribuzione: Vogliono recuperare il contenuto ma non ha molta importanza quale server fornisce i dati. Per riempire il vuoto di questo disallineamento, la distribuzione di contenuti viene eseguita utilizzando approcci di copertura CDN o P2P. Le proposte per il futuro sono le Information-Centric Networks (ICNs): modificare i protocolli di livello rete per trasformare Internet in una architettura per la distribuzione di contenuti. Fanno rispettare congiuntamente nuovi requisiti:
  1. distribuzione di contenuti scalabile
  2. Supporto alla mobilità
  3. Sicurezza della rete

### Content Distribution in Internet: CDN

- L'internet TCP/IP odierno si basa sulle Reti Content Delivery per accogliere le esigenze degli utenti correnti. Una Content Delivery Network è un sistema distribuito composto da molti "server surrogati" (o anche "server replica") utilizzato per offrire una distribuzione di contenuti con un servizio trasparente e gestita da un unico proprietario (in maniera centralizzata). Essere centralizzati significa che il proprietario CDN può ottimizzare il posizionamento del server replica, il posizionamento dell'oggetto replica e l'instradamento della richiesta. Le Content Delivery Networks (CDNs) rendono possibile ospitare il traffico delle richieste degli utenti nell'internet TCP/IP attuale.



- I meccanismi di instradamento delle richieste sono un componente chiave: DNS-based / URL Rewriting / HTTP redirection. Gestire una CDN è molto costoso a causa di enormi spese per la distribuzione dei server Replica e anche perché essa è anche costosa per la gestione della infrastruttura di "Mappatura". Inoltre, la sicurezza è non banale: usa i certificati condivisi Akamai oppure lascia trasferire in maniera sicura i contenuti sotto il proprio dominio.
- La diffusione di contenuti con l'architettura Web ha avuto uno sviluppo notevole grazie al suo paradigma semplice e di grande efficacia (per mezzo dell'architettura Web è possibile trasferire contenuti di tipo eterogeneo: testo, audio, video, immagini, ecc. Storicamente i contenuti via Web sono stati resi disponibili per mezzo di server centralizza: (origin server) nella rete di backbone. Molti client che accedono alla medesima informazione generano un carico su tale server e sulla rete che può essere evitato o ridimensionato. Nuove strategie per la diffusione efficiente di contenuti via Web sono state definite per fronteggiare l'aumento del traffico in rete, assicurare latenze accettabili e occupare le risorse in modo efficiente.
- L'introduzione di sistemi che replicano i contenuti (sistemi di caching) e si frappongono tra client e origin server (detti Proxy o Proxy Applicativi) è una pratica che tende a migliorare il sistema di distribuzione dei contenuti. Una possibilità è usare dei Reverse proxy utilizzati come front-end del server dai fornitori di contenuti per ridurre il carico del server per la diffusione di contenuti statici. I Forward proxy sono sistemi intermedi con funzioni di replica dei contenuti posizionati in prossimità dei client e dispiegati nella rete aziendale o dall'ISP nella sua rete. Questa posizione consente di ridurre la latenza di accesso e contenere il carico di rete per contenuti popolari. Chiameremo sia i Forward che i Reverse proxy con il termine generico di cache. La replica dei contenuti è efficace se i contenuti sono consistenti e validi e sono richiesti da una pluralità di utenti (località spaziale e temporale). Ci sono due diverse modalità di caching: il contenuto può

essere replicato dalle cache opportunisticamente quando viene richiesto da un utente (sistema pull) oppure le repliche dei contenuti possono essere sistematicamente programmate (sistema push). Ci sono inoltre due diverse tipologie di accesso alle cache: nel Transparent Caching le cache sono trasparenti rispetto ai client (intercettano il traffico in transito), mentre nel Caching Esplicito i client sono configurati per puntare ad un sistema intermedio che fa caching. La capacità di storage delle cache che possono essere posizionate vicino agli utenti è usualmente scarsa. Gli accessi sono spesso correlati tra loro e si dice che possiedono località temporale (informazione consultata in tempi brevi) o spaziale (informazione consultata da punti adiacenti). Il caching deve garantire anche consistenza, ovvero assicurare che le repliche siano coerenti e allineate.

- Esistono diversi gradi di consistenza: forte (evita consegna di repliche non consistenti) o debole (bassa probabilità di consegna di repliche non consistenti). Esistono 3 meccanismi per controllare le repliche di contenuti nella cache: invalidation (dipende dall'expected expiry time, definito dall'origin server. Una replica viene invalidata dopo la scadenza di tale tempo), freshness (garantisce che una replica in cache sia considerata "fresca", ovvero non obsoleta) e validation (permette di controllare se una replica nella cache è ancora valida, anche dopo la scadenza dell'expected expiry time). Il caching può essere anche cooperativo: quando la cache non contiene un contenuto specifico (cache miss), anziché chiederlo all'origin server, lo chiede ad altre cache. Esistono due tipologie di cache cooperativo: flat (tutte le cache sono a pari livello) o gerarchico (le cache sono strutturate in livelli gerarchici e la diffusione dei contenuti è organizzata ad albero).
- Le direttive HTML e HTTP consentono a client e server di impostare le modalità di caching di un contenuto. In particolare, le direttive HTTP imperative hanno precedenza su altri controlli della cache: nelle richieste e nelle risposte si usa cache-control: no-store o no-transform per impedire caching degli oggetti o della sola trasformazione dei dati e solo nelle richieste si usa cache-control: only-if-cached per richiedere uso esclusivo di un contenuto presente in cache.

Le direttive sul ciclo di vita di un contenuto sono date da Last-modified (istante in cui il contenuto è modificato da origin server), Date (istante in cui oggetto è inviato da origin server a cache), Expires (predizione del server di quando le copie devono essere sostituite) e Age (tempo passato dall'oggetto in cache).

Esistono poi delle direttive di tempistica come Max-age (il client può non gradire informazioni con una certa obsolescenza), Min-fresh (il client si assicura che un contenuto sia sufficientemente distante dallo stato di Expiry) e Max-stale (il client potrebbe accettare un contenuto un po' obsoleto). L'origin server limita il tempo di vita dei contenuti che invia alle cache per mezzo dell'Expires. L'expiry time è però una predizione del server e può essere sbagliata; per questo è necessario ricorrere alla validazione una volta raggiunto l'expiry time. La validazione da parte del client è svolta in questo modo: il client cerca una replica valida, la validazione è la verifica effettuata per capire se, una volta che l'expiry time scade, una copia è ancora utilizzabile e se l'expire time è stato raggiunto per il contenuto richiesto il client invia una GET request con alcuni parametri settati e il server risponde con il contenuto se modificato o un response code Not Modified.

- Le tipologie di contenuti presenti sono eterogenee: possono esserci contenuti statici, volatili o dinamici. I contenuti multimediali sono solitamente statici. Una porzione dei contenuti è "uncacheable": le principali fonti di uncacheability sono volatilità, dinamicità, SSL e Advertising/Analytics. Tuttavia la maggior parte dei contenuti volatili o dinamici ha una dimensione modesta, mentre i contenuti statici e multimediali sono voluminosi.
- Una CDN è un'infrastruttura creata per distribuire efficacemente i contenuti dei server Web più popolari agli utenti internet. Le CDN si basano sulla distribuzione programmata e intelligente di repliche dei contenuti del server principale del Content Provider (origin server) ad ogni molteplicità di server disposti sulla rete da un CDN Provider. Il servizio CDN punta a migliorare le prestazioni (riduzione latenza di accesso al contenuto e riduzione della banda occupata in rete). I componenti dell'architettura CDN sono:
  1. Componenti di content delivery (origin server e insieme di replica server)
  2. Componente di distribuzione del contenuto (Replica il contenuto dell'origin server nei Replica server e mantiene la consistenza)
  3. Componente di request routing (indirizza le richieste degli utenti verso un server e interagisce con il componente di distribuzione per mantenere una coppia aggiornata del contenuto)
  4. Componente di accounting (mantiene i log degli accessi degli utenti e effettua analisi del traffico e permette al Content Provider di effettuare la tariffazione).

Nasce un problema di ottimizzazione per il placement dei replica server. È variante del problema di k-means: dato un insieme di punti (utenti) e k (=numero replica server) bisogna dividere i punti/utenti in k cluster tali da minimizzare una funzione obiettivo.

- Per indirizzare una richiesta di un client ad uno specifico cache server della CDN si utilizza il sistema DNS con i meccanismi di DNS redirection (Il DNS autoritativo dei siti Web può delegare la risoluzione dell'hostname in

un IP a un name server controllato dalla CDN o effettuare direttamente la risoluzione di un indirizzo a un cache server della CDN (se la CDN può gestire direttamente il DNS autoritativo). In entrambi i casi la scelta di un determinato cache server della CDN è effettuata con la traduzione da hostname a indirizzo IP dal sistema DNS interno alla CDN) e URL rewriting (il Content Provider riscrive le URL presenti nella pagina HTML in modo da far apparire che gli embedded object sono localizzati su un cache server. Così ci sarà bisogno di una risoluzione specifica dell'hostname dei vari embedded object il cui name server autoritativo è sotto il controllo della CDN. È possibile usare più di un cache server per gli embedded object di una pagina).

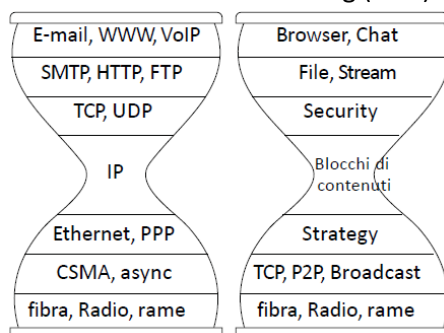
- Akamai è una società statunitense che possiede la CDN più estesa al mondo e numerosissimi Content Provider utilizzano al CDN akamai per la diffusione dei propri contenuti. Un sito Web che vuole avere una parte dei propri contenuti distribuiti da Akamai deve rinominare le URL ad esse relative con un prefisso specifico. La risoluzione dell'hostname in un indirizzo IP di un cache server di Akamai è eseguita dal DNS di Akamai. Il cache server prescelto è «vicino» al client e non deve essere sovraccarico. Il content provider seleziona il contenuto che sarà ospitato da Akamai. Akamai fornisce uno strumento che trasforma l'URL nell'ARL (Akamai Resource Locator). In questo modo, il client accede ai cache server di Akamai e non all'origin server. Se il server Akamai non ha il contenuto in cache esso viene richiesto all'origin server. Akamai prevede due livelli di ridirezione DNS: Akamai Top-Level Name Server (TLNS) e Akamai Low-Level Name Server (LLNS). I TLNS rispondono con un LLNS preso da un insieme di 8 vicini all'utente. I LLNS puntano verso gli Akamai Edge Server che consegnano i contenuti.

### Content Distribution in Internet: ICNs (NDN e CCN)

- Progressivamente si assiste ad un cambio di paradigma dell'uso preminente della rete internet: da sistema di condivisione di risorse e di conversione tra host a sistema di distribuzione di contenuti in varie forme e con volumi crescenti. La consapevolezza di queste tendenze ha sollecitato lo studio di un nuovo paradigma per Internet che sposta il fuoco dell'attenzione sul trattamento dei contenuti: Information Centric Networking. Esso è un paradigma alternativo a IP, basato sui contenuti piuttosto che sugli indirizzi.
- ICN è un marchio comune per molti design di internet del futuro. Come CDN, i design ICN propongono di appiattire l'internet e replicare contenuti sul "bordo" della rete, più vicino alla posizione degli utenti finali. Diversamente da CDN le ICNs sono gestite da molti operatori (in maniera distribuita) e esse sono di solito costruite come protocolli tabula rasa di livello rete. Tutte le proposte ICN condividono un insieme di principi: un nuovo namespace di indirizzamento orientato ai contenuti, funzionalità di caching aggiunte ai nodi di rete e lo stesso contenuto può potenzialmente essere recuperato da molte posizioni (addirittura terze parti non attendibili – la sicurezza può essere eseguita fissando il canale di comunicazione, ma deve essere costruito proprio all'interno del contenuto stesso).

Tra tutte le proposte ICN ci focalizziamo su NDN/CCN.

Il Content-Centric Networking (CCN) e il progetto Named Data Networking (NDN) hanno come principio di progettazione il creare una nuova "vita" sottile per la clessidra di internet. In CCN i nomi sono a struttura gerarchica, opachi alle applicazioni. Ogni nome è una lista di componenti a lunghezza variabile. Sono previsti due tipi di pacchetti: il pacchetto interesse e il pacchetto dati:



Pacchetto Interesse	
Nome contenuto	
Selettore	
(Ordine di preferenza, filtro editore, scopo, ...)	
Nonce	

Pacchetto dati	
Nome contenuto	
Firma	
(algoritmo compresso, testimone, ...)	
Informazioni firmate	
(ID editore, locazione chiave, tempo stantio, ...)	
Dati	

I nodi CCN hanno 3 componenti: FIB (Forwarding Table-abilita più interfacce di uscita), il Content Store (cache dei pacchetti dati) e il PIT (Pending Interest Table). Il consumatore invia a tutti il suo interesse su tutte le connessioni disponibili. I pacchetti Dati sono trasmessi solo in risposta a pacchetti Interesse e consumati da chi interessano. I pacchetti Dati soddisfano un Interesse se ContentName nel pacchetto Interesse è un prefisso di quello dei pacchetti Dati. FIB comprende una lista di interfacce di uscita – sorgenti multiple di dati. PIT tiene traccia degli Interessi inviati in ingresso => I Dati sono inviati in uscita. I pacchetti Interesse sono inviati in ingresso – I pacchetti Dati seguono lo stesso percorso all'indietro. Ogni riga della tabella PIT è una "braciola di pane" che segna il percorso e viene cancellata dopo essere stata usata.

- Processamento di un Interesse: Se I dati di interesse sono trovati nel Content Store => inviali e consuma Interesse. Se l'interesse è in attesa nel PIT => aggiungi questa face alla lista di RequestingFaces. Usa FIB per inviare l'Interesse sulla face di uscita, aggiungila a PIT.

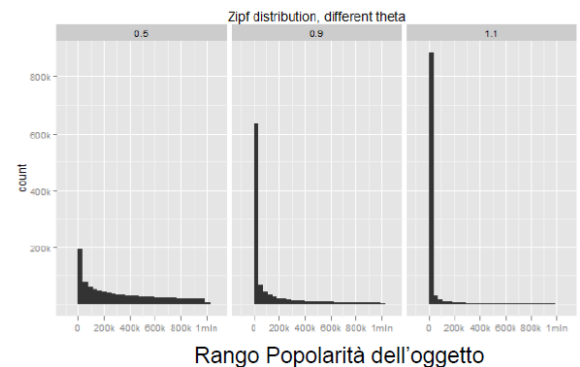
Processamento di un pacchetto Dati: I Dati seguono una catena se le righe di PIT tornano alla sorgente. I duplicate e i Dati non sollecitati sono cancellati.

- Le comunicazioni sicure in NDN/CCN possono essere implementate facendo rispettare tre proprietà al consumatori: Integrità dei dati, provenienza e rilevanza. Mentre nell'odierno Internet TCP/IP, invece, si protegge il canale di comunicazione tra i due punti finali. In NDN ogni pacchetto è firmato dal legittimo produttore (il key-locator è specificato nel pacchetto). Ogni nodo può servire il contenuto, ma il cliente può verificare validità/integrità dei dati, provenienza e rilevanza. Solo i pacchetti Data sono firmati. La firma crea un collegamento fra il Content Name = C, i dati = D e la chiave privata PK del produttore:  $\langle C, D, \text{Sign}_{PK}(C, D) \rangle$ . La locazione della chiave pubblica può esser trovata nel campo Key-Locator.

Le attuali proposte CCN non forniscono i mezzi per far rispettare comunicazioni confidenziale, accesso di contenuti tracciabili e non supportano l'evoluzione delle politiche di accesso.

ConfTrack-CCN: il primo strato di crittografia fa rispettare la riservatezza, il secondo strato fa rispettare la tracciabilità e si ha una derivazione di Chiave: a sostegno della evoluzione della politica. ConfTrack-CCN è Cache-friendly.

- Nei modelli di popolarità la popolarità del contenuto è il parametro che più influenza il risultato. Alcune assunzioni comuni fatte nella letteratura sono che le richieste seguono il Modello di Riferimento Indipendente (IRM) e che l'oggetto di popolarità è Zipf.



- Il posizionamento dei server surrogati si ottiene con il modello K-mediana.

Denotiamo :

- L'insieme di server, router e consumatori surrogati con:

$\mathcal{D}, \mathcal{R}, \mathcal{C}$ , rispettivamente

- Per ogni router  $j \in \mathcal{R}$ , la variabile binaria  $k_j$  è impostata a 1 se noi colleghiamo un nodo CDN a quel router
- Indichiamo con  $c_{i,j}$  il numero di salti sul percorso più breve fra il consumatore  $i \in \mathcal{C}$  e router  $j \in \mathcal{R}$
- Assegniamo ogni consumatore ad un nodo CDN. Impostiamo  $y_{i,j}$  a 1 se il consumatore  $i \in \mathcal{C}$  è assegnato al CDN schierato sul router  $j \in \mathcal{R}$

- Il problema K-mediano può essere formulato come segue:

$$\min \sum_{\substack{\forall i \in \mathcal{C} \\ \forall j \in \mathcal{R}}} y_{i,j} \cdot c_{i,j}$$

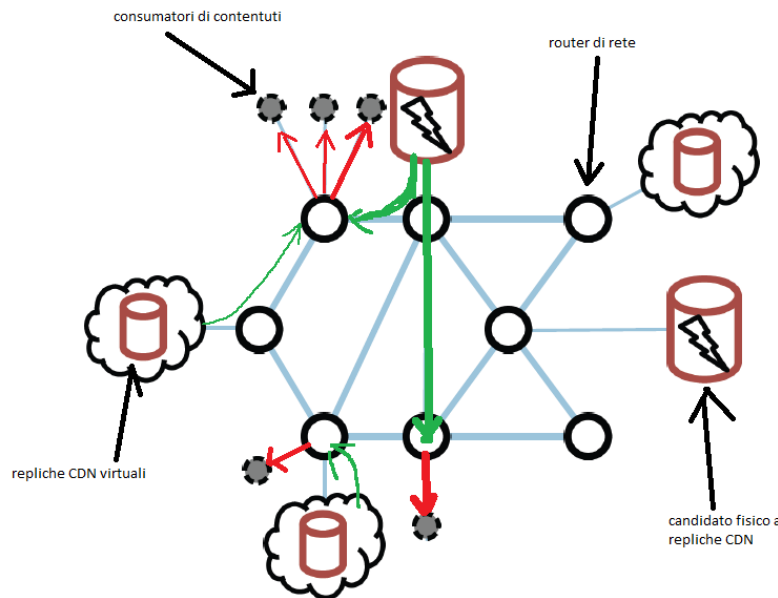
subject to:

$$\begin{aligned} x_j &\geq y_{i,j} & \forall (i,j) \in \mathcal{C} \times \mathcal{R} \\ \sum_{j \in \mathcal{R}} y_{i,j} &= 1 & \forall i \in \mathcal{C} \\ \sum_{j \in \mathcal{R}} x_j &= |\mathcal{D}| \\ x_j &\in \{0, 1\} & \forall j \in \mathcal{R} \\ y_{i,j} &\in \{0, 1\} & \forall (i,j) \in \mathcal{C} \times \mathcal{R} \end{aligned}$$

## Modelli di ottimizzazione stocastica per pianificazione reti virtuali Content Delivery

- Gli utenti al giorno d'oggi sfruttano Internet come una Infrastruttura di distribuzione di contenuti: uno scenario di utilizzo molto diverso rispetto al disegno originale degli obiettivi che hanno guidato la progettazione del Protocollo Internet.
- Virtualizzazione Funzioni di rete (NFV): funzioni di rete eseguite in un ambiente virtualizzato, sopra una infrastruttura fisica condivisa. L'infrastruttura fisica è fatta da server industriali standard a alto volume, memorie e switch. Uno dei casi d'uso per NFV è Virtual Content Delivery Network (VCDN).

Analizzando le previsioni della domanda del traffico, possiamo porci alcuni interrogativi: se la domanda è minore del previsto la rete è sovradimensionata e molte risorse sono sprecate, mentre se la domanda è maggiore del previsto la rete è sottodimensionata e insufficiente per servire la richiesta. Noi affrontiamo il problema stocastico di progettazione della di una vCDN costruita su NFV. La nostra formulazione può togliere le informazioni aggiuntive riguardanti l'incertezza della domanda di traffico.



Nel lungo periodo si può eliminare il candidato fisico a destra poiché non ci sono consumatori. La domanda di traffico (tempo-variante e stocastica) si rappresenta con una freccia dal router di rete al consumatore (freccie rosse). Per come è strutturata la rete la domanda è servita in maniera ottimale usando i CDN fisici attivati e i virtuali (freccie verdi).

Lo scopo del provider è quello di eseguire 2 scelte:

- 1) Selezionare se e dove i nodi CDN fisici dovrebbero essere installati nella topologia di rete
- 2) Selezionare l'ottimale richiesta di routing, dato quello che già esiste.

### Software Defined Networking (SDN)

- Software-Defined Networking (SDN) è un nuovo approccio alla programmabilità della rete, ovvero la capacità di inizializzare, controllare, modificare e gestire dinamicamente il comportamento della rete per mezzo di interfacce aperte. È quindi in breve un modo diverso di pensare alle reti.

In una tipica rete i nodi sono connessi tra loro con protocolli peer-to-peer: I protocolli peer-to-peer sono eccellenti (espandibili, robusti e scalabili (internet)) ma anche costosi da esercire, i problemi sono difficili da localizzare e molto molto difficili da aggiornare ed innovare.

Se si separa il piano dati dal piano di controllo di un nodo di rete? SDN sposta le funzioni di rete in un Sistema Operativo di Rete. La pila SDN ha 3 livelli (strato delle applicazioni, strato dei servizi di rete e strato dei dispositivi) e 2 interfacce (interfaccia northbound (tra applicazioni e controller) e southbound (tra controller e dispositivi)).

- I nodi infrastrutturali fanno moltissime cose ma potrebbero farne di meno ma meglio: Le astrazioni permettono programmi più facili da scrivere e da mantenere. Le astrazioni di piano dati sono gli strati OSI, ma le astrazioni di piano di controllo? Devono essere sviluppati lo strato dei dispositivi e lo strato dei servizi di rete. L'astrazione dei dispositivi si può fare condensando in un dispositivo astratto (tabella di flussi) i vari dispositivi attuali (router, switch, firewall, ...): l'astrazione a tabella di flussi è indipendente dallo strato nel quale il dispositivo dovrà lavorare. Un flusso è definito da una regola di classificazione dei pacchetti in base al valore dei campi dell'intestazione. Ogni pacchetto viene classificato in base a una regola e ad una priorità decrescente.

L'astrazione dei servizi di rete si può fare condensando in due servizi astratti (mappa della rete e intenzioni di rete) i servizi attuali (topology discovery, path computation, state dissemination e fault recovery).

- I vantaggi di business tangibili portati da SDN sono provisioning più rapido delle risorse di rete, maggiore automazione e una concomitante riduzione delle spese operative, più flessibilità e personalizzazione nella configurazione di rete, maggiore utilizzo della capacità di rete a fronte di una riduzione della spesa di capitale e più sicurezza. Tra i vantaggi fatti ricondurre a SDN risulta, inoltre, il supporto ai cloud provider per meglio realizzare e gestire livelli di servizio garantiti applicabili dalle garanzie di uptime alla velocità del deployment, dal provisioning di sicurezza all'utilizzo della larghezza di banda.

Implementare reti basate sul software richiede un ingente investimento iniziale per la sostituzione degli apparati e una revisione complessiva del network per farlo evolvere verso il "software defined" abbandonando l'architettura statica delle reti convenzionali, poco adatta alle dinamiche esigenze di calcolo degli odierni ambienti datacenter, delle reti campus e dei carrier.

Nell'approccio imperativo classico l'obiettivo è instaurare la connettività tra Host 1 e Host 2 attraverso:



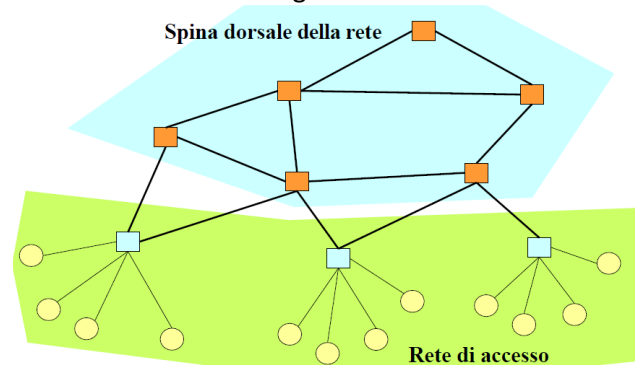
1. Scoprire la topologia della rete
2. Calcolare un percorso
3. Scrivere le regole che definiscono i flussi e le azioni corrispondenti
4. Installare le regole sui dispositivi

Questo approccio molto immediato può fallire in molti modi: ci possono essere regole mancanti, rifiutate o cancellate (controllare continuamente che i dispositivi siano raggiungibili e garantire il raggiungimento di uno stato consistente tra due aggiornamenti) e modifiche alla topologia (ascoltare eventi di guasto da tutti i dispositivi e collegamenti e calcolare i nuovi percorsi e i nuovi flussi). Ogni applicazione richiede il calcolo di percorsi di instradamento, l'installazione di regole, l'aggiornamento di macchine a stati. In caso di guasti si rischiano comportamenti inconsistenti. Bug devono essere sistemati in vari punti della rete. L'aggiornamento di algoritmi che coinvolgono più applicazioni è costoso. Difficile risolvere conflitti tra applicazioni. Bisogna applicare una programmazione dichiarativa (intenzioni di rete): le intenzioni di rete sono un'interfaccia ad alto livello che descrive quale risultato si vuole ottenere e delega allo strato dei servizi di rete come ottenerlo, nasconde alle applicazioni la complessità della rete e garantisce il mantenimento del risultato anche in presenza di modifiche della topologia.

## Tecnologie di rete Wireless: WLAN, WPAN, reti ad hoc

### Introduzione alle reti wireless

- In una rete senza fili il mezzo di trasmissione non è la sola differenza rispetto alle reti cablate: le caratteristiche peculiari medie hanno un grande impatto sulle caratteristiche di sistema e le reti wireless consentono agli utenti di muoversi e naturalmente gestire la mobilità.



Le reti wireless sono principalmente reti di accesso. Le reti dorsali composte da collegamenti radio punto-punto non sono di solito considerate reti wireless. Le reti di accesso wireless sono più impegnative e hanno molte differenze fondamentali rispetto alle reti di accesso cablate. La prima differenza principale è che il mezzo di trasmissione è broadcast (condiviso).

- Prima di inoltrarci sulle tecnologie wireless analizziamo i canali senza fili: generalmente parlando i canali wireless hanno caratteristiche "peggiori" rispetto a quelle dei canali cablati (Forte attenuazione, comportamento variabile nel tempo, distorsioni, ect.). I segnali di propagazione sono colpiti da attenuazione dovuta alla distanza TX-RX, attenuazione dovuta a ostacoli e propagazione su più percorsi. Nel canale wireless si utilizzano le onde radio caratterizzate da una lunghezza d'onda  $\lambda = c/f$ , con  $c$  velocità della luce e  $f$  frequenza. Per esempio, le reti telefoniche mobili usano 900-2200MHz (antenne semplici e piccole. Con potenze emesse intorno a 1W possono coprire fino a pochi km e penetrare nei muri degli edifici), i link point-to-point e link satellitari usano 3-3GHz (abbondanza di larghezza di banda disponibile ma forte attenuazione dovuta agli effetti meteorologici) mentre le reti wireless dati (WLAN, WPAN) usano 2.4 e 5 GHz (ISM band) che però hanno interferenze con altri sistemi e nei 5 GHz ho attenuazione dovuta a pioggia e nebbia.
- Le alte frequenze hanno elevata disponibilità di larghezza di banda, lo spettro è meno pieno di altri sistemi e la propagazione è difficile a causa della bassa penetrazione degli ostacoli (che appaiono come opachi). Nelle basse frequenze c'è bassa disponibilità di larghezza di banda, grandi antenne e molte fonti di interferenza a causa di altre attività umane.

Trasmissione e ricezione sono raggiunte tramite di un antenna: essa è un conduttore elettrico o un sistema di conduttori che in trasmissione irradia energia elettromagnetica nello spazio e in ricezione raccoglie l'energia elettromagnetica dallo spazio. Nella comunicazione bidirezionale, la stessa antenna può essere utilizzata per la trasmissione e la ricezione. L' antenna isotropa (Idealizzata) irradia potenza uguale in tutte le direzioni (3D) => le antenne reali hanno sempre effetti direttivi (verticali e/o orizzontali).

- Le caratteristiche direttive di antenne reali concentrano il potere in alcune direzioni. Questo effetto può essere modellato utilizzando il guadagno  $g(\theta)$  nella direzione  $\theta$ . Il massimo guadagno  $g_T$  è convenzionalmente in direzione  $\theta = 0$ . La densità di potenza nella massima direzione di guadagno è data da:  $F(d) = \frac{P_T g_T}{4\pi d^2}$ . Il

prodotto  $P_{Tg_T}$  è chiamato EIRP (Effettiva potenza isotropica irradiata) ed è l'energia richiesta per raggiungere la stessa densità di potenza con un radiatore isotropico. La potenza ricevuta dipende dalla densità di potenza sull'antenna ricevente e la sua area equivalente:  $P_R = F(d)A_e$  che per un antenna isotropica è  $A_e = \lambda^2/4\pi$  mentre per un antenna direttiva possiamo concentrare l'energia e quindi  $P_R = F(d)g_R A_e$  con  $g_R$  guadagno dell'antenna ricevente. Perciò  $P_R = P_{Tg_T} g_R (\lambda/4\pi d)^2$ . Questo modello è noto come modello di propagazione free space e può essere utilizzato con collegamenti radio punto-punto. Ricordiamo che tra gli effetti della propagazione sono presenti riflessi, shadowing, diffrazione e scattering.

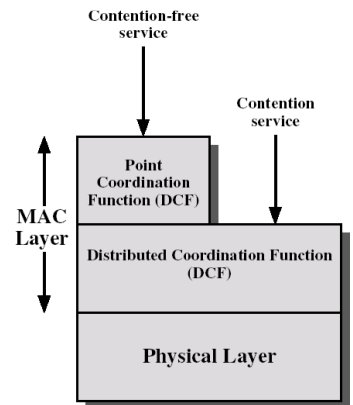
- Se a causa di riflessioni, diffrazioni e dispersioni più copie dello stesso segnale arrivano al ricevitore, si combinano vettorialmente. In caso di propagazione con due raggi, un raggio diretto e uno completamente riflesso, è possibile calcolare l'attenuazione di un segnale ricevuto in forma chiusa. Questo è detto modello two-ray e  $P_R(d) \propto d^{-4}$  e quindi il rapporto tra potenza ricevuta e trasmessa è  $\frac{P_R}{P_T} = g_R g_T \left( \frac{h_1 h_2}{d^2} \right)^2$ . Assumendo una propagazione two-ray, la potenza ricevuta decresce per la distanza più veloce ( $\sim 1/d^4$ ) rispetto al caso di propagazione free space ( $\sim 1/d^2$ ). In realtà, la propagazione tipica nei sistemi wireless è spesso diversa e più complessa che in questi due casi. Tuttavia, un approccio comune alla modellazione della propagazione nei sistemi wireless presuppone che la propagazione sia data da un formula simile ai due casi sopra in cui tuttavia l'esponente della distanza è differente (Coefficiente di propagazione  $\eta$ ) che si può ottenere valori compresi tra 2 (Spazio libero) e 5 (Forte attenuazione nelle aree urbane):  $P_R = P_{Tg_T} g_R (\lambda/4\pi)^2 (1/d^\eta)$ .
- Ci sono diverse tecniche più sofisticate per la stima della potenza ricevuta che si basano sulla la modellazione dettagliata delle caratteristiche della zona in cui il segnale si propaga e sulla simulazione della propagazione (tecniche del tracciato dei raggi). Questa tecnica è di solito molto complessa in termini di calcolo e difficile da usare a causa di una modellazione non accurata dell'ambiente di propagazione. Per questo motivo, molto spesso i modelli empirici sono adottati rispetto a attenuazioni calcolati dovuti alla distanza con formule approssimate appena catturando caratteristiche generali dell'area di propagazione. Il più famoso modello empirico di modellazione delle attenuazione delle distanze è Okumura-Hata (1980). Esso fornisce le formule di attenuazione in vari scenari di riferimento (Grandi città; medio-piccole città; aree rurali e distanze > 1 km).
- Nella propagazione tra trasmettitore e ricevitore, il segnale può seguire percorsi differenti dovuti a totale o parziale riflessione sugli ostacoli. Il comportamento delle onde quando interagiscono con oggetti dipende dalla loro frequenza e dalle caratteristiche e dimensioni degli oggetti. In generale, i segnali a bassa frequenza possono attraversare molti oggetti (che appaiono come trasparenti) con piccola attenuazione, mentre più i segnali di frequenza aumentano, più tendono a essere assorbiti o riflessi dagli ostacoli (a frequenze molto alte - al di sopra di 5 GHz - è possibile una propagazione solo direttiva).
- Nella propagazione il segnale sbatte o è parzialmente riflesso e difratto dagli ostacoli. Questo genera un'ulteriore attenuazione che è generalmente indicata con il nome di shadowing. Questa è una dissolvenza variante lentamente che cambia solo quando il movimento è abbastanza grande per modificare i componenti del segnale. In pratica shadowing è usato per modellare tutti gli altri effetti non catturati da modelli basati su distanza e multi-path.

## WLAN

- Lo spettro è una risorsa scarsa. C'è necessità di regolamentazione, con priorità ad applicazioni "delicate" (militari, mediche ecc.). Molte bande sono licenziate (tassa sull'utilizzo). L'uso dello spettro di frequenze radio è regolato da Federal Communications Commission (FCC) in Nord America e European Telecommunications Standard Institute (ETSI) in Europa. Le bande non licenziate (Bande Industrial Scientific and Medical (ISM)) sono allocate attorno ai 900 MHz e ai 2.4 GHz (80 MHz di banda fino a 2.40÷2.48 GHz) per le comunicazioni di utenti individuali. La banda a 2.4 GHz è disponibile "worldwide". Mentre FCC alloca sia la banda a 900 MHz che quella a 2.4 GHz, ETSI alloca solo la banda a 2.4 GHz (la banda a 900 MHz in Europa è usata per il GSM). Esse hanno un basso costo e un'alta interferenza. Per l'utilizzo della banda ISM si può usare la tecnica di Spread Spectrum (non più utilizzata), limitare la massima potenza trasmessa in banda e limitare le emissioni fuori banda. In Europa si usa anche la banda attorno ai 5 GHz per i sistemi HiperLan mentre in nord america questa banda è utilizzata come banda UNII. In questa banda c'è limite solo sull'uso della potenza. I vantaggi/svantaggi della banda a 5 GHz sono che pochi sistemi utilizzano la banda (minore interferenza, maggiore disponibilità e maggiore velocità nominale di trasmissione) e la frequenza portante è più elevata (maggiore attenuazione in spazio libero del segnale, maggiore potenza in trasmissione, ostacoli più opachi, a pari potenza trasmessa il raggio d'azione è inferiore rispetto ai sistemi a 2.4 GHz e c'è necessità di installare più AP (fattore 1.5)).
- Le reti wireless sono standardizzate da IEEE (Institute of Electrical and Electronics Engineers) sotto il comitato degli standard 802 LAN/MAN e in particolare nello standard 802.11. Nel luglio 97 nacque lo standard 802.11 legacy (emulazione dell'802.3 con 3 livelli fisici specificati per 1 e 2 Mbps). Nel settembre

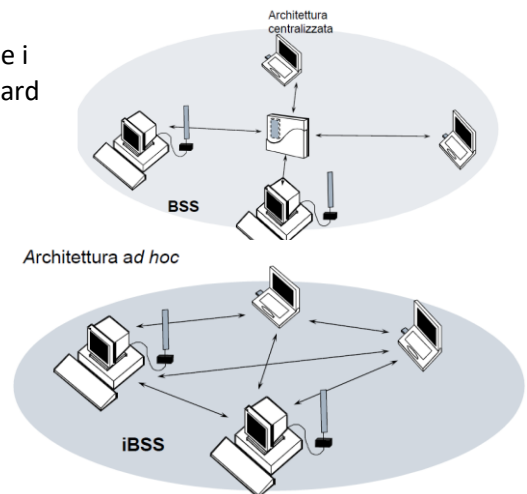
99 nacquero altri 2 livelli fisici a alto rate: 802.11a (da 6 a 54 Mbps in 5GHz band(OFDM)) e 802.11b (5.5 e 11Mbps in 2.4GHz band). Nel 2003 si arrivò a livelli fisici fino a 54 Mbit/s in 2.4GHz band: lo standard 802.11g. Nel 2004 nacque l'802.11h (802.11a compatibile con la regolamentazione dello spettro europeo in 5 GHz band). Negli anni dopo nacquero vari standard: 802.11i (miglioramento del framework di sicurezza), 802.11e (MAC avanzato con supporto QoS), 802.11n (alto tasso di rate fisico e MAC) e poi 802.11s (reti mesh), 802.11p (accesso WAVE-Wireless per l'ambiente veicolare), 802.11v (gestione rete senza fili), 802.11ac (very high throughput), 802.11af (White-Fi), 802.11ad (60 GHz che porta 7Gb/s ad alta velocità per streaming) e 802.11ah (800MHz per 8 MB/s per IoT).

- L'alleanza Wi-Fi (wireless fidelity) conta 500+ membri e oltre 350 prodotti certificati. La sua missione è certificare l'interoperabilità dei prodotti WLAN (802.11): Wi-Fi è il timbro di approvazione e si deve promuovere Wi-Fi come standard mondiale.
- Lo standard fornisce due modi di funzionamento: DCF (obbligatorio) (servizio best effort contention – usa CSMA con Collision Avoidance (CSMA/CA)) e PCF (opzionale) (la stazione base controlla l'accesso al mezzo - usa un meccanismo di votazione con maggiore accesso prioritario al mezzo, più tre tipi di frame: dati, controllo e gestione).



### WLAN: architettura di rete

- I componenti di una architettura di rete sono la stazione (STA), un punto di accesso (AP) (collegamento cablato/wireless), i BSS (Basic Service Set – può essere infrastruttura BSS (basata su infrastruttura) o BSS indipendente (IBSS) ad hoc), gli ESS (Extended Service Set – è un set di infrastrutture BSS e un set di punti di accesso collegato tramite un DS) e i DS (Sistema di distribuzione – non direttamente indirizzato nello standard – può essere cablato o senza fili).
- Il BSS è un set di stazioni (STAs) controllato dalla stessa “funzione di coordinamento” (funzione logica che gestisce l’accesso al canale condiviso). È simile al concetto di “cella” in reti radiomobili. Come detto prima esistono due tipi di BSS: infrastruttura BSS o BSS indipendente.
- In un sistema di distribuzione STA associa ad un, e solo un, AP attraverso una procedura di associazione. Essa è equivalente a collegare il cavo ethernet. Un ESS è una rete di livello 2, e quindi una singola sottorete IP con il proprio spazio di indirizzamento. Gli AP si comportano come un Ethernet bridge (switch di livello 2). Le tabelle di associazione vengono utilizzate per i processi di accoppiamento. Per esempio, i frame ricevuti tramite il DS e indicanti come destinazione un wireless STA vengono inoltrati all’interfaccia wireless una volta convertiti nel formato 802.11.



### WLAN: Medium Access Control

- I servizi del MAC sono accesso al canale, recovery dell'errore, frammentazione e riassemblaggio, salvataggio di energia, indirizzamento e framing.

L'accesso al mezzo di trasmissione è regolato dalle cosiddette “funzioni di coordinamento”. Sono definite due funzioni di coordinamento: Distributed Coordination Function (DCF) (basata su CSMA con backoff) e Point Coordination Function (PCF) (accesso libero da collisioni basato su polling).

Il recovery dell'errore è assolutamente necessario su un canale “rumoroso” (wireless): solo per trasmissioni unicast (il servizio di trasmissione è inaffidabile). Basato su una conferma positiva per frame ricevuto (“Stop & wait”) e richiede l'uso di timers di ritrasmissione.

Diversi intervalli di tempo regolano l'accesso al canale: esiste una spaziatura interframe. Questi sono intervalli di attesa minimi dopo l'ultimo e si basano sul meccanismo fisico carrier sensing.

Esistono 4 tipi di intervallo:

Short Inter Frame Spacing (SIFS): Le trasmissioni ad alta priorità possono iniziare dopo un SIFS della precedente trasmissione

PCF Inter Frame Spacing (PIFS): Spazio di interframe utilizzato per emettere frame di polling in modalità PCF

DCF Inter Frame Spacing (DIFS): La trasmissione regolare dei dati in modalità DCF può iniziare dopo un DIFS

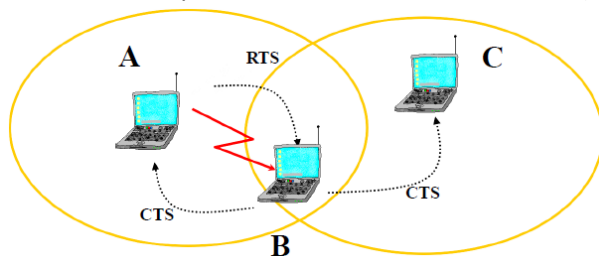
Extended Inter Frame Spacing (EIFS): Usato in casi speciali quando la trasmissione precedente non può essere decodificata.

DCF permette la coordinazione tra le stazioni senza l'esigenza di un'entità centrale di controllo. Esso può essere usato in una IBSS e in una infrastructure BSS. Esso è basato su Carrier Sense Multiple Access con Collision Avoidance (CSMA/CA): prima di cominciare una trasmissione, la stazione ascolta il canale e se il canale è inattivo (per meno di un DIFS): inizio trasmissione altrimenti se il canale è occupato c'è un'attesa e inizio backoff.

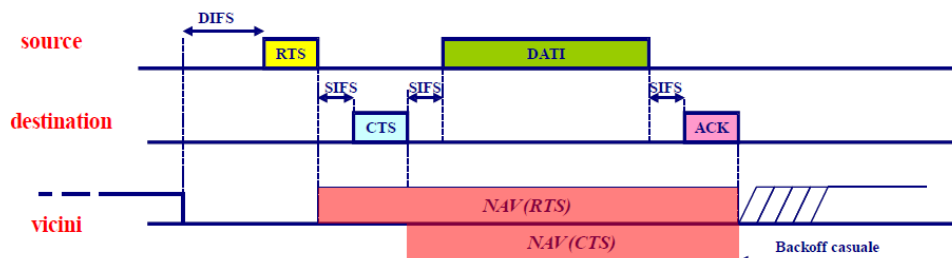
Prima di trasmettere, una stazione attende un periodo di tempo pari a un numero casuale di slot (backoff) + DIFS. Il numero casuale è uniforme tra 0 e CW (finestra di contesa). Se durante il backoff il canale diventa occupato, il conto alla rovescia degli slot viene fermato, e viene poi ripreso quando il canale ritorna inattivo. Se devono essere trasmessi pacchetti consecutivi, la procedura di backoff viene utilizzata tra i pacchetti anche quando il canale è inattivo. CW è impostato dinamicamente: se si verifica un errore/collisione=>circa il doppio CW fino a max 1023 slot, se la trasmissione è corretta CW=CWmin=31 slot.

La stazione trasmittente può recuperare frame danneggiati attraverso ritrasmissione. La risposta di trasmissione del ricevitore è basata su un "riconoscimento positivo". Si usano inoltre dei contatori di riprova (contatore Riprova breve (per frame "corto") e contatore Riprova lungo (per frame "lungo")).

Per risolvere il problema del terminale nascosto (terminale facente parte di due reti in cui ci sono due altri

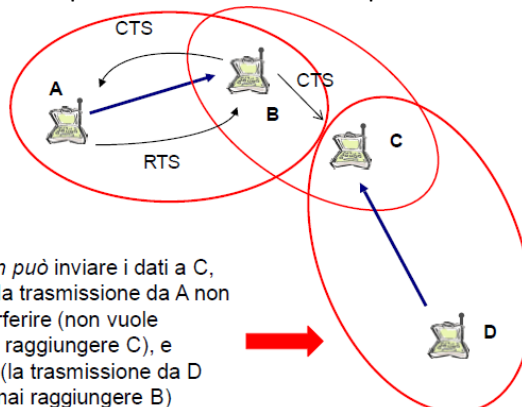


terminali che non si vedono tra loro) lo standard aggiunge un procedimento di carrier sensing logico (virtuale) al fisico. Sono usati dei frame di controllo, in cui viene codificato il cosiddetto «vettore di assegnazione di rete» (NAV). Il NAV contiene la durata della comunicazione che attualmente occupa il canale. Le stazioni mobili che ricevono tali frame di controllo



specificato nel NAV.  
frame di controllo:  
RTS=Request To Send  
CTS=Clear To Send  
Network allocation vector (NAV)

Si crea un altro problema: il terminale esposto:



Qui, D non può inviare i dati a C, anche se la trasmissione da A non vuole interferire (non vuole nemmeno raggiungere C), e viceversa (la trasmissione da D non vuol mai raggiungere B)

Lo scambio di frame di controllo riduce la capacità del canale. L'efficienza di trasmissione dipende da:

■ Qualità del canale

■ Dimensione frame dati

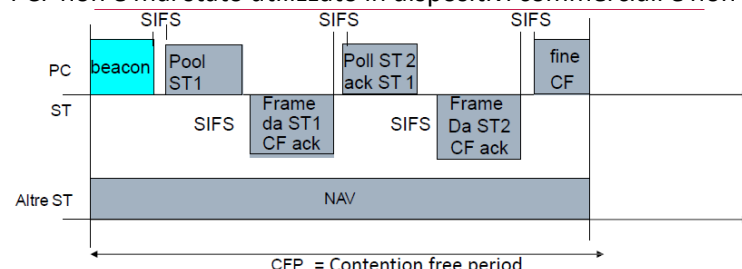
Lo standard 802.11 definisce un soglia (RTSThreshold) sulla dimensione (D) dei frame dati:

■ Se  $D < \text{RTSThreshold}$ , scambio RTS/CTS è NON usato

■ Se  $D > \text{RTSThreshold}$ , scambio RTS/CTS è usato

In CSMA, sul canale abbiamo cicli di periodo occupato (almeno una stazione sente il canale come occupato) e inattivo (tutte le stazioni sentono il canale libero). Il throughput S può essere dato da  $S = \frac{\alpha}{B+I}$  con B e I periodi di occupato medio e inattivo e  $\alpha$  probabilità che ci sia una trasmissione riuscita in un periodo occupato.

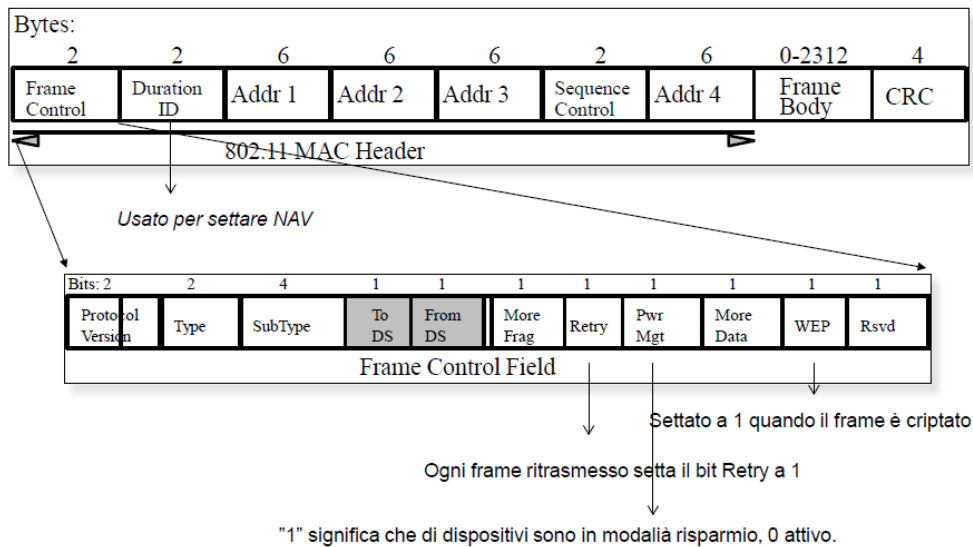
- PCF non è mai stato utilizzato in dispositivi commerciali e non può garantire QoS a causa di un paio di "errori".



In PCF c'è un imprevedibile intervallo inter-beacon e non ci sono vincoli sulla durata della trasmissione del frame.

## Sintassi del MAC 802.11

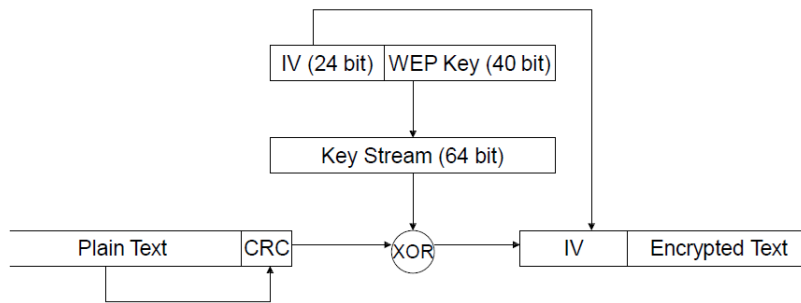
- L'approccio dello standard è quello di definire un unico MAC che supporti diversi livelli fisici con l'obiettivo di replicare funzionalità e servizi dell'ethernet. Il MAC 802.11 è complesso dal punto di vista sintattico per l'elevato numero di trame e per la complessità nell'interpretazione.



## Network Management

- Le procedure di Management delle reti sono lo scanning (individua BSS disponibili), l'autenticazione (autentica la stazione all'interno del BSS scelto), l'associazione (crea l'associazione STA/BSS), il power management (gestisce il risparmio di potenza) e la sincronizzazione (procedure per il corretto funzionamento del livello fisico).
- L'obiettivo dello scanning è di individuare un BSS a cui collegarsi. Non esiste questo metodo nelle reti cablate. L'operazione di scanning è effettuata dalla stazione. Sono definite due modalità di scanning: modalità passiva e modalità attiva. Nel passive scanning la stazione ascolta in sequenza tutti i canali disponibili e memorizza tutte le trame di beacon che riceve. Nell'active scanning per ogni canale disponibile, la stazione utilizza delle trame di Probe Request per sollecitare l'invio di una trama di beacon. Le trame di Probe Request possono essere sia unicast che broadcast. Alla fine della fase di scanning la stazione si costruisce un data base con una entry per ogni BSS individuato. Per ciascuna entry sono registrati BSSID, SSID, BSSType, frequenza dei beacon, info di sincronizzazione, info sul livello fisico e frequenza frame DTIM (gestione potenza). La scelta del BSS è fuori standard e dipende generalmente dall'implementazione (di solito si sceglie manualmente).
- La procedura dell'associazione equivale di fatto a connettere il cavo di rete alla presa di rete. A valle della procedura di associazione l'AP registra la stazione nel database di associazione e la STA può usare i servizi del Distribution System. Lo standard proibisce associazioni multiple. La procedura è iniziata dalla STA, poi avviene uno scambio di trame di management unicast e l'AP assegna alla STA un Association ID (AID) che la identifica univocamente.
- La procedura di Power Saving dipende dal tipo di BSS: nella infrastructure BSS si applicano le funzionalità di buffering nell'AP, le stazioni alternano periodi di sleep e di activity e l'AP segnala alle stazioni di attivarsi tramite informazione contenuta nelle trame di beacon, mentre nell'independent BSS non abbiamo un'efficienza pari a quella del caso infrastrutturato, c'è necessità di algoritmi distribuiti e generalmente non è usato.
- La sincronizzazione, nell'infrastructure BSS, è gestita dall'AP che inserisce un valore del proprio clock locale all'interno delle trame di beacon e di Probe Response. Nel caso di Independent BSS le STA si sincronizzano sul clock del primo che trasmette la trama di beacon.
- Nell'ambiente wireless il mezzo trasmissivo è condiviso. Potenzialmente ogni stazione dotata di un apparato ricetrasmittente standard compliant può accedere alla rete. C'è necessità di verificare l'identità delle stazioni accedenti e necessità di controllare l'accesso. Ci sono due tipi di approcci all'autenticazione: la Open System Authentication (obbligatoria) (vincoli blandi sull'accesso - l'AP autentica qualunque STA che ne faccia richiesta ma è poco sicura e c'è possibilità di applicare MAC Address Filtering) e la Shared Key Authentication (opzionale) (autenticazione basata sullo scambio di una chiave condivisa con due componenti: il meccanismo di challenge/response e l'algoritmo di crittografia a chiave privata basato su WEP (algoritmo di cifratura di tipo keystream basato su RC4 con keystream a 64 bit)).

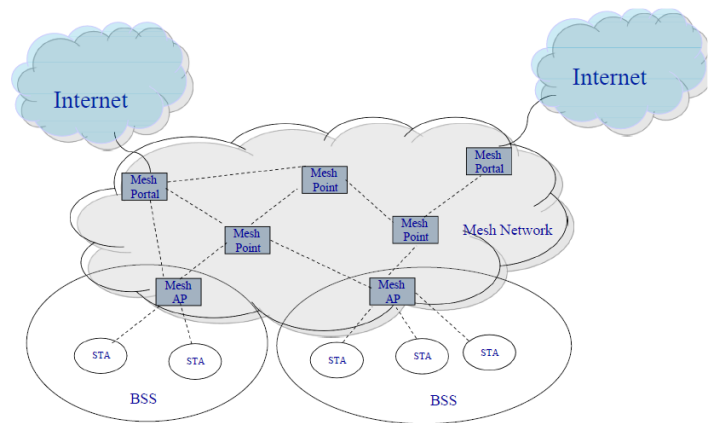




due debolezze del WEP sono che riusa la stessa WEP Key per diversi pacchetti cambiando solo l'IV ed è vulnerabile dal punto di vista dell'integrità (CRC debole). Come problemi di sicurezza dobbiamo controllare i problemi di autenticazione (solo le stazioni devono autenticarsi e non gli AP e l'approccio è vulnerabile ad attacchi di tipo man-in-

the-middle) e le problematiche di privacy (il WEP può essere violato in tempi ragionevoli). C'è necessità di paradigmi di autenticazione robusti e algoritmi di crittografia avanzati (che sono stati introdotti in 802.11i).

- Nel giugno 2004 si è concluso il lavoro su 802.11i: in questo standard le caratteristiche sono l'autenticazione demandata ai livelli superiori, l'introduzione di protocolli/infrastrutture per l'autenticazione e il miglioramento delle procedure di privacy e integrità. Si è inoltre introdotto il Wireless Protected Access (WPA1 e WPA2). Questo protocollo usa l'autenticazione del protocollo 802.1X (basata su Extensible Authentication Protocol (EAP)) e per garantire privacy usa il Temporary Key Integrity Protocol (TKIP) e il Counter Mode/CBC MAC Protocol (CCMP).
- Per estendere le dimensioni degli hotspot 802.11 tramite un'infrastruttura di tipo mesh e ampliare gli scenari applicativi della tecnologia WLAN le infrastrutture trovate in 802.11 sono state le infrastrutture decentralizzate e le reti magliate di Infrastructure BSS con gli AP connessi tramite un sistema di distribuzione wireless.



Gli scenari applicativi sono accesso residenziale (concorrenza con WiMax), gli uffici, le reti pubbliche di accesso a internet, le reti pubbliche di sicurezza e le reti militari.

Il TG 802.11s ha lo scopo di definire un Extended Service Set (ESS) per supportare servizi broadcast/multicast ed unicast in reti multihop. In esso abbiamo routing robusto ed efficiente (Mesh Topology Learning, Routing and Forwarding), sicurezza (Compatibilità con 802.11x), flessibilità del livello MAC (Mesh Measurement, Mesh Discovery and Association, Mesh Medium Access Coordination e Supporto alla QoS), trasparente ai livelli superiori e compatibilità con dispositivi legacy. Nelle reti mesh avviene qualche modifica a livello MAC e a livello di routing ma nessuna modifica a livello fisico. Molte aziende producono già dispositivi per l'implementazione delle reti mesh e tutte le soluzioni commerciali forniscono l'hardware e il software (proprietario) per implementare le reti mesh.

## WPAN

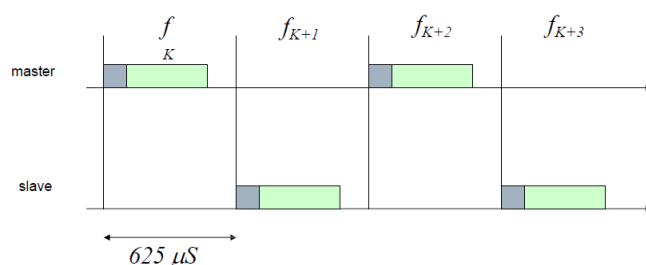
- Le Wireless Personal Area Network (WPANs) sono standardizzate nello standard 802.15 sono reti a corto raggio (piccole reti), a bassa energia, a basso costo e definite come "spazio operativo personale". Questo standard è nato in associazione alla nascita dello standard Bluetooth.

## Bluetooth

- Bluetooth è uno standard industriale per WPAN nato come progetto interno a Ericsson e poi nel '98 tramutato in Bluetooth Special Interest Group (SIG) a cui si aggiungono altre aziende nel '99. WG 802.15.1 adotta delle specifiche Bluetooth per i livelli 1 e 2.

Bluetooth è una tecnologia radio a basso costo e a corto raggio (10-20m) con complessità bassa, dimensione piccola e banda di trasmissione ISM a 2.4GHz. Solo i primi due livelli sono standardizzati da IEEE 802.15.1.

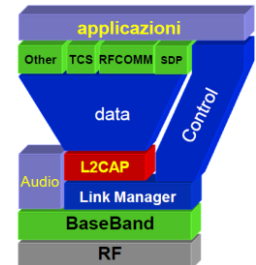
Gli scenari applicativi di Bluetooth sono cuffie, sincronizzazione dati e punti di accesso. A livello fisico si



adopera la banda ISM 2.4GHz con 79 canali distanziati di 1 MHz (2402-2480 MHz) e modulazione G-FSK (FSK gaussiana). Viene adoperato il salto di frequenza con 1600 salti/s e la sequenza FH (Frequency Hop) è pseudo casuale e definita dal clock e l'indirizzo della stazione master che regola l'accesso al canale. Gli altri dispositivi sono slave e seguono la sequenza  $f_k$  definita dal master.

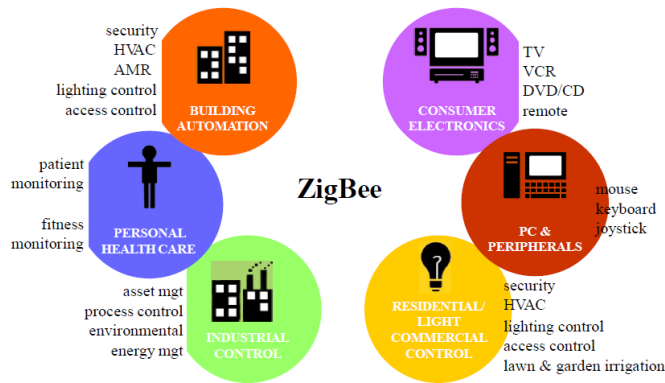
I pacchetti possono essere spalmati anche su 1, 3 o 5 slot (da 625 uS l'uno).

- Piconet è l'architettura semplice di una rete Bluetooth. Una Piconet è una rete ad hoc composta da 2 o più dispositivi di cui uno interviene come master e tutti gli altri come slave. La comunicazione è solo tra master e slave: gli slave non possono comunicare direttamente tra loro. Possono essere attivi fino a 7 slave e gli altri nodi possono essere in stand-by (non membri di piconet) o parcheggiati (ancora membri di piconet ma non attivi; fino a 256 slave massimo). Gli indirizzi usati in piconet sono indirizzi MAC a 48 bit, AMA (Active Member Address (3bit)-> massimo 8) e PMA (Parked Member Address (8bit)-> massimo 256).
- Bluetooth considera due tipi di connessioni: le SCO (Synchronous Connection Oriented – connessioni simmetriche, bidirezionali a portata fissa, facoltativamente FEC e di base con velocità 64 kbit/s) e le ACL (Asynchronous ConnectionLess – servizio di pacchetti tra master e slave sulla base di un meccanismo di polling, con diversi formati di pacchetto a disposizione e rate fino a 433,9 kbit/s simmetrici (usando 5 pacchetti di slot in entrambe le direzioni) e 723,2/57.6 kbit/s asimmetrici (usando 5 slot in una direzione e 1 slot nell'altra)).
- L'architettura del protocollo ha uno stack di protocollo non conforme al modello OSI (adottato da specifiche 802.15.1 con alcuni compromessi). Si usa un RF + Baseband equivalente a livello fisico + MAC e c'è un piano di controllo per creazione e gestione della connessione). Il formato del pacchetto BT include tre parti: un Codice d'accesso usato per la sincronizzazione e identificazione della piconet, un Intestazione che si usa per il link control (LC) e ARQ e un Payload per cui dipende il tipo di connessione e tipo di pacchetto.
- Gli stati in cui può trovarsi il link controller (responsabile del LC) sono: Stand-By (dispositivo disconnesso e radio off), Connection (dispositivo connesso con altri), Inquiry (dispositivo in cerca di altri dispositivi nel raggio d'azione), Inquiry Scan (dispositivo libero ma sente i possibili messaggi per intervalli brevi di tempo (basso duty cycle)), Page (il dispositivo sta provando a connettersi a uno specifico dispositivo) e Page Scan (simile a Inquiry Scan ma per i messaggi di Page).
- Se un dispositivo si vuole collegare ad un altro dispositivo, deve conoscere il suo indirizzo e poi iniziare la procedura Page. Dall'indirizzo può essere derivato il Device Access Code (DAC). Un dispositivo in stand-by entra periodicamente in scansione dello stato della pagina e ascolta per ricevere il suo DAC. Dovuto alla banda ISM, la procedura di Page non può essere eseguita su un canale fissato. Il dispositivo in Page scansionata segue una sequenza di sintonizzazione pseudo casuale su 32 canali. Per limitare il consumo di energia, il dispositivo esegue lo scan delle page per 10ms su un canale e poi va a dormire per alcuni secondi (da 1.28 a 3.85 s). In ogni scansione, un canale differente è usato in base alla sequenza di scansione pseudo-casuale. Il dispositivo di paging può calcolare la sequenza, ma solitamente non conosce il clock (la fase). Quindi trasmette il DAC a tutte le possibili frequenze sequenzialmente. In 10 ms, il dispositivo di paging può trasmettere il DAC su 16 dei 32 canali. La sequenza di trasmissione è ripetuta fino a che si riceve risposta. Se dopo un tempo di sleep nessuna risposta viene ricevuta, vengono considerati gli altri 16 canali. Il messaggio di risposta è lo stesso DAC. La connessione è stabilita in 2 tempi di sleep nel caso peggiore. Il dispositivo di paging risponde con un pacchetto FHS includendo tutte le informazioni del dispositivo, incluso indirizzo e clock. La connessione è quindi stabilita e il dispositivo di paging diventa Master e il dispositivo di scan diventa Slave.
- La procedura di inquiry permette di scoprire tutti gli altri dispositivi attivi nel raggio. È simile alla page procedure, ma l'Inquiry Access Code (IAC) è adottato al posto del DAC. Le collisioni possono avvenire a causa di più dispositivi nel range. Dopo un inquiry, il dispositivo passa a scan per instaurare la connessione. Tuttavia, poiché conosce il clock del dispositivo, il tempo di scansione è ridotto al minimo.
- Quando connesso, il dispositivo può opzionalmente entrare in modalità risparmio. Ci possono essere 3 stati: Hold (Lo slave smette di sentire il canale per un periodo di tempo deciso col master), Sniff (Lo slave alterna ascolto e sleep in accordo con un ciclo deciso col Master) e Park (in questo stato, lo slave rilascia il suo AMA (Active Member Address, preso nei due stati Hold e Sniff) e prende un PMA (Parked Member Address) dal master. Ascolta il canale con un duty cycle basso per ricevere il messaggio di unpark dal master.
- I dispositivi possono partecipare a varie piconet simultaneamente tramite la formazione Scatternet. Un dispositivo può essere Master solo in una piconet. I dispositivi possono passare da una piconet a un'altra usando le modalità hold e sniff. La formazione Scatternet e il routing sono fuori da specifiche standard. Scatternet permette, quando necessario, di creare collegamenti diretti.



## Zigbee

- La maggior parte delle applicazioni nelle reti wireless richiedono un tasso di trasmissione elevato. A partire dagli anni 90, un sacco di sforzi sono stati fatti per queste applicazioni e per le tecnologie wireless a alta velocità: WLAN (IEEE 802.11), Bluetooth (IEEE 802.15), WiMax (IEEE 802.16). Però, ci sono anche diverse



applicazioni che richiedono un raggio breve, un consumo basso di energia e bassa velocità. Le Low Rate WPAN (LR-WPAN) sono state considerate per questo segmento specifico di applicazioni. In queste WPAN abbiamo un basso costo hardware (<1 \$) e software, una bassa gamma di trasmissione (~10-30m), una bassa latenza, se necessario e, soprattutto, basso consumo di energia. A partire da metà anni '90, diversi produttori progettano soluzioni proprietarie per reti di sensori con evidente

compatibilità e problemi di costo elevato. Una attività di normazione si è resa necessaria: il Working Group 4 viene creato all'interno del progetto IEEE 802.15 (2001). Lo standard IEEE 802.15.4, considera i livelli fisici e MAC e viene pubblicato a maggio 2003. La tecnologia prende il nome commerciale di ZigBee.

- A differenza di Bluetooth, ZigBee sfrutta DSSS-11 chips/simbolo (mentre Bluetooth usa FHSS), 62.5 Ksimboli/s (contro 1M simboli/s) con 4 bits/simbolo e un picco del tasso di informazione di circa 128 Kbit/sec (contro i circa 720 Kbit/sec di Bluetooth). Il tempo di unione alla rete è di circa 30 ms (contro 3s di Bluetooth), gli slave dormienti

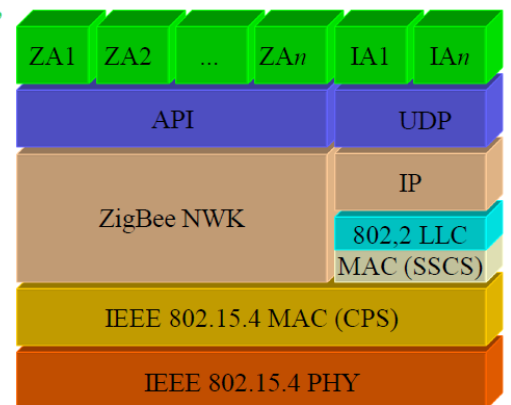
**Applicazioni di sviluppatori finali, progettate utilizzando profili di applicazione**

**Interfacce di applicazioni costruite usando profili generici**

**Gestione della topologia, gestione MAC, routing, protocolli di discovery, gestione della sicurezza**

**Accesso al canale, manutenzione PAN, trasporto dati affidabile**

**Trasmissione e ricezione sul canale radio fisico**



cambiano in attivo in 15ms (contro i 3s) e il tempo di accesso al canale per slave attivi è 15ms (contro i 2ms). Per ZigBee lo standard definisce due tipi di dispositivo: il Full Function Device (FFD – può trasmettere frame di beacon, direttamente comunicare con altri FFD, fare instradamento e agire come coordinatore PAN) e il Reduced Function Device (RFD – non può instradare traffico, non può comunicare direttamente con altri RFD e può comunicare direttamente con un FFD).

Per ZigBee sono definite inoltre 3 topologie: a stella (coordinatore PAN centrale e FFD e RFD attorno che comunicano solo con il coordinatore), a maglia (i RFD comunicano solo con un FFD e i FFD comunicano con altri FFD e con il coordinatore PAN) e ad albero a grappolo (il coordinatore PAN è la radice dell'albero e comunica con solo FFD e ogni RFD comunica con un FFD superiore. Quindi gli RFD sono foglie).

- A livello MAC ci sono due modalità di funzionamento di ZigBee: la Beacon Enabled (slotted CSMA/CA) e la Non Beacon Enabled (unslotted CSMA/CA). La prima modalità ha degli slot di tempo garantiti assegnati al frame di beacon e il coordinatore PAN potrebbe allocare fino a 7 di questi GTS (slot di tempo garantiti) e un GTS potrebbe occupare più periodi di slot. La durata della frame va dai 15ms ai 252ms. L'unità di tempo adottata è il periodo di ripristino (BP), normalmente pari a 20 simboli. Vengono adottate tre variabili: NB, il numero di tentativi di accesso per un pacchetto, CW, numero di BP liberi a attendere la fine del periodo di backoff prima di cominciare una trasmissione, e BE, esponente che definisce il numero massimo di BP richiesti prima di iniziare la procedura di CCA (Clear Channel Assessment). La trasmissione dei dati (e facoltativamente l'ack) deve terminare all'interno del CAP. Nel caso non sia possibile, MAC deve sospendere il backoff casuale e attendere l'inizio del prossimo CAP. Se il bit macBattLifeExt è impostato a 1, il conto alla rovescia del backoff può essere eseguito solo durante i primi 6 BP dopo il beacon.

Per la seconda modalità si usa lo schema di accesso classico CSMA/CA (dati - ACK) senza sincronizzazione. Le funzionalità dello strato MAC sono la gestione del beacon (sincronizzazione), la gestione del canale di accesso, la gestione slot di tempo garantiti, l'associazione e la dissociazione e il riconoscimento delle frame.

- Per la formazione della rete, un dispositivo FFD cerca un canale libero e seleziona un PANid (scansione canale). Poi si inizia a trasmettere il frame di beacon. Un dispositivo che vuole associarsi a una rete, scansiona il canale e ascolta i frame beacon. Una volta completa la scansione, una rete viene selezionata impostando i parametri di accesso secondo le informazioni nel frame beacon. L'associazione viene eseguita emettendo un Associate Request Command al coordinatore PAN. Il coordinatore PAN risponde con un Association Response Command.

- Analizzando lo ZigBee routing si trovano tre tipi di dispositivi: ZB Coordinator (FFD), ZB Router (FFD) e ZB End-Device (RFD o FFD). Il Routing è “zigbee oriented” e considera i due tipi di dispositivi fisici (FFD RFD). Il Routing usa due algoritmi: Ad-hoc On-demand Distance Vector (AODV) e Cluster Tree Algorithm. Ad-hoc On-demand Distance Vector è un semplice protocollo di instradamento on-demand in cui si vedono parti di reti ad hoc, mentre nel Cluster Tree Algorithm la creazione di un albero avviene in questo modo: la Procedura viene avviata da un FFD che funge da coordinatore della rete. Il coordinatore della rete seleziona uno dei canali disponibili (funzione MAC) e seleziona un PANidentifier alla rete e assegna a sé l’indirizzo di rete “0” (Coordinatore). Gli altri dispositivi possono adesso aderire alla rete associata al Coordinatore della rete. Essi possono agire come ZB Router (FFD) o ZB End-Device. Una volta connesso, lo ZB Router può quindi consentire agli altri dispositivi l’adesione alla rete. L’assegnazione dell’indirizzo è completamente distribuita e gerarchica.

## Reti ad hoc

- Le Mobile Ad Hoc Networks (MANET) sono reti di potenziali nodi di rete mobili dotati di interfacce di comunicazione wireless in cui non c’è nessuna infrastruttura prestabilita e la comunicazione tra peer coinvolge più salti. Ci sono alcune implicazioni: i nodi lavorano sia come host che come router e si ha una topologia a rete dinamica. Si può astrarre questo tipo di rete: ogni nodo può comunicare direttamente con un sottoinsieme di nodi mobili (vicini). Il “range” di comunicazione di un nodo varia in base ai cambiamenti fisici ed è visto come un cerchio. La Mobilità provoca cambiamenti di topologia: le modifiche alla topologia portano a cambiamenti nella consegna delle decisioni dei dati e si introduce l’adattamento dei requisiti in tempo reale. Alcune applicazioni d’esempio di queste reti sono le applicazioni di recupero dei disastri, di emergenza, di sicurezza (rinforzo della legge e recupero dei disastri naturali e artificiali), le applicazioni civili (reti per sale conferenze, collegamenti nelle grandi navi, PAN e reti veicolari) e le applicazioni militari (reti per campi di battaglia e per piattaforme ibride).
- Il Routing in reti ad hoc dovrebbe rappresentare la mobilità dell’host, che porta a topologie dinamiche. I protocolli di routing sono progettati per reti statiche (o lentamente mutevoli). Come al solito, nessun protocollo è ottimale per tutti i tipi e le condizioni delle reti ad hoc. Il protocollo viene suddiviso a sua volta in sotto-protocolli: protocolli reattivi (determinano i percorsi su richiesta), protocollo proattivi (mantengono i percorsi a prescindere dalle condizioni del traffico), protocolli ibridi (generalmente mantengono percorsi locali in modo proattivo, e creano percorsi reattivi su larga scala) e protocolli geografici (basati su posizione geografica dei nodi). I protocolli reattivi generalmente riguardano grandi ritardi tra la richiesta e la consegna del primo pacchetto e incorrono in basso overhead in scenari con poco traffico. Nei protocolli proattivi i pacchetti vengono immediatamente inviati su percorsi prestabiliti e i risultati nel sovraccarico di manutenzione del percorso sono elevati poiché i percorsi sono mantenuti indipendentemente dai modelli di traffico. I protocolli ibridi operano a metà strada tra prestazione di ritardo e di sovraccarico, mentre i protocolli geografici possono essere utilizzati solo quando le informazioni sulla posizione sono disponibili. Come caratteristiche per valutare il trade-off abbiamo una latenza nella scoperta del percorso (I protocolli proattivi possono avere una minore latenza poiché le rotte sono sempre mantenute, i protocolli reattivi possono avere maggiore latenza perché un percorso da X a Y sarà trovato solo quando X tenta di inviare a Y) e un overhead della scoperta/manutenzione del percorso (I protocolli reattivi possono avere minori costi poiché i percorsi sono determinati solo se necessario, mentre i protocolli proattivi possono (ma non necessariamente) risultare in alti overhead a causa dell’aggiornamento continuo del percorso). L’approccio che realizza un migliore trade-off dipende dal traffico e dai modelli di mobilità.
- Anche in queste reti c’è il flooding per la consegna dei dati: il mittente S invia a tutti i vicini il pacchetto dati P. Ogni nodo che riceve P inoltra P ai suoi vicini. Il numero di sequenza è usato per permettere la possibilità di inoltrare lo stesso pacchetto più di una volta. Il pacchetto P raggiunge la destinazione D a condizione che D sia raggiungibile da S. Il nodo D non inoltra il pacchetto.
- I vantaggi del flooding sono la semplicità, la potenziale maggior efficienza rispetto a altri protocolli quando il rate di trasmissione delle informazioni è sufficientemente basso da ridurre il sovraccarico della scoperta esplicita/manutenzione del percorso sostenuta da altri protocollo (Questo scenario può verificarsi, per esempio, quando i nodi trasmettono piccoli pacchetti di dati relativamente di rado, e molte topologie verificano i cambiamenti tra trasmissioni di pacchetti consecutivi) la potenzialmente più elevata affidabilità della consegna dei dati (Poiché i pacchetti possono essere spediti alla destinazione su percorsi multipli). Gli svantaggi sono che potenzialmente l’overhead è molto alto (I pacchetti di dati possono essere consegnati a troppi nodi che non hanno bisogno di riceverli), la potenziale minor affidabilità di consegna dei dati (Il flooding utilizza trasmissioni broadcast – difficile attuare una consegna broadcast affidabile senza aumentare significativamente i costi generali).

- Molti protocolli eseguono (potenziale limitazione) il flooding dei pacchetti di controllo, invece di pacchetti dati. I pacchetti di controllo sono usati per scoprire i percorsi e i percorsi scoperti sono successivamente utilizzati per inviare pacchetti dati. Il sovraccarico di pacchetti di controllo in flooding è ammortizzato sui pacchetti dati trasmessi tra flooding di pacchetti di controllo consecutivi.

### Protocolli reattivi

- Un esempio di protocollo reattivo è il Dynamic Source Routing (DSR): Quando il nodo S vuole inviare un pacchetto al nodo D, ma non sa un percorso per D, il nodo S avvia una scoperta del percorso. Il nodo mittente S inonda la richiesta di percorso (RREQ) e ogni nodo aggiunge il proprio identificatore quando inoltra RREQ. La destinazione D sulla ricezione del primo RREQ, invia una risposta del percorso (RREP). RREP è inviata su una rete ottenuta per retromarcia del percorso allegato al RREQ ricevuto. Il RREP comprende il percorso da S a D sulla quale RREQ è stato ricevuto dal nodo D.
- La risposta del percorso può essere inviata invertendo la rotta nel Route Request (RREQ) solo se i collegamenti sono garantiti per essere bidirezionali. A garantire ciò, RREQ dovrebbe essere inoltrato solo se ricevuto da un link che è conosciuto per essere bidirezionale. Se unidirezionali (asimmetrica) i collegamenti sono consentiti, quindi a RREP potrebbe essere necessario un route discovery per S da D, a meno che il nodo D sappia già un percorso per S. Se un route discovery è avviato da D per un rotta verso S, allora la Route Reply è piggybacked sulla Route Request da D. Il nodo S, quando riceve RREP, memorizza nella cache il percorso del RREP. Quando il nodo S invia un pacchetto dati a D, l'intero percorso è incluso nell'intestazione del pacchetto: da qui il nome source routing. I nodi intermedi usano il source route incluso nel pacchetto per determinare a chi un pacchetto dovrebbe essere inoltrato. (La dimensione dell'header del pacchetto cresce con la lunghezza del percorso). Bisogna eseguire una Route Discovery quando il nodo S vuole inviare dati al nodo D, ma non conosce un nodo valido del percorso D. Quando il nodo S impara che un percorso per il nodo D è rotto, utilizza un altro percorso dalla sua cache locale, se esiste nella cache. Altrimenti, il nodo S inizia la route discovery inviando una route request. Il nodo X sulla ricezione della richiesta di percorso per D può inviare un Route Reply se conosce una via per D. L'utilizzo della cache di percorso può accelerare la scoperta del percorso e ridurre la propagazione di richieste di percorso. Se un collegamento è rotto, il nodo precedente al collegamento invia un RERR (Route Error) al mittente lungo il percorso a ritroso e tutti i nodi che ricevono questo RERR aggiornano la cache eliminando il collegamento.
- Le cache non aggiornate possono influire negativamente sulle prestazioni. Con il passare del tempo e la mobilità degli host, i percorsi memorizzati nella cache possono diventare non validi e un host mittente può provare diverse rotte stantie (ottenute dalla cache locale o risposta dalla cache di altri nodi), prima di trovare una buona strada.

I vantaggi del DSR sono che i percorsi sono mantenuti solo tra nodi che devono comunicare (riduce overhead della manutenzione del percorso), che la cache dei percorsi può ulteriormente ridurre l'overhead della scoperta di percorsi e un'unica scoperta del percorso potrebbe produrre molte rotte per la destinazione, a causa di nodi intermedi che rispondono dalle cache locali.

Gli svantaggi di questo protocollo sono che le dimensioni dell'intestazione del pacchetto aumentano con la lunghezza del percorso a causa del routing di origine, che il flooding di richieste di percorso può potenzialmente raggiungere tutti i nodi della rete, che è necessario prestare attenzione per evitare collisioni tra le richieste di instradamento propagate dai nodi adiacenti e c'è aumento della contesa se troppe risposte di percorso tornano a causa della risposta dei nodi che utilizzano la cache locale. Inoltre, un nodo intermedio può inviare Route Reply utilizzando una route memorizzata nella cache, in modo da inquinare altre cache. Questo problema può essere facilitato se viene incorporato un meccanismo per eliminare (potenzialmente) percorsi memorizzati nella cache non validi.

- DSR include percorsi di origine nelle intestazioni dei pacchetti. Le intestazioni di grandi dimensioni risultanti possono a volte peggiorare le prestazioni (in particolare quando i contenuti dei dati di un pacchetto sono piccoli). AODV (Ad Hoc On-Demand Distance Vector Routing) tenta di migliorare il DSR mantenendo le tabelle di routing ai nodi, in modo che i pacchetti di dati non debbano contenere percorsi. AODV mantiene la caratteristica desiderabile del DSR che i percorsi vengono mantenuti solo tra i nodi che devono comunicare.

### Protocollo proattivi

- Un esempio di protocollo proattivo è Link State Routing: Ogni nodo periodicamente invia lo stato dei suoi collegamenti, ritrasmette informazioni sullo stato dei collegamenti ricevuti dal suo vicino, tiene traccia delle informazioni sullo stato dei collegamenti ricevute da altri nodi e utilizza le informazioni di cui sopra per determinare il salto successivo in ciascuna destinazione.
- Una versione più evoluta del LSR (Link State Routing) è l'Optimized Link State Routing: Il sovraccarico delle informazioni sul flooding dello stato del collegamento viene ridotto richiedendo meno nodi per l'inoltro delle



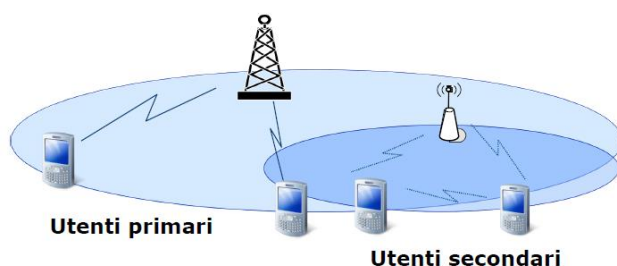
Informazioni. Una trasmissione dal nodo X viene inoltrata solo dai suoi ripetitori multipunto, che sono i suoi vicini, in modo tale che ciascun vicino a due hop di X è un vicino di almeno un hop di un ripetitore multipunto di X. OLSR riversa le informazioni attraverso i ripetitori multipunto. Le informazioni inondate sono per i collegamenti che collegano i nodi ai rispettivi ripetitori. Le rotte utilizzate da OLSR includono solo i ripetitori multipunto come nodi intermedi.

### Instradamento geografico

- Piuttosto che mantenere tabelle di routing e scoprire percorsi, si può anche usare la posizione geografica dei nodi: questo richiede che ogni nodo conosca la propria posizione (ad esempio, utilizzando il GPS) e la conoscenza di tutte le località vicine.  
Il Geographic Distance Routing (GEDIR) si basa sull'invio del pacchetto al vicino più vicino alla destinazione: funziona solo se i nodi sono densamente localizzati e ostacoli e bassa densità di nodi possono portare a problemi di routing.  
Per superare il problema di non trovare vicini più vicini, vengono proposti anche algoritmi di ricerca locale più estesi: Se bloccato, trasmetti una richiesta di individuazione del percorso con TTL di piccole dimensioni, e utilizza il percorso scoperto per l'inoltro dei dati.
- Una evoluzione del GEDIR nasce con un altro algoritmo di routing geografico: il Greedy Perimeter Stateless Routing (GPSR). Come GEDIR, si basa anch'esso su inoltro avido: Mantiene un elenco di vicini con le loro posizioni, invia il pacchetto al nodo più vicino alla destinazione (Most Forward in Radius - MFR) e evita loop di routing. Esso evita lacune di routing: usa il routing perimetrale e contrassegna la linea collegando il nodo intermedio con la destinazione, prendi l'hop a sinistra (in senso antiorario) e poi usa la regola della mano destra. Il routing perimetrale richiede che i grafici siano planari (nessun bordo nel grafico attraversa un altro bordo). Questo è realizzato attraverso algoritmi di planarizzazione.

### CRN

- Una notevole quantità di spettro fissato resta inutilizzata. Secondo la Federal Communication Commission, l'utilizzo dell'assegnazione fissata dello spettro è circa 15-85% basato su variazioni temporali e geografiche.
- Nelle reti radio cognitive (CRN) un utente primario (o con licenza) ha una licenza per operare in una determinata banda dello spettro; il suo accesso è generalmente controllato dall'operatore primario (PO) e non dovrebbe essere influenzato dalle operazioni di altri utenti senza licenza. Gli utenti senza licenza (secondari) non hanno licenza dello spettro, e attuano funzionalità aggiuntive per condividere la banda di frequenze con licenza senza interferire con gli utenti primari. Gli utenti Cognitive Radio (secondari) sono in grado di trasmettere su bande senza licenza (come la banda ISM) e bande di frequenza autorizzate (che sono condivise con utenti primari). Questo può aumentare considerevolmente la loro disponibilità di banda, e



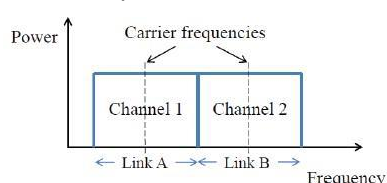
quindi la loro capacità di accedere a risorse remote, che potrebbero essere mobili.

In questa figura, una rete Cognitive Radio secondaria coesiste con la rete primaria (con licenza) nella stessa posizione e sulla stessa banda dello spettro. I buchi dello spettro inutilizzati esistono nella banda dello spettro con licenza. Gli utenti secondari (senza licenza) possono sfruttare questi buchi dello spettro

per comunicare tra loro o a una base station secondaria, per accedere a Internet. Le tecniche di comunicazione radio cognitiva devono essere utilizzate per limitare le interferenze verso gli utenti primari e tra utenti secondari stessi.

La questione più importante è evitare qualunque interferenza verso gli utenti primari. Per questo motivo, gli utenti secondari devono sempre ascoltare lo spettro occupato. Se un utente primario è rilevato, l'utente secondario deve passare immediatamente ad un nuovo spettro disponibile (se c'è) => Spectrum handoff.

- Lo spettro RF è una risorsa scarsa nei sistemi di comunicazione wireless. Lo sviluppo drammatico dell'industria delle telecomunicazioni mobili ha fatto sì che il FCC creasse lo spettro inutilizzato nelle bande TV (anche chiamate "White Space") disponibili per dispositivi wireless a banda larga senza licenza. Lo scenario TVWS (TV White Space) è composto da un database TV gestito da un Database Operator (DO) e una serie di dispositivi senza licenza / a bande TV (TVBDs). L'accesso allo spettro TVWS è spesso progettato senza



prender dentro gli account ACI. Tuttavia, ACI può verificarsi tra le trasmissioni di stazioni tv e TV Bands Devices (TVBDs) così come tra le diverse trasmissioni di TVBDs. Le ACI sono Adiacente-Channel interference e sono le interferenze tra canali vicini.

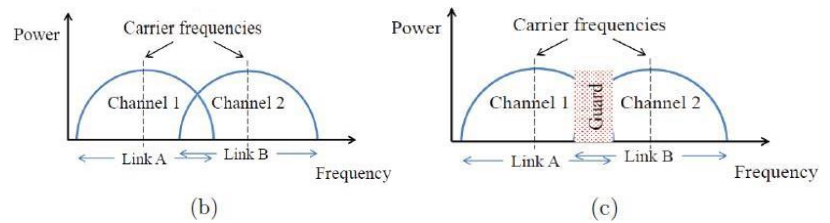
Nell'immagine a fianco la densità di spettro è di potenza ideale.



Nelle immagini di fianco si vede un PSD in un sistema di comunicazione pratico (b) e con "bande di guardia" (c).

Con riuso delle bande di guardia (GB): le GB possono esser condivise

da due interlocutori differenti. Se ho un non riuso di GB: due trasmissioni adiacenti richiedono i loro GB.



### Modelli di accesso multiplo – MAC Analysis

- Consideriamo uno scenario con  $N$  stazioni, in cui ogni stazione ha sempre un pacchetto pronto per la trasmissione e trasmette in uno slot con probabilità  $p$ . Se una stazione trasmette, la probabilità di successo è data dalla probabilità che le altre  $N-1$  non trasmettano:  $P_s = (1 - p)^{N-1}$ . La probabilità che in uno slot arbitrario una particolare stazione trasmetta e abbia successo è dunque uguale a  $p \cdot P_s = p(1 - p)^{N-1}$  e dunque la probabilità che una qualunque stazione trasmetta e abbia successo è  $S = Np(1 - p)^{N-1}$ . Questo è anche il numero medio di trasmissioni con successo in uno slot, che chiamiamo throughput ( $S$ ),  $0 \leq S \leq 1$ . Il numero medio di trasmissioni sul canale, che chiamiamo traffico ( $G$ ) è dato da:  $G = Np$ . Sostituendo nella formula del throughput  $p = G/N$  si ha  $S = G(1 - \frac{G}{N})^{N-1}$ . Questa formula ci dà il numero medio di successi in funzione del numero medio di trasmissioni. È dunque la frazione di slot utilizzati proficuamente. Il limite per  $N$  che tende ad infinito del throughput è noto ed è  $S = Ge^{-G}$ .

Per Aloha (non slottato) la collisione è più probabile, dunque l'efficienza è minore:  $S = Ge^{-2G}$ . se le trasmissioni sono in qualche modo sincronizzate (slotted Aloha) il periodo di vulnerabilità si riduce a  $T$  e quindi  $S = 2Ge^{-2G}$ .

