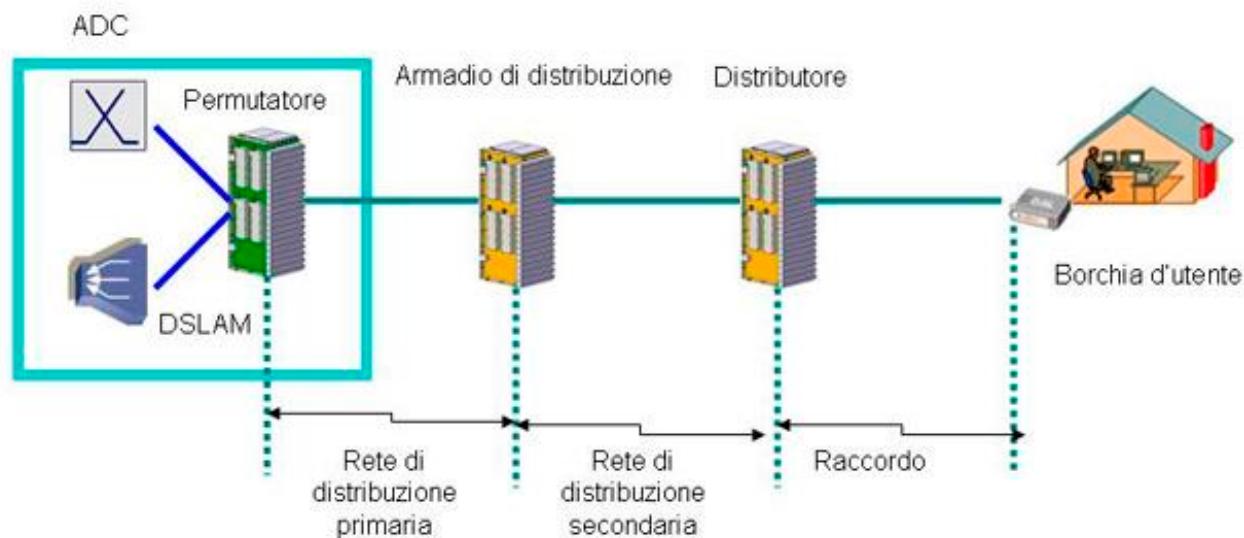


Appunti Sistemi e Servizi

Telecomunicazione

1.0 Reti di accesso Telefoniche



In telecomunicazioni con il termine rete di accesso si indica la parte di rete destinata al collegamento fra la sede dei singoli utenti finali fino alla prima centrale di commutazione e più in generale al collegamento tra un utente e il suo provider. La rete d'accesso rappresenta l'infrastruttura fissa che consente la connessione tra le centrali periferiche e l'utenza terminale. Viene anche chiamata rete di distribuzione oppure "**ultimo miglio**" (last mile) poiché distribuisce fisicamente il segnale ai vari utenti su distanze che nella maggior parte dei paesi copre distanze lineari di circa 2 km.

È costituita da un elevato numero di centrali terminali da cui partono cavi che assicurano una copertura capillare della relativa area geografica di competenza. In particolare, nella rete italiana, tali collegamenti sono realizzati prevalentemente attraverso cavi in rame, sostituiti negli ultimi anni, ove possibile, con fibra ottica.

Più precisamente la rete d'accesso è costituita dai collegamenti fisici (cavi) e da tutti quegli apparati che intervengono per il trasporto bidirezionale del segnale trasmisivo dalla centrale periferica al cliente.

Lo scopo della rete di accesso è quello di concentrare opportunamente i vari flussi di traffico generati dagli utenti terminali, prima che questi vengano immessi nella rete di giunzione. Proprio per la sua capillarità, la rete di accesso rappresenta la parte più complessa e costosa di tutta l'infrastruttura di rete. La rete d'accesso in rame può essere ulteriormente suddivisa in rete primaria e rete secondaria, come schematizzato in figura.

La "**rete primaria**" rappresenta quella parte della rete di distribuzione che va dal permutatore, presente nello stadio di linea, ad un terminale posto in posizione intermedia rispetto alla terminazione di utente detto **armadio di distribuzione** (o armadio ripartilinea). Tale tratta di rete è ad alta potenzialità in quanto dallo stadio di linea sono posati cavi contenenti fino ad 2400 coppie, i quali si diramano (con struttura ad albero) verso gli armadi di distribuzione su cui si attestano cavi da 400 coppie. Va precisato che per la rete di distribuzione primaria vi può essere la presenza di cavi aerei, anche se la loro quota è in genere minima e presente prevalentemente nelle aree rurali; la lunghezza media di una coppia nella rete primaria è di 1,1 Km.

La "**rete secondaria**" comprende invece il collegamento dall'armadio di distribuzione alla sede d'abbonato. In essa sono solitamente presenti ulteriori punti di flessibilità. Più precisamente la rete secondaria collega l'armadio di distribuzione con il distributore propriamente detto. La lunghezza media delle coppie della rete secondaria è 0,4 Km. Normalmente tale tratta di rete è a medio-bassa potenzialità (10-

400 coppie) e con tipologia di posa sia sotterranea che aerea. Le coppie del cavo secondario uscente dall'armadio sono distribuite mediante giunti, secondo una configurazione ad albero, in cavi di potenzialità inferiore che vanno a servire i distributori posizionati il più vicino possibile all'utenza da collegare. Sul distributore si attestano tipicamente cavi da 10 a 50 coppie. Le aree di influenza dell'armadio e del distributore prendono rispettivamente il nome di Area di Armadio ed Area del Distributore. Si definisce raccordo quella parte del collegamento che funge da rilegamento tra il distributore e l'utente.

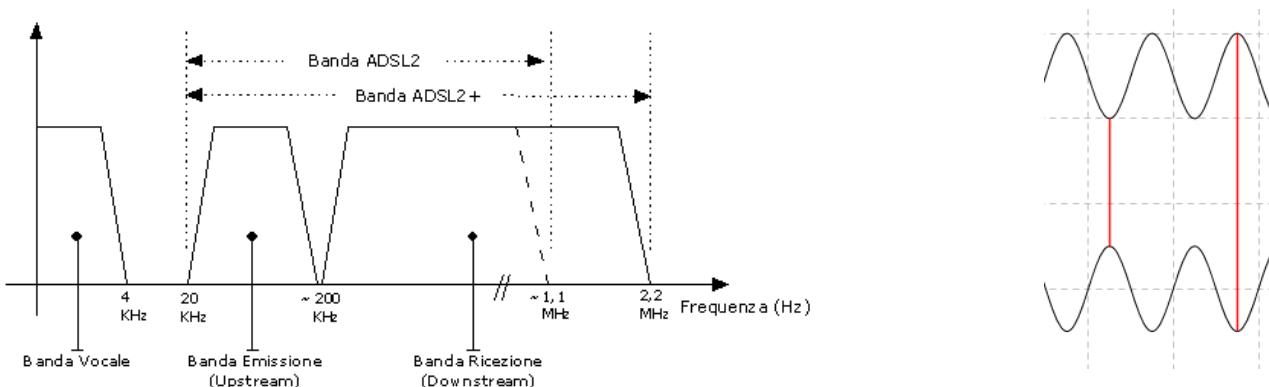
ADSL 2+

Il termine ADSL (sigla dell'inglese Asymmetric Digital Subscriber Line), nel campo delle telecomunicazioni, indica una classe di tecnologie di trasmissione a livello fisico, appartenenti a loro volta alla famiglia xDSL, utilizzate per l'accesso digitale a Internet ad alta velocità di trasmissione su doppino telefonico, cioè nell'ultimo miglio della rete telefonica (o rete di accesso). Nelle reti telefoniche pubbliche, il collegamento tra le utenze (le nostre abitazioni) e la centrale telefonica più vicina è chiamato **local loop**. Il local loop è nato inizialmente per trasportare un segnale analogico vocale e la scelta del mezzo di trasmissione è caduta sul doppino intrecciato: un cavo composto di due fili di rame con guaina di plastica intrecciati tra loro detto anche twisted pair. La scelta è dovuta al costo contenuto ed al fatto che la trasmissione vocale non richiede una banda elevata. Incomincio a utilizzare la banda a disposizione. La caratteristica centrale da considerare nell'uso di un mezzo di trasmissione è l'ampiezza di banda ovvero l'intervallo di frequenze che esso consente di trasmettere.

In informatica e in telecomunicazioni, il termine **banda** indica la quantità di dati informativi che possono essere trasferiti, attraverso una connessione, in un dato periodo di tempo.

Sullo stesso mezzo fisico, che in telefonia trasportava solo il segnale vocale, si trovano a viaggiare tre flussi di segnale separati. Vediamo di seguito la suddivisione delle frequenze:

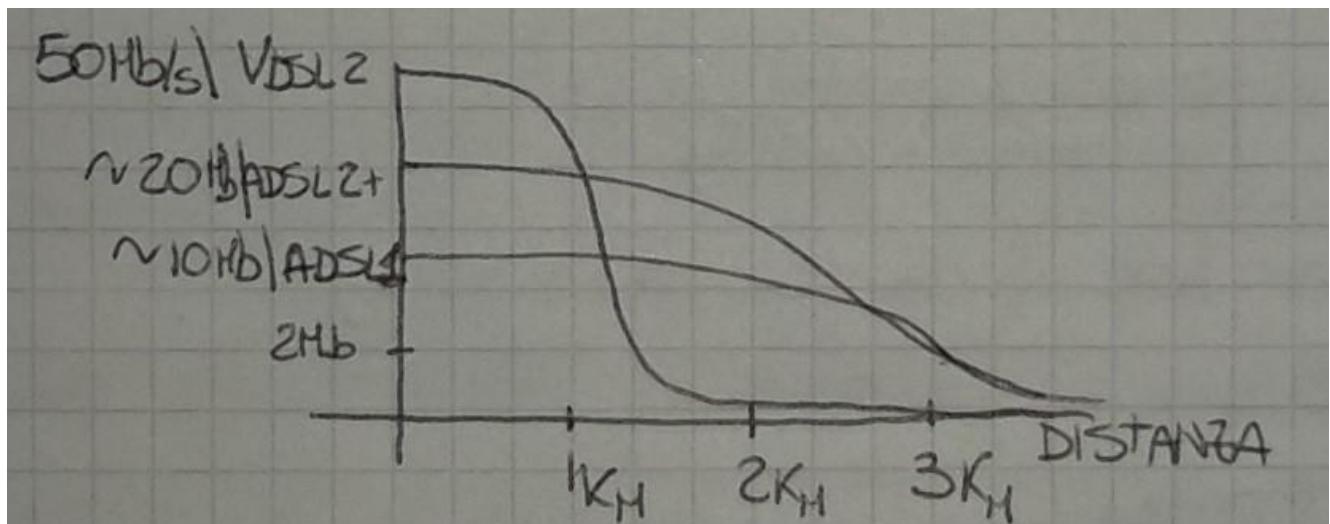
- canale Voce da 0 a 4KHz
- canale di trasmissione verso la rete da 25 a 138 KHz (**UPSTREAM**)
- canale ricezione dalla rete da 138KHz a 2.2 MHz circa (**DOWNSTREAM**)



I doppini di rame sono attorcigliati. Posso avere delle interferenze, e se ho delle controfasi, si annulla il segnale. Ci possono essere segnali che si disperdoni. Il segnale vocale trasmesso sul local loop copre l'intervallo da 0 a 4Khz. La banda disponibile sul doppino è più ampia ma dipende a sua volta dalla sua lunghezza, più un terminale è distante dalla propria centrale, più il cavo è lungo e il segnale subisce un deterioramento. Riducendo le distanze, le velocità crescono. La velocità di trasmissione (o di trasferimento detta anche frequenza di cifra o bit-rate) indica la quantità di dati digitali che possono essere trasferiti, attraverso una connessione/trasmissione, su un canale di comunicazione in un dato intervallo di tempo ovvero:

$$R = \frac{\text{quantità delle informazioni}}{\text{tempo di trasferimento}}$$

Quando la distanza è piccola, la differenza di velocità di trasmissione è forte. Con l'aumentare della distanza, la differenza di velocità diminuisce. Se siamo vicini alla centrale, avremo una differenza di velocità alta se facessimo il confronto tra una adsl a 24 Mb/s e una a 12 Mb/s.



Come posso migliorare?

- VDSL: standard più moderno, ma funziona su distanze molto più brevi. Le elaborazioni dei segnali sono più sofisticate. Questo è il motivo per cui è sofisticato.
- VDSL2: occupa una banda pari a 30 MHz. A seconda della distanza, può arrivare a una velocità di trasferimento pari a 50 Mb/s in downstream. La velocità a 50 Mb/s si ha entro un chilometro di lunghezza di cavo.

Lo schema di prima non va più bene e per ovviare al problema della distanza, si utilizza l'FTTC (fiber to the cabinet).

Bonding o pairing

Legare o accoppiare i doppini in modo da avere una migliore performance. Moltiplico la capacità per il numero di doppini.

Vectoring

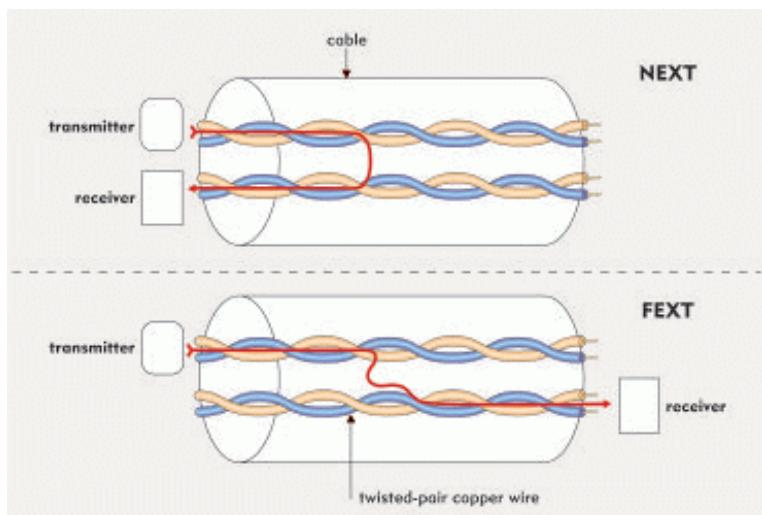
Si tratta di una nuova tecnologia che consente di migliorare di molto le prestazioni della rete di rame in fatto di trasmissione dati, portandole fino a 100 Mega e oltre laddove il cliente si trovi a non più di 400 metri dall'armadio della compagnia fornitrice. Sotto i 30 metri posso avere la velocità di 500 Mb/s. Lo standard che permette di fare questo è il **G FAST**. G fast è uno standard che abilita velocità di trasmissione tra 200 Mbit/s e 500 Mbit/s. In speciali circostanze la velocità può raggiungere 1 Gbit/s. Le alte velocità sono raggiungibili su distanze molto brevi (meno di 250 metri).

CROSSTALK (DIAFONIA) E FEXT E NEXT

In telecomunicazioni ed elettronica con il termine intonazione , anche detta crosstalk o cross-talk, si indica il rumore o interferenza elettromagnetica che si può generare tra due cavi vicini di un circuito o di un apparato elettronico. La causa è il campo elettromagnetico tempo-variabile che si genera attorno a un cavo in cui passa corrente non costante (segnale) generando uno scambio di energia da una linea all'altra, all'interno dello stesso conduttore, creando un disturbo indesiderato (la diafonia appunto).

Supponiamo di avere due linee di trasmissione; ho due disturbi:

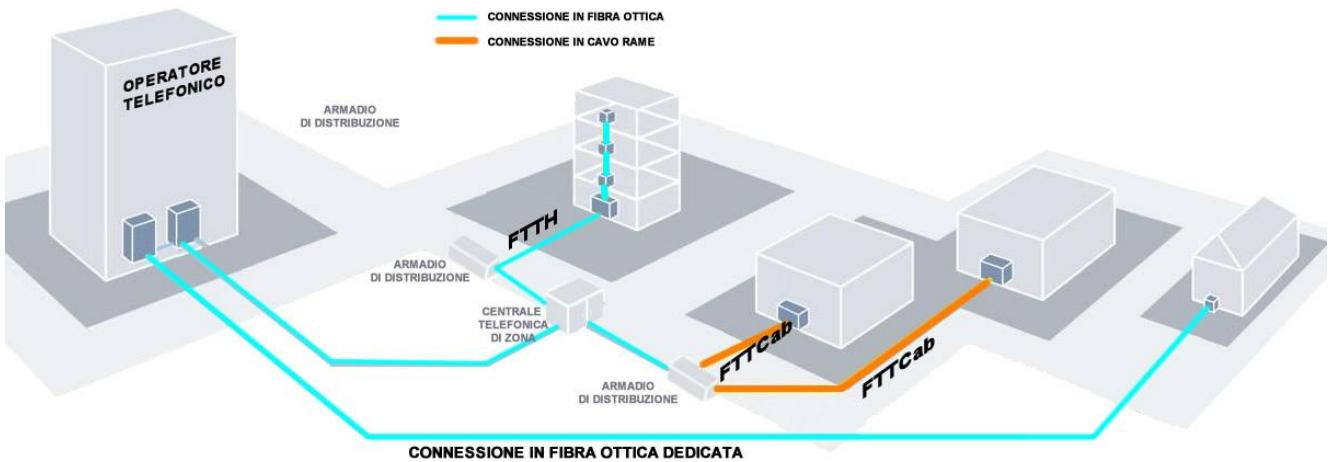
- **Next** è il rumore che il mio trasmettitore dà al mio ricevitore
- **Fext** è il rumore che il mio trasmettitore dà al ricevitore dalla parte opposta del trasmettitore



2.0 Reti in fibra

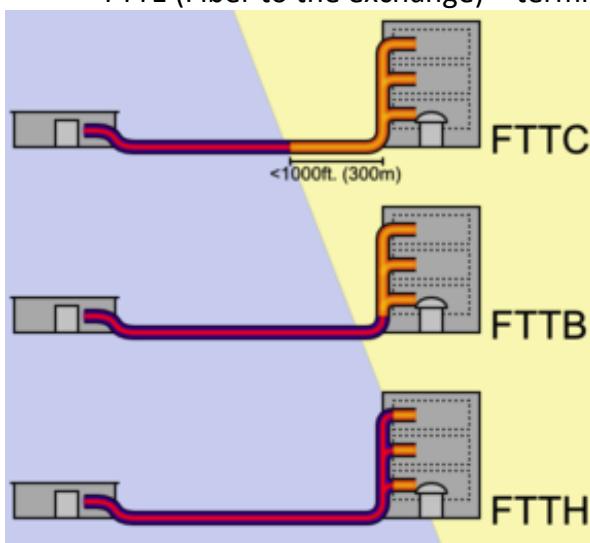
FTTx e la FIBRA

L'acronimo inglese FTTx (Fiber To The x, dove la x indica un elemento dell'infrastruttura di rete come Home, "casa", o Cabinet, "armadio di zona") indica un'architettura di rete di telecomunicazioni a banda larga che utilizza la fibra ottica per la sostituzione parziale o completa del tradizionale doppino in rame utilizzato nel cosiddetto ultimo miglio della rete di accesso. Con il fiber to the cabinet (FTTC) la fibra ottica è portata sino all'armadio stradale, ultima "centrale" di gestione e smistamento dell'infrastruttura telecomunicativa prima che il cavo venga portato alle singole abitazioni. Nella distanza centrale – cabina abbiamo la fibra, ma dopo nella distanza cabina–casa abbiamo il doppino di rame. Perché non fare anche la distanza cabina – casa in fibra? Per problemi di costi; dalla centrale alla cabina, i costi sono 20, mentre dalla cabina a casa, i costi sono 80.



Altre tipologie di FTTx sono:

- FTTCab o FTTC (Fiber to the Cabinet) – terminazione della fibra ottica all'interno del ripartilinea stradale.
- FTTB (Fibert to the Building) – terminazione della fibra ottica presso l'edificio dell'utente. In verticale la fibra non può arrivare. Se prendo un filo di rame, questo continua a funzionare e le informazioni arrivano a destinazione, mentre la fibra no.
- FTTH (Fibert to the Home) – terminazione della fibra a casa dell'utente – tutto il circuito è in fibra.
- FTTE (Fiber to the exchange) – terminazione della fibra fino alla centrale



Cosa dice Shannon? $C = B * \log_2(1 + \frac{S}{N})$

Dove:

- B = banda del canale
- C = capacità del canale
- S = potenza del segnale
- N = rumore (noise)

Non si può avere potenza infinita per la trasmissione. Il vantaggio della fibra è che **B** è grande e **N** è inesistente. Sul doppino di rame **B** è limitato. **N** è abbastanza elevato (rumore). Se ho un cavo in fibra e lo devo congiungere con un altro cavo in fibra, devo utilizzare apparecchi specifici e competenze. La fibra deve essere fusa e allineata con precisione. Questo spiega i costi elevati.

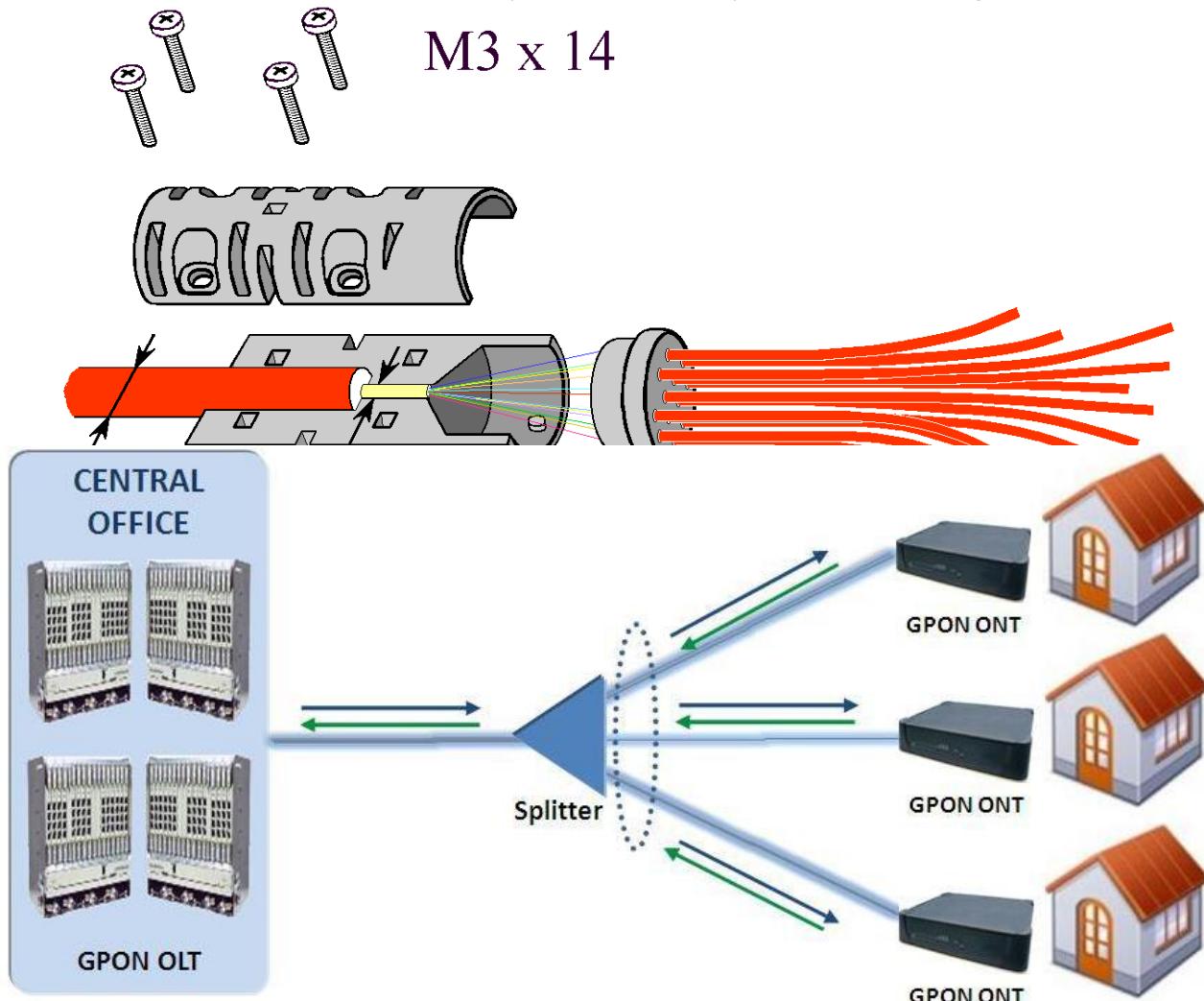
GPON

Il programma Fiber to The Home (FTTH) è ampiamente riconosciuto come soluzione ottimale per la fornitura di banda larga a comunità nuove e già esistenti. A differenza dei servizi xDSL e via cavo che sfruttano le linee telefoniche, il FTTH prevede l'installazione di fibra ottica da una centrale verso singole utenze.

Una **PON** (Passive Optical Network) è una rete ottica, priva di elementi attivi nel percorso da sorgente a destinazione e utilizzata di solito in configurazioni point-to-multipoint. È costituita da un **OLT** (Optical Line Terminal) e da N **ONU** (Optical Network Unit o **ONT** (Optical Network Termination)). Il primo funziona da interfaccia tra la PON e la rete di backbone, mentre le seconde da interfaccia con gli utenti.

Tra le diverse tipologie di PON, troviamo la GPON. La **GPON** (Gigabit Passive Optical Network), fornisce un'ampiezza di banda senza precedenti (fino a 2,5 Gb/s di velocità di downstream, condivisa da un massimo di 128 edifici) e una maggiore distanza dalla centrale (da 20 a 40 chilometri, invece di 4~5 chilometri per la DSL), consentendo ai provider di servizi di abilitare applicazioni a uso intensivo di larghezza di banda e stabilire una posizione strategica a lungo termine nel mercato della banda larga.

GPON utilizza una topologia punto-multipunto. Per separare e instradare la fibra verso diversi edifici viene utilizzato uno splitter passivo, riducendo così la quantità di fibra e di apparecchiature necessarie per la centrale rispetto alle architetture punto-punto. Lo splitter divide il cavo di fibra in sottocavi di fibra; splitto la fibra ottica fino a 128 optical unit. La natura passiva di GPON elimina l'impiego della corrente elettrica, rendendo possibile l'installazione dello splitter in luoghi dove non è facile avere l'alimentazione. Inoltre, è più efficiente dal punto di vista energetico.



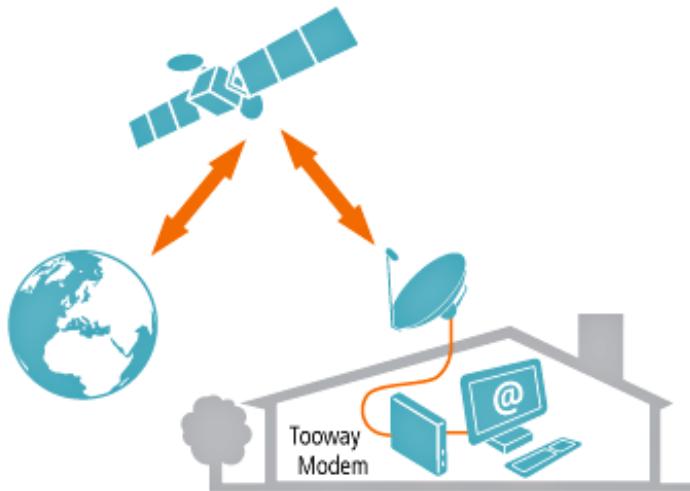
IL GPON presenta problemi di sicurezza e privacy. Non ci sono modelli di crittografia dei dati. Nessuno ha ancora inventato qualcosa che eviti la possibilità a qualcun altro di intromettersi nella rete e introdurre un segnale di disturbo nella rete in fibra.

WDM - PON

I sistemi WDM (Wave Division Multiplexing) hanno costi accettabili. Una frequenza o lunghezza d'onda viene assegnata a un operatore e un'altra a un altro operatore. Questo per poter condividere la pon. La capacità viene moltiplicata per il numero di frequenze che utilizzo.

3.0 Reti che sfruttano onde radio

Il divario digitale o digital divide è il divario esistente tra chi ha accesso effettivo alle tecnologie dell'informazione e chi ne è escluso, in modo parziale o totale. Il termine digital divide può essere utilizzato sia per riferirsi ad un divario esistente tra diverse persone, o gruppi sociali in una stessa area, che al divario esistente tra diverse regioni di uno stesso stato, o tra stati (o regioni del mondo) a livello globale. Io non riesco ad avere buone prestazioni o addirittura nulla. Per queste persone i cavi fanno fatica ad arrivare fisicamente e quindi si utilizza il segnale radio: **satellite**.



RETE SATELLITARE

La grandezza della parabola dipende dalla banda. I satelliti hanno varie bande:

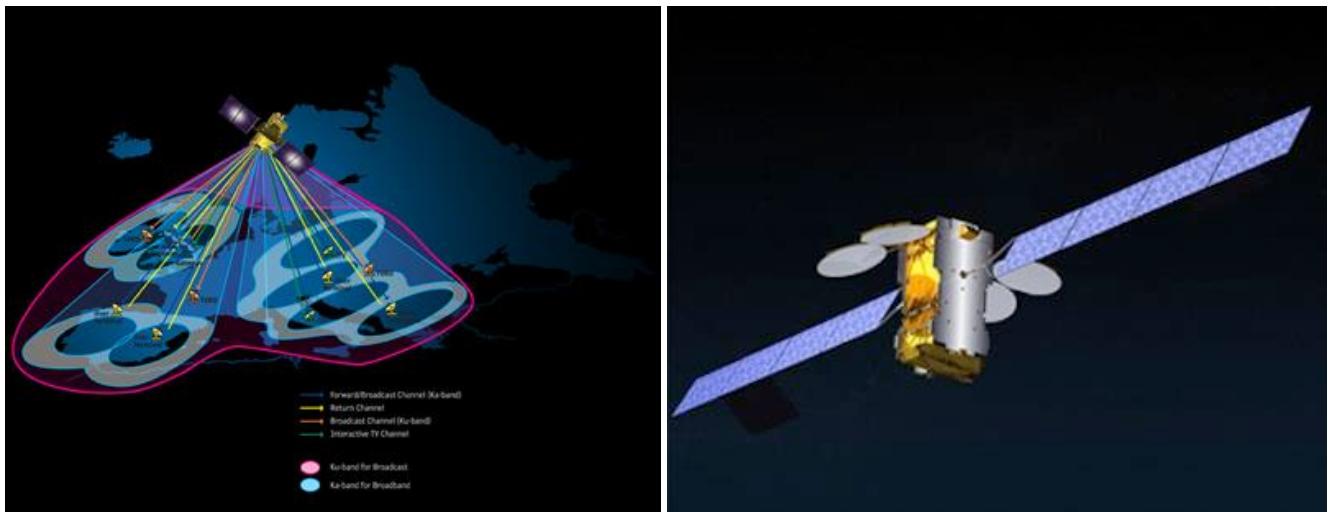
- **C BAND:** 4 – 16 GHz
- **Ku BAND:** 11 – 14 GHz
- **Ka BAND:** 20 – 30 GHz

I satelliti sono di tre tipologie:

- **GEO** (geostazionari): stanno a una altezza di 35.800 km di quota. Utilizzati per la Tv, internet... Viene utilizzata la Ku e Ka BAND.
- **MEO** (orbita media): utilizzati per la geolocalizzazione. Stanno tra i 5.000 km e i 13.000 km. L'Europa sta lanciando i satelliti per il sistema di geolocalizzazione Galileo.

- **LEO** (orbita bassa): utilizzati per scopi militari. Hanno un ritardo molto basso (5 ms) in quanto sono in orbita bassa e sono a distanza minore dalla terra. Se sono in basso, ovviamente coprono un'area molto più piccola rispetto ai satelliti che stanno a media e alta orbita.

Al giorno d'oggi è arrivata una nuova generazione di **satelliti geostazionari ka band multibeam** (multibeam=che ha più antenne). Questa generazione di satelliti ha più antenne che coprono aree separate diverse. Ex il satellite KA SA7 Telsat ha 80 antenne. La velocità è di 900 Mb/s

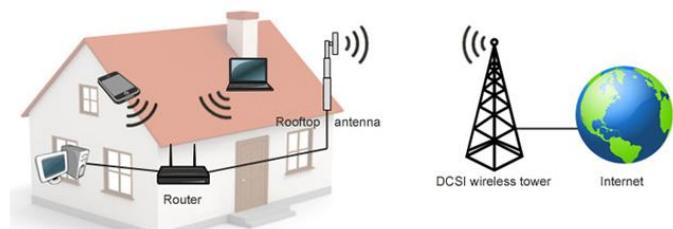


FWA

Tra le altre soluzioni per vincere il digital divide, abbiamo l'**FWA**.

L'**FWA**: è acronimo di **Fixed Wireless Access** e indica un insieme di sistemi di trasmissione sviluppati per sfruttare determinate frequenze dello **spettro radio** allo scopo di fornire servizi di connettività a **Internet a banda larga** con velocità di connessione nominali pari a **1 Gbps**. La tecnologia FWA viene utilizzata per collegare due luoghi (due palazzi o una torre e un palazzo) tramite onde radio. L'obiettivo di questa tecnologia, è quella di abilitare la comunicazione tra due i due siti e/o edifici. Solitamente questa tecnologia è una valida alternativa alla fibra e all'installazione di cavi, in termini di costi. La tecnologia FWA ha il vantaggio che permette di connettere utenti che si trovano in aree remote. Esistono tre soluzioni FWA:

- Wi - Fi, adotta gli standard IEEE 802.11 a e 802.11 n, sfrutta frequenze di 2.4 GHz e 5GHz. Questa tecnologia è una tecnologia più domestica e può essere spesso trovata nelle reti di casa, negli uffici...
- Il WI-MAX, adotta lo standard 802.16, che utilizza frequenze sui 3.5 GHz. Sono frequenze licenziate (frequenze ottenute da un operatore in seguito a un pagamento verso lo stato). Le distanze coperte sono in condizioni buone fino a 15 Km. Ci deve essere una buona visibilità (disturbi...).



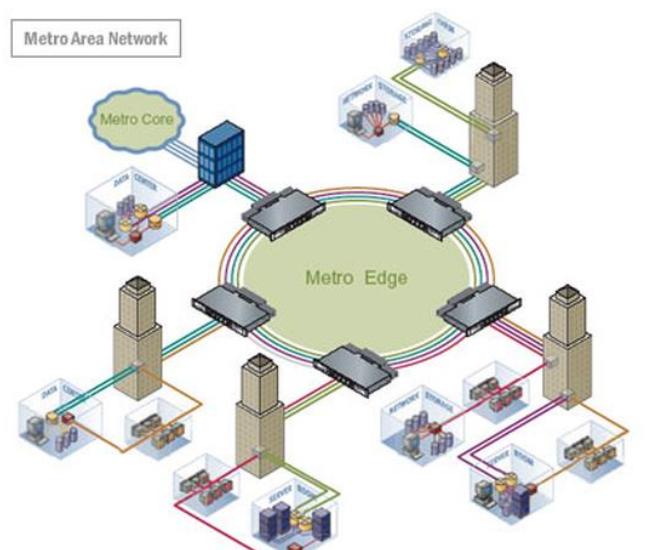
POWER LINE

I dispositivi Powerline sono degli adattatori – solitamente venduti in coppia diffondono il segnale Internet utilizzando i cavi dell'elettricità e permettono di “coprire” le aree della casa che normalmente non sono raggiunte dal segnale del router.

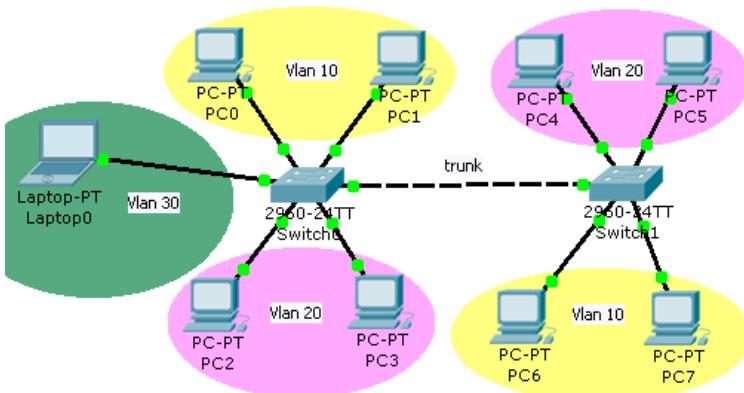
4.0 Reti metropolitane



Analizziamo ora la rete metropolitana. La rete MAN (Metropolitan Area Network) è una rete che copre delle distanze metropolitane, cioè in un'area urbana di grande dimensioni o dislocate tra paesi vicini e distanti pochi chilometri. I computer sono interconnessi tra loro e collegati a un server centrale nell'intero territorio comunale o metropolitano. Nella rete metropolitana, troviamo gli switch (scatole in grigio) che formano 2 o tre livelli e rappresentano migliaia di nodi. Più saliamo di livello e più diminuisce il numero degli switch. Gli switch al secondo livello son chiamati **fiber node**, mentre quelli al terzo livello son chiamati **metropolitan node** e sono collegati alla dorsale (backbone).



5.0 VLAN



Una VLAN (Virtual LAN) è una rete LAN realizzata logicamente, isolata quindi virtualmente ma non fisicamente, da altre LAN Virtuali. La VLAN permette di avere un'infrastruttura fisica unica, su cui coesistono più reti logiche. Io posso attaccare qualsiasi dispositivo e decidere a quale VLAN annetterlo.

Vantaggi VLAN

È possibile, ad esempio, definire diverse VLAN all'interno di un unico switch, oppure dislocare la stessa Virtual LAN su diversi switch. Una Virtual LAN, quindi, consente di:

- Separare host appartenenti allo stesso dominio di broadcast;
- Connettere host separati fisicamente, alla stessa rete logica virtuale.

Ciascuna VLAN si comporta come una LAN separata dalle altre, e per la loro interconnessione si utilizza routing. I vantaggi della VLAN:

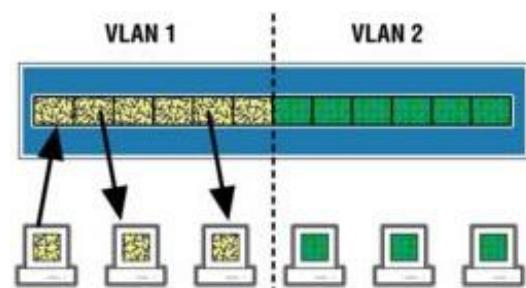
- **Risparmio:** Si realizzano LAN Virtuali sulle **stesse strutture fisiche**, con notevole **risparmio di tempo e di denaro**.
- **Aumento sicurezza:** Gli host possono vedere solamente il **traffico della loro VLAN**, e non quello delle altre.
- **Aumento prestazioni:** I frame non vengono propagati verso destinazioni non necessarie, grazie al confinamento del traffico broadcast alla singola VLAN.
- **Flessibilità:**
 - Spostamento fisico di host: l'host rimane collegato alla stessa Virtual LAN, senza riconfigurare gli switch.
 - Spostamento fisico di un utente nell'infrastruttura di rete: l'utente può rimanere assegnato ad una Virtual LAN, dopo un'opportuna riconfigurazione degli apparati.

Come realizzare una VLAN

Ci sono due modi per realizzare una Virtual LAN:

- **Port Based (Private VLAN):** lo switch assegna una VLAN a delle porte (immagine accanto);
- **Tagged (802.1Q):** lo switch associa un indirizzo IP/MAC ad una VLAN.

Le VLAN si definiscono all'interno dello switch, attraverso un Nome e un ID (VID: VLAN Identifier), quest'ultimo



con range 1-1005, e un blocco di indirizzi. Per gestire più VLAN sulla stessa struttura fisica, lo switch deve essere in grado di svolgere funzioni di:

- **Ingress**: capire la VLAN di provenienza del frame;
- **Forwarding**: capire la porta di destinazione del frame, in base alla VLAN di destinazione;
- **Egress**: trasmettere il frame in modo che la sua appartenenza alla VLAN venga correttamente interpretata da altri eventuali switch.

Standard 802.1Q

IEEE 802.1Q è uno standard che permette a più reti virtuali VLAN di condividere lo stesso collegamento fisico senza perdita di informazioni tra un apparato e un altro. 802.1Q non incapsula il frame originale, ma aggiunge 4 byte all'header.

- I primi 2 byte modificati riguardano il tag protocol identifier TPID. Questo contiene il tag EtherType che viene cambiato in 0x8100, numero che evidenzia il nuovo formato del frame.
- I successivi 2 byte riguardano il tag control information TCI (detto anche VLAN Tag) così suddiviso:
 - **user_priority**: Questo campo a 3 bit può essere utilizzato per indicare un livello di priorità per il frame. L'utilizzo di questo campo è definito in: IEEE 802.1p.
 - **CFI**: Campo di 1 bit che indica se i MAC address nel frame sono in forma canonica.
 - **VID**: campo di 12 bit che indica l'ID delle VLAN, che possono così essere fino a 4096 (ossia 2^{12}). Di queste, la prima (VLAN 0) e l'ultima (VLAN 4095) sono riservate, quindi gli ID realmente usabili sono 4094.

Il resto del frame Ethernet rimane identico all'originale.

6.0 Modello Internet

Connettività generalizzata:

- Tutti parlano con tutti
- Risorse condivise
- Instradamento effettuato con un unico principio

Connettività dedicata:

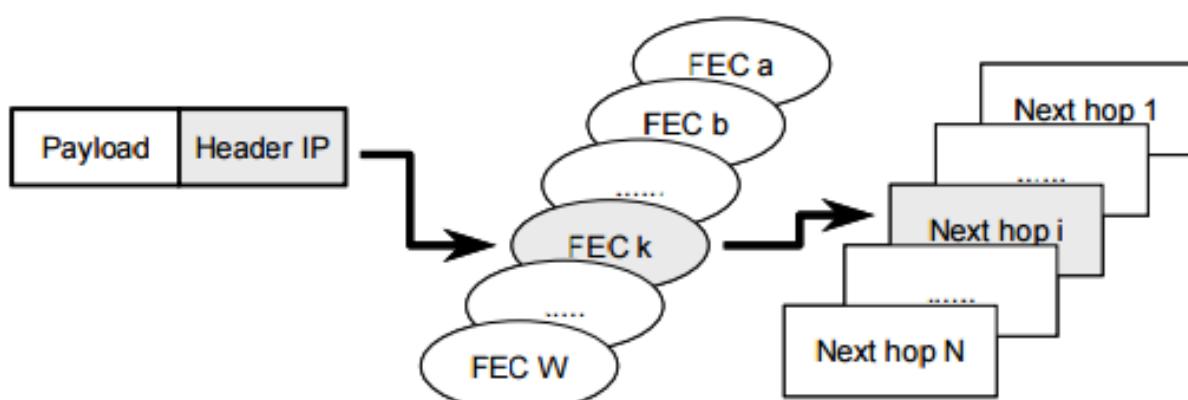
- Indirizzamento privato
- Instradamento privato
- Risorse dedicate o garantite. La differenza tra dedicato e garantito è la seguente: **dedicato**, intendo che è solo mio; **garantito**, non dico che tutti i nodi son tuoi, ma che da questo nodo a questo ti garantisco una velocità di 10 Mb/s.
Il dedicato è inefficiente, non uso sempre tutte le risorse, allora condivido un po'.

6.1 MPLS

La tecnica MPLS ha continuato a mantenere un ruolo chiave perché è in grado di fornire ad una rete IP, oltre ad un miglioramento delle prestazioni, una serie di funzionalità addizionali, quali:

- **Traffic Engineering** : La tecnica MPLS consente l'instaurazione di cammini in rete in modo da ottimizzare l'utilizzazione delle sue risorse. Questa funzione, normalmente indicata con il termine Ingegneria del traffico (Traffic Engineering – TE), non può essere realizzata, almeno in modo semplice, mediante le tecniche tradizionali di instradamento utilizzate nelle reti IP. La ragione di questo risiede nel fatto che nelle reti IP il traffico tra due punti segue sempre un'unica via, mentre con MPLS tra due punti può essere utilizzata una pluralità di cammini; i flussi di traffico possono essere quindi instradati utilizzando tutti i cammini disponibili in modo da ottenere una distribuzione uniforme del traffico sulle risorse di rete e di conseguenza un miglioramento complessivo delle prestazioni di rete.
- La tecnica MPLS consente di definire reti private virtuali (Virtual Private Network – VPN) all'interno di una rete IP. Mediante questo servizio il traffico tra punti d'accesso remoti può transitare in modo trasparente e completamente segregato dagli altri flussi di traffico all'interno della rete IP con conseguenti vantaggi sia per la gestione della qualità del servizio che per i requisiti di sicurezza
- La tecnica MPLS consente, al momento dell'instaurazione di un cammino in rete, la predisposizione di cammini alternativi, detti di protezione o di back-up, da utilizzarsi in caso di guasto di uno o più tratte del cammino principale per re-instradare il flusso di traffico supportato da quest'ultimo;

In una rete senza connessione, come la rete IP, il cammino seguito da un pacchetto tra la sorgente e la destinazione viene determinato mediante la composizione di operazioni di instradamento elementari ed indipendenti eseguite dai router che sono attraversati dal pacchetto. Ogni router sceglie il router successivo (next-hop) verso cui rilanciare il pacchetto. Tale scelta è eseguita esaminando l'header del pacchetto e accedendo ad una tabella di instradamento che è aggiornata mediante l'utilizzazione di un protocollo di instradamento. La scelta del next-hop operata da un router può essere modellata come la concatenazione di due funzioni distinte: i) la suddivisione dell'insieme dei pacchetti da rilanciare in una serie di sottoinsiemi distinti, denominati Forwarding Equivalent Class (FEC); ii) l'associazione di una FEC ad uno specifico next-hop. Secondo questo



modello, i pacchetti appartenenti ad una stessa FEC saranno rilanciati da un router verso lo stesso nexthop. In MPLS [RFC3031] l'assegnazione di un pacchetto ad una FEC è effettuata, una volta per tutte, al momento in cui il pacchetto entra in una rete MPLS. La FEC assegnata al pacchetto è codificata in un'etichetta, di lunghezza breve e fissa. Questa etichetta sarà indicata nel seguito con il termine label. Quando il router attraverso cui il pacchetto è entrato in una rete MPLS rilancia il pacchetto, questi assegna al pacchetto il valore della label che sarà utilizzata dal router successivo per effettuare la commutazione. Quando un pacchetto entra in un router, la label è utilizzata infatti come indice per l'accesso diretto ad una tabella che conterrà il valore del next-hop e il valore della nuova etichetta. La vecchia etichetta è sostituita con la nuova e il pacchetto è rilanciato verso il router successivo. Un pacchetto può avere più label. La fase di aggiunta di una label a un pacchetto è chiamata push. Mentre l'estrazione della label dal pacchetto, è chiamata pop.

LSR

Nel paragrafo precedente è stato già definito il concetto di FEC come un insieme di pacchetti IP che devono essere trattati da un router nello stesso modo, ad esempio: che devono essere rilanciati verso lo stesso next-hop e appartenenti alla stessa classe di servizio. Ad ogni FEC è assegnata una label che sarà utilizzata dai router per eseguire la funzione di commutazione dei pacchetti. Un router che supporta la tecnica MPLS è denominato Label Switching Router (LSR) e la tipologia di commutazione è denominata in generale come label switching. Un dominio di rete MPLS è formato quindi da un insieme di LSR direttamente connessi tra loro. Il traffico entrante ad un dominio MPLS può provenire sia da reti esterne al dominio, quali ad esempio le reti locali d'utente, sia da router IP tradizionali appartenenti a sezioni di rete IP che non supportano la tecnologia MPLS (Figura I.3.1). Un LSR che connette un dominio MPLS con altri nodi che sono all'esterno del dominio è detto Edge LSR, mentre un LSR che è connesso solo ad altri LSR è detto Core LSR.

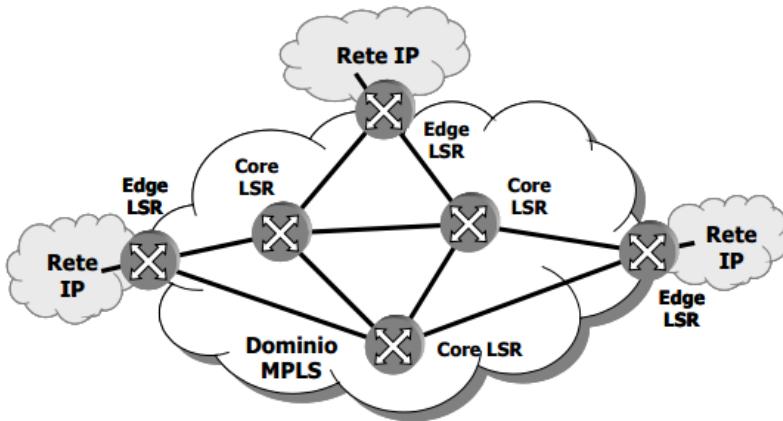


Figura I.3.1 – Rappresentazione di un dominio MPLS.

Una label è un identificatore di lunghezza fissa che è utilizzato per identificare una FEC. L'operazione di associazione di una label ad una FEC è denominata binding. Due LSR, indicati come Ru e Rd, possono accordarsi per eseguire un'associazione tra la FEC F e l'etichetta L, ciò significa che quando Ru trasmetterà verso Rd un pacchetto appartenente alla FEC F, il pacchetto venga etichettato con la label L. Tale etichetta sarà indicata come label uscente dal LSR Ru e come label entrante al LSR Rd. Inoltre nei confronti di questo binding, Ru sarà indicato come upstream LSR, mentre Rd avrà il ruolo di downstream LSR. La Figura I.3.2 illustra i concetti ora introdotti. E' responsabilità dei due

LSR, Ru e Rd, assicurare l'univocità dell'associazione tra la FEC F e la label L, ciò significa che non dovranno essere accettati ulteriori binding tra la label L e FEC diverse da F.



Nell'architettura MPLS la decisione di effettuare un'associazione tra una FEC F e una label L è sempre presa dal downstream LSR che informa l'upstream LSR

dell'avvenuto binding. Quest'ultima operazione è detta distribuzione della label ed è quindi sempre eseguita nella direzione downstream-upstream rispetto alla direzione del traffico. Le procedure seguite 8 da un downstream LSR per distribuire le etichette verso l'upstream LSR sono definite in un protocollo denominato genericamente protocollo di distribuzione delle etichette (**Label Distribution Protocol. - LDP**). L'architettura MPLS prevede un modello molto flessibile di uso delle label in cui un singolo pacchetto può trasportare un numero m, con $m \geq 1$, di label organizzate in m livelli gerarchici (label stack). La label di livello gerarchico più basso sarà indicata come label di livello 1, mentre la label di livello gerarchico più elevato sarà indicata come label di livello m (Figura I.3.3). In ogni caso, qualsiasi sia il numero di label trasportate l'instradamento di un pacchetto in un LSR dipende sempre ed esclusivamente dalla label di livello gerarchico maggiore trasportata dal pacchetto stesso.



Figura I.3.3 – Illustrazione del concetto di label stack

Una label MPLS [RFC 3032] ha una lunghezza uguale a 32 bit ed il suo formato è

mostrato in Figura I.3.4. Il significato dei campi è il seguente:

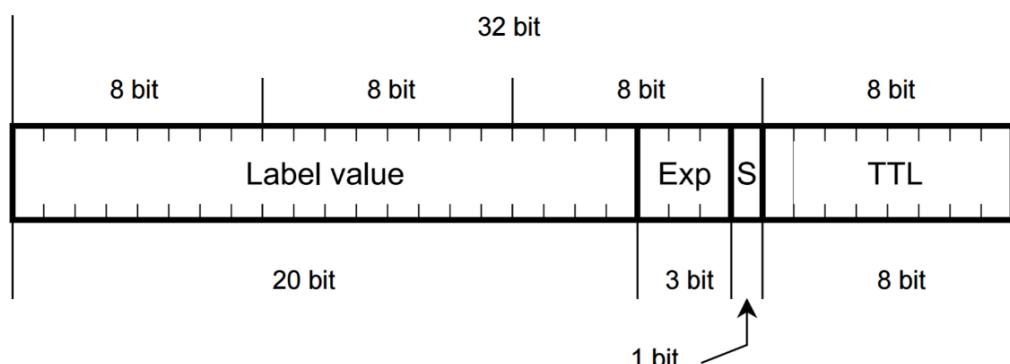


Figura I.3.4 – Formato di una label MPLS.

- Label value (20 bit): indica il valore della label ed è utilizzato come indice per l'accesso alla tabella di routing dell'LSR in cui sono indicati l'identificatore della porta d'uscita verso cui deve essere rilanciato il pacchetto e il valore della label sulla tratta successiva.
- Experimental Use (EXP) (3 bit): questi bit sono riservati per usi successivi, ad esempio, nel caso di architettura Diffserv over MPLS, possono codificare la classe di servizio a cui appartiene il pacchetto.
- Bottom of Stack (S) (1 bit): se questo bit è posto ad 1, indica che la label è quella di livello più basso, in tutti gli altri casi il bit S è sempre posto a 0.
- Time To Live (TTL) (8 bit): indica il numero massimo di (ti amo <3>) salti che ancora il pacchetto può eseguire in rete prima che raggiunga la destinazione o venga scartato. Il valore di tale campo viene decrementato di uno ogniqualvolta viene elaborato da un LSR.

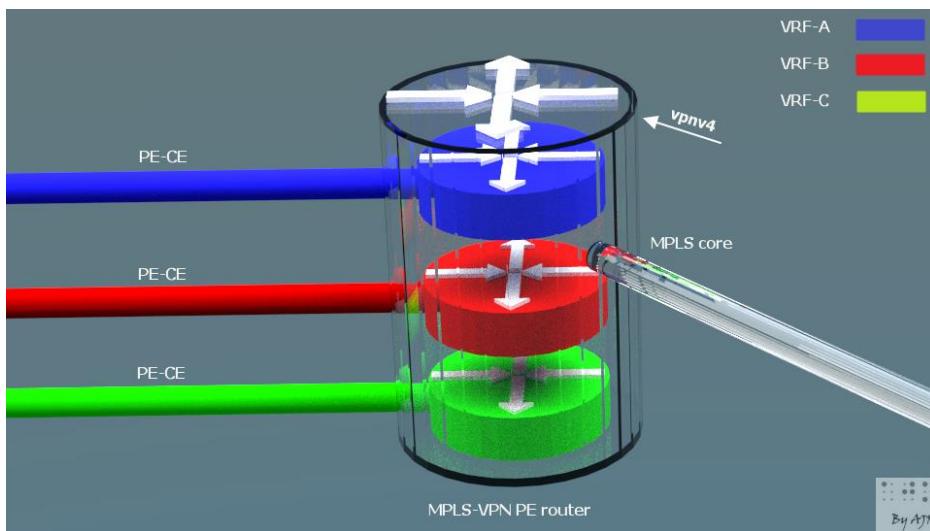
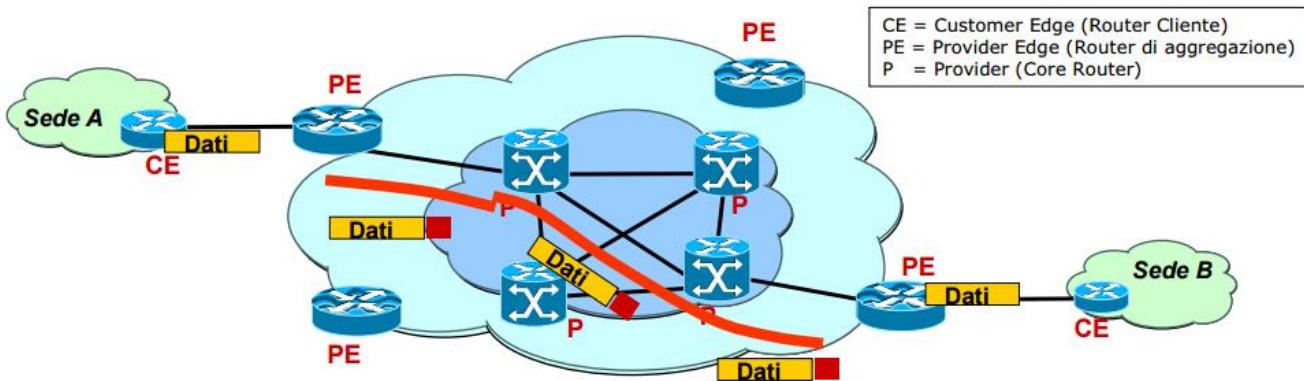
Label Switching Path (LSP): definizione e funzioni degli LSR

Il cammino seguito da un pacchetto in una rete MPLS è denominato Label Switching Path (LSP). In particolare, per uno specifico pacchetto P, un LSP di livello m è definito dalla sequenza di LSR (R1, R2, ..., Rn) che soddisfano le seguenti proprietà:

- l'LSR R1, che rappresenta il punto di inizio del LSP, è il router che applica la label di ordine m al pacchetto P;
- in tutti gli LSR Ri ($1 < i < n$) il pacchetto P sarà instradato attraverso l'esame della label di ordine m, inoltre il numero di label contenute nel pacchetto sarà sempre non inferiore a m;
- se nel transito tra due LSR, Ri e Ri+1, il pacchetto P attraversa altri elementi di rete che effettuano l'instradamento sulla base di una label diversa da quella di ordine m, ad esempio di ordine m+k, ciò avviene solo se altre label k addizionali sono state aggiunte dal router Ri e da altri elementi di rete intermedi.

6.2 VPN

La tecnica MPLS consente di definire reti private virtuali (Virtual Private Network – VPN) all'interno di una rete IP. Mediante questo servizio il traffico tra punti d'accesso remoti può transitare in modo trasparente e completamente segregato dagli altri flussi di traffico all'interno della rete IP con conseguenti vantaggi sia per la gestione della qualità del servizio che per i requisiti di sicurezza. In telecomunicazioni una VPN (virtual private network) è una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come infrastruttura di trasporto, un sistema di trasmissione pubblico e condiviso, come ad esempio la backbone. Scopo delle reti VPN è offrire alle aziende, a un costo inferiore, le stesse possibilità delle linee private in affitto ma sfruttando reti condivise pubbliche: si può vedere dunque una VPN come l'estensione, a scala geografica, di una rete locale privata aziendale che collega tra loro siti interni all'azienda stessa variamente dislocati su un ampio territorio, sfruttando l'instradamento tramite IP per il trasporto su scala geografica e realizzando di fatto una rete LAN, detta appunto virtuale e privata, logicamente del tutto equivalente a un'infrastruttura fisica di rete (ossia con collegamenti fisici) appositamente dedicata. Le VPN sono percepite come reti private dalle persone che le utilizzano, ma sono costruite

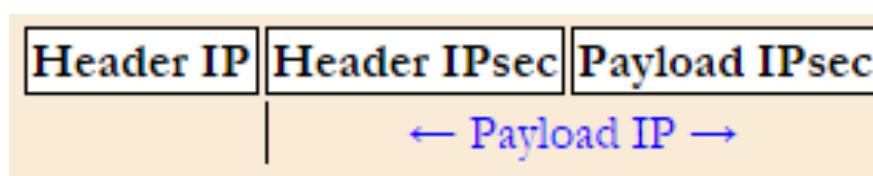


sopra una infrastruttura condivisa. Le strutture condivise, consistono di una backbone condivisa e di provider edge (PES). Una VPN consiste di un grande numero di clienti privati dislocati in aree geografiche, collegati ai PES tramite i customer edge(CE) e comunicano tra loro utilizzando una backbone condivisa. I PES,

nella realtà, è un nodo fisico fatto da tanti nodi virtuali. Mentre il CE è specifico per quella VPN, il PE può terminare con altre reti collegate, quindi lui è un nodo fisico, ma è collegato in diverse tipologie, in base alle vpn che gli arrivano. Ricordiamo che in una VPN MPLS un LSR che connette un dominio MPLS con altri nodi che sono all'esterno del dominio è detto Edge LSR, mentre un LSR che è connesso solo ad altri LSR è detto Core LSR.

IPSEC

IPsec è stato sviluppato ampiamente per implementare reti private virtuali (VPN), reti che sono costruite usando infrastrutture pubbliche per connettere nodi privati. Questi sistemi usano meccanismi di crittografia e di sicurezza per assicurare l'accesso ai soli utenti autorizzati e per evitare l'intercettazione dei dati. Ma per offrire il servizio di riservatezza dei dati, il traffico tra le sedi periferiche deve essere criptato prima di essere immesso nella rete pubblica. Si pensi ad una azienda che ha una sede centrale in una città, molte sedi periferiche in altre città ed inoltre ha agenti di vendita che possono viaggiare per recarsi presso i clienti. Gli host che comunicano attraverso la rete locale della sede centrale o delle sedi periferiche usano il tradizionale protocollo IP, non avendo necessità di criptare i pacchetti. La crittografia è richiesta quando i pacchetti devono viaggiare sulla rete pubblica. Quando un host della sede principale invia un pacchetto ad un agente di vendita che si trova in un albergo con il suo computer portatile, il router di default della rete della sede centrale



converte il datagramma IP in un datagramma IPsec e trasmette questo datagramma IPsec su Internet. Questo datagramma

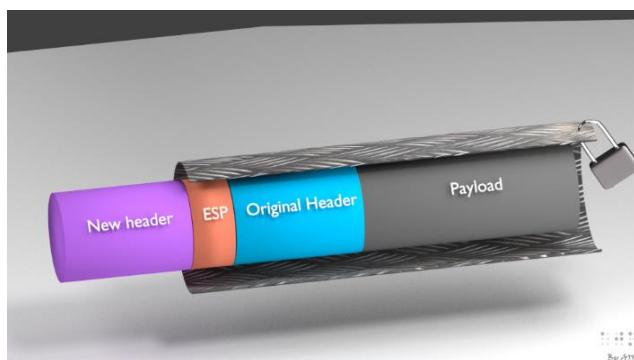
IPsec ha l'intestazione nel formato IPv4, in modo che i router della rete pubblica Internet possano elaborare normalmente il datagramma. Ai router, il datagramma ricevuto appare come un ordinario datagramma nel formato IPv4. Il datagramma originario completo convertito nel formato IPsec, contenente l'header e il payload, è contenuto nel payload del datagramma IPv4. Quando il datagramma IPsec giunge al computer dell'agente di vendita, il sistema operativo del computer decripta il payload (verifica anche l'integrità dei dati) e consegna il pacchetto decriptato al livello superiore (TCP o UDP).

Il protocollo IPsec può indicare nell'header uno tra due protocolli: il protocollo Authentication Header (AH) e il protocollo Encapsulation Security Payload (ESP) protocol. L'entità sorgente di IPsec (un host o un router) invia un datagramma protetto ad un'entità destinazione (un altro host o un router) usa uno dei due protocolli: AH o ESP. Il protocollo AH fornisce i servizi di autenticazione della sorgente e il controllo di integrità dei dati, ma non fornisce la riservatezza dei dati. Il protocollo ESP fornisce i servizi di autenticazione, integrità e riservatezza. Poiché la riservatezza è un requisito che deve possedere una VPN, e altre applicazioni di IPsec, il protocollo ESP è molto più usato del protocollo AH.

I pacchetti IPsec vengono scambiati tra due entità di rete, ad esempio due host, due router, o un host e un router. Prima di trasmettere i datagrammi IPsec dall'entità sorgente all'entità destinazione, le due entità sorgente e destinazione creano una connessione logica a livello Rete. Questa connessione logica è chiamata una security association (SA). Una SA è una connessione simplex, cioè è una connessione unidirezionale da sorgente a destinazione. Se entrambe le entità devono scambiarsi datagrammi sicuri, allora devono essere stabilite due SA, cioè due connessioni logiche, una in ogni direzione.

L'IPSEC supporta due modalità di trasferimento:

- **transport mode:** il metodo Transport cifra solo la porzione dei dati (payload) di ogni pacchetto e lascia intatta l'intestazione (header). L'intestazione IPsec viene inserita subito dopo quella dell'IP.
- **tunnel mode:** costruisco un tunnel che mi permette di trasferire flussi di pacchetti. L'osservatore non è capace di vedere cosa c'è dentro. Il metodo più sicuro Tunnel, cifra entrambi l'header e la payload. Nella modalità tunnel l'intero pacchetto IP, compresa l'intestazione, viene incapsulato nel corpo di un nuovo pacchetto IP con un'intestazione IP completamente diversa.



L'intestazione IPsec più utilizzata sia nella modalità trasporto che nella modalità tunnel è ESP (Encapsulating Security Payload). Il campo ESP è una specie di identificativo della connessione.

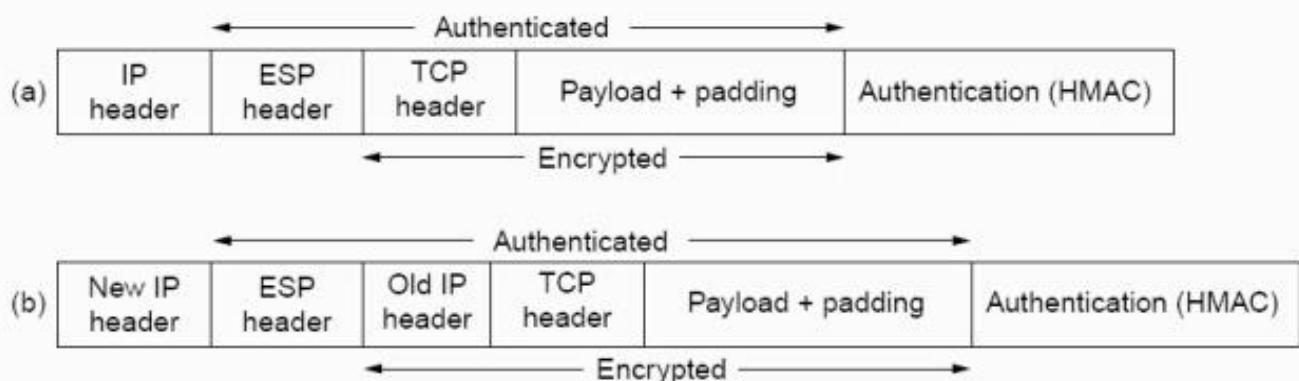


Fig. 8-28. (a) ESP in transport mode. (b) ESP in tunnel mode.

VPN Network Based e Customer-premises-based

Ottengo una rete come se fosse un enorme switch. Abbiamo due tipologie di VPN:

- **Network based**
- **customer-premises-based secure VPNs:** l'utente sa che è una rete privata che non si vede all'esterno.

7.0 APPARATI DI RETE

Se vogliamo costruire una rete, dobbiamo mettere delle scatole come:

- Router
- Switch
- Server principali:
 - DNS
 - Autenticazione (AAA=authentication, authorization, accounting) concedo accesso alla rete a un utente.
- Dispositivi per la sicurezza
 - Firewall
 - Intrusion detection system
- Load balancer (nei data center per gestire il carico)
- Proxy (ottimizzare l'accesso a internet ai contenuti resi disponibili)
- Sip server

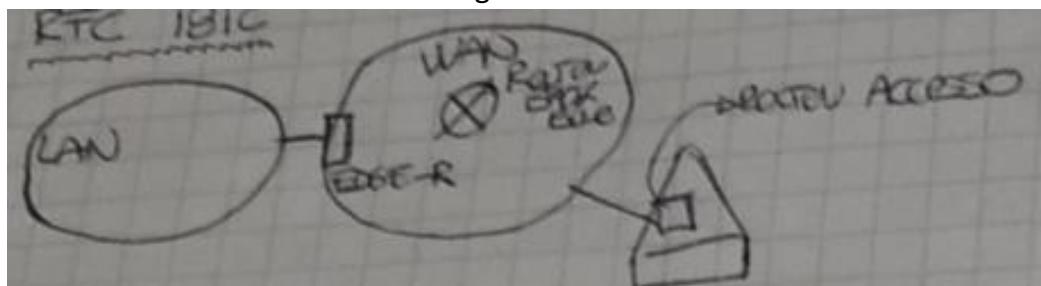
Ricordiamo che In telecomunicazioni e informatica l'**Open Systems Interconnection** (meglio conosciuto come modello ISO/OSI) è uno standard dei calcolatori, che stabilisce per l'architettura logica di rete una struttura a strati composta da una pila di protocolli di comunicazione

di rete suddivisa in 7 livelli, i quali insieme espletano in maniera logico-gerarchica tutte le funzionalità della rete. I 7 livelli sono:

7. Livello di applicazione
6. Livello di presentazione
5. Livello di sessione
4. Livello di trasporto
3. Livello di rete
2. Livello di collegamento
1. Livello fisico

Router

Un **intradattore** (dall'inglese **router**) è un dispositivo elettronico che, in una rete informatica a commutazione di pacchetto, si occupa di intradare i dati, suddivisi in pacchetti, fra reti diverse. L'intradramento può avvenire verso reti direttamente connesse, su interfacce fisiche distinte, oppure verso altre sottoreti non limitrofe che, grazie alle informazioni contenute nelle tabelle di intradamento, siano raggiungibili attraverso altri nodi della rete. Il router serve a collegare una rete di PC a un'altra LAN o a internet.



Esistono diverse tipologie di router:

- **Edge router:** Questo router si prende il carico della LAN. È un router specializzato che si trova al confine (edge) di una rete. Questo router assicura la connettività della sua rete (LAN) con reti esterne (WAN). Ha funzionalità di valore aggiunto. Per esempio io posso avere delle schede che possono fare l'encryption dei dati perché ho bisogno di proteggere per questioni di sicurezza.
- **Access router:** sono i router di casa. Ha certe funzionalità come terminal wifi e terminal adsl.
- **Backbone router:** permette di gestire grandi quantità di dati (parliamo di trasferimento di dati dell'ordine dal terabit alla decina di terabit). Sono meno ricchi di funzionalità.

I router operano a livello di rete (livello di rete). Le sue funzionalità di livello 3 sono:

- gestione protocollo versione ipv4

- gestione protocollo versione ipv6
- gestione multicast
- funzione di label switch routing(MPLS)
- Funzionalità routing, implementazione di un numero di protocolli:
 - UNICAST: OSPF, BGPV4
 - MULTICAST: PIM (Protocol Indipendent Multicast), DVMRP (Distance Vector Multicast Routing Protocol), IGMP (permette di capire quanti utenti di gruppo multicast sono presenti in una sottorete, se sono zero o più).
 - DHCP
 - NAT
- Funzionalità forwarding:
 - WFQ: algoritmo che permette di gestire il forwarding, separando il traffico per tipologia in maniera intelligente.
 - RED/WRED: La congestione è un problema non da poco. Sarebbe bello avere buffer infiniti, ma significa anche introdurre ritardi molto grandi. Buffer grandi significa ritardi grandi. In caso di congestione, scarto in maniera intelligente i pacchetti.

Per quanto riguarda i servizi abbiamo:

- Compressione della voce
- Sicurezza: posso implementare all'interno del router, alcune o tutte le funzionalità di sicurezza come firewall, intrusion detection system...

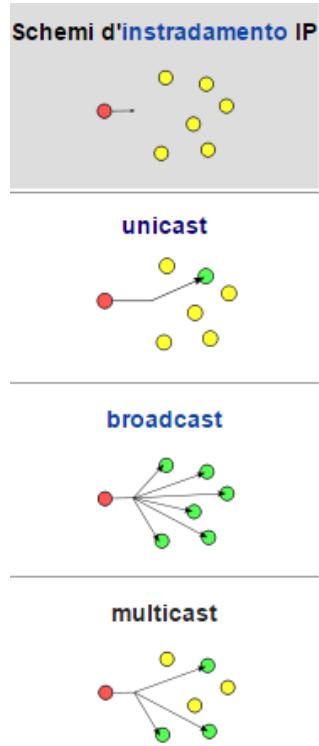
Gestione degli apparati

Noi pensiamo che tutto sia plug and play, ovvero attacco e funziona. Tutta via, plug and play non è neanche un televisore. Gli apparati di networking che sono sostanzialmente plug and play, e sono gli switch. Gli switch sono 95% plug and play. Sono configurabili in maniera molto semplice. Ci sono apparati che sono molto più complicati da configurare, come i router. Gestione vuol dire configurazione e gestione dei guasti (fault performance). Per poter fare la **configurazione**, ci sono degli strumenti:

- **Command line interface**: proietta direttamente a schermo linee di comando per far sì che il router faccia quello che si vuole, per la configurazione.
- **Protocolli**: Negli ultimi 10 anni sono comparsi protocolli che permettono di fare la configurazione in maniera più semplice (Netconf, Network Configuration). Permette di fare la configurazione in maniera più semplice.

Con la **gestione dei guasti** (fault performance), raccolgo delle informazioni, dei dati. Raccolgo degli eventi e per farlo utilizzo il protocollo **SNMP** (simple network manager protocol). Oggi viene utilizzato per raccogliere eventi di guasto. Questi eventi, guasti, si chiamano **trap**.

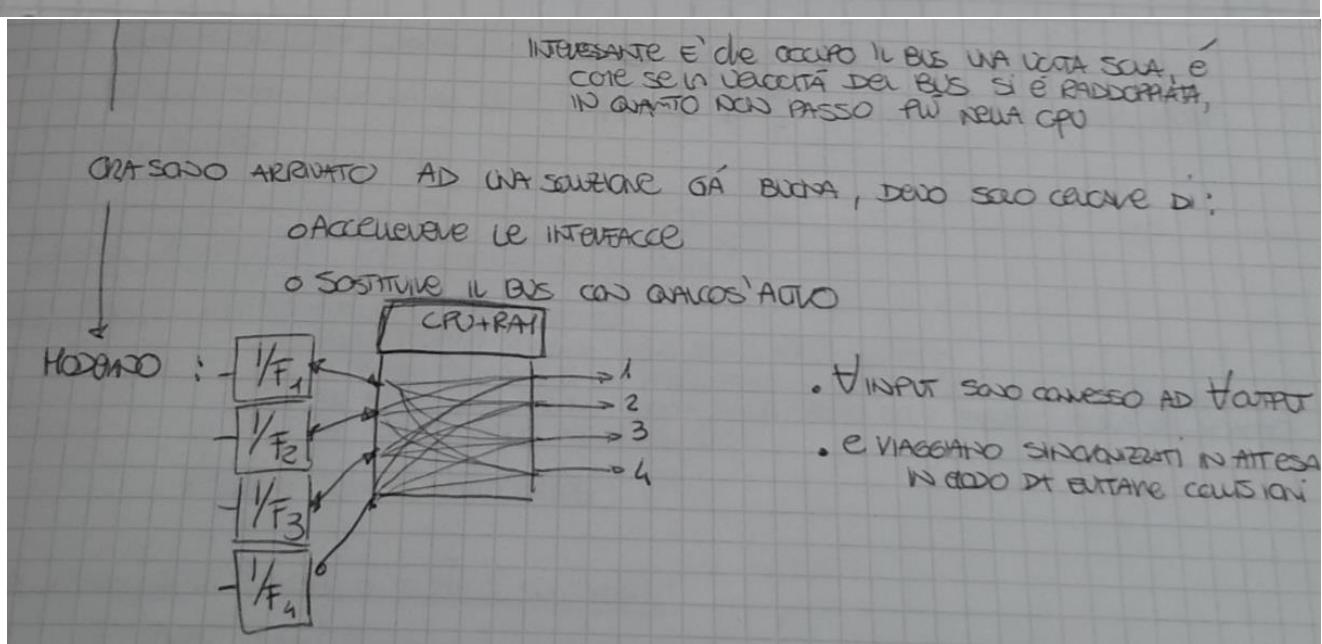
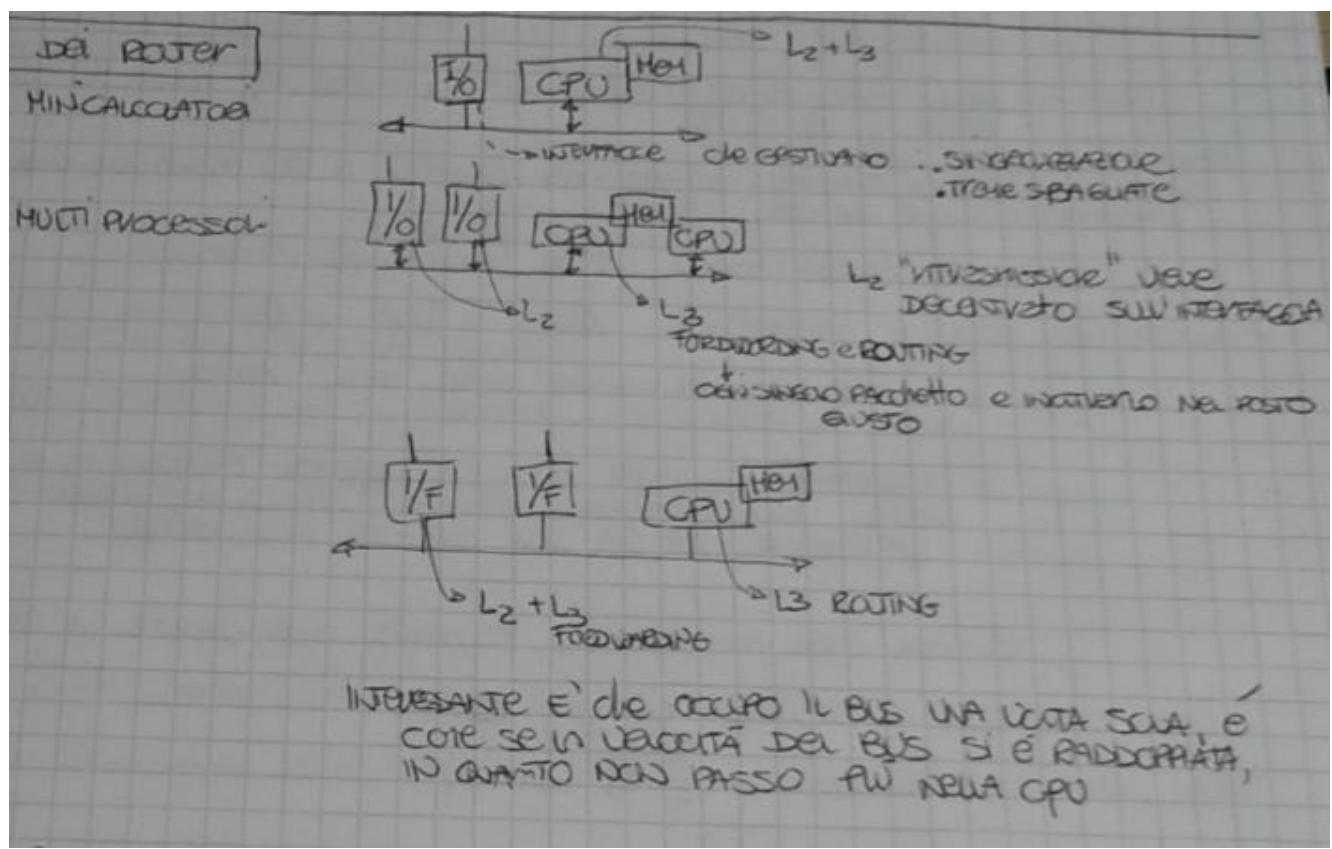
Per quanto riguarda la questione **affidabilità**, abbiamo il protocollo **VRRP** (Virtual Router Redundancy protocol), che permette di realizzare la duplicazione degli apparati. Metto gli apparati



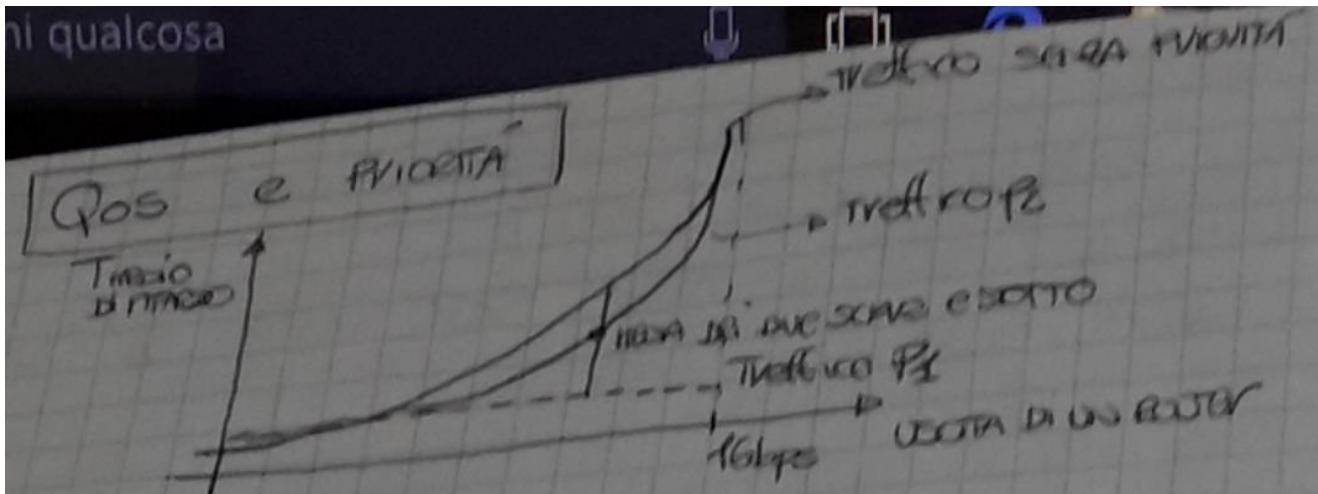
uno accanto all'altro, cosicché in caso di guasto, se uno dei due non funziona, subentra l'altro. Presso le grandi sedi è possibile installare come misura di sicurezza periferiche di rete duplicate, con una periferica principale e l'altra in hot standby che diviene attiva solo se la prima si guasta. Il protocollo VRRP viene eseguito su un collegamento tra i router, in modo che ciascun router rilevi lo stato di attività dell'altro e quello attivo reagisca automaticamente in caso di interruzione del collegamento.

Evoluzione architetture router

I primi router degli anni 70 erano dei minicalcolatori. All'inizio erano singolo processore; dopo si passò al multiprocessore.



Dal punto di vista qualitativo, come vediamo dal grafico sotto, se arrivano più pacchetti che il router non è in grado di smaltire, il ritardo cresce in maniera indefinita. Se butto dentro il router 1 Gbit di traffico il ritardo tende a un ritardo infinito. Se il traffico è molto basso, avrò una costante che è dovuta ai tempi meccanici per la trasmissione, ma abbiamo ritardi piccoli. Abbiamo una forte non linearità del comportamento.



Cosa succede se arrivano pacchetti con due livelli di priorità? Supponiamo di avere il 20% del traffico a priorità P1 e l'80% del traffico a priorità P2 con p1 strettamente maggiore di P2. Il pacchetto P1 nella coda, salta davanti a tutti. Il traffico di P1 è come se non vedesse gli altri pacchetti, quelli di P2, talmente è importante; è come se il link fosse carico al 20%.

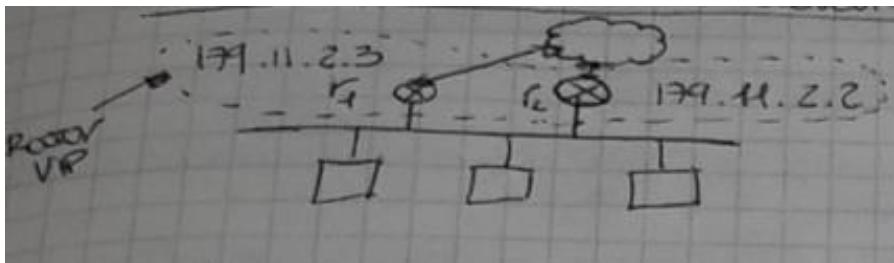
RIDONDANZE E REPLICAZIONI APPARATI PROTOCOLLO VRRP

Se vogliamo duplicare qualche risorsa, e vogliamo che il cambiamento della risorsa sia invisibile alle applicazioni, dobbiamo costruire qualcosa di abbastanza sofisticato.

- Nelle WAN, se ho una sede A e una sede B e in mezzo una rete, io ho un percorso di rete, ma posso anche avere un percorso alternativo di rete, tipicamente disgiunto e devo essere in grado di passare da uno all'altro, nella maniera più efficace possibile.
 - Una prima soluzione è quella di utilizzare gli algoritmi di routing. Se io utilizzo ospf, (ospf perché voglio utilizzare un algoritmo che utilizzi il concetto di costo). Ospf fa vedere al router le alternative per andare in una certa direzione, valutando i costi. I pacchetti verranno instradati sul cammino con costo ridotto. Nel caso in cui io abbia un guasto per qualche motivo, le ospf identificano la disconnessione o crescita del costo del percorso. Il problema è che questo meccanismo è lentissimo perché dipende dal tempo impiegato per riconoscere il guasto e dal tempo di propagazione su tutta la rete del messaggio ospf. Bisogna aspettare che tutti i router della rete capiscano e comprendano il guasto.
 - L'alternativa è l'MPLS. È in grado di definire delle strade secondarie, in maniera molto veloce. Il percorso è precalcolato. L'unico problema è capire che il percorso non è più disponibile

- A livello di LAN l'idea è la seguente: il mio problema, non è più generale di un percorso, ma di apparati, ovvero di front-end, che devono essere messi in condizione di intervenire in

maniera calda, non appena l'altro ha un problema. I vari host vedono un router. Quando voglio andare su internet, mando un messaggio al default router. Ma se questo si rompe? Supponiamo



che r1 abbia indirizzo 179.11.2.3 e che l'altro r2, abbia indirizzo 179.11.2.2, mi invento un concetto di vip. vip è un virtual ip. Prendo un altro indirizzo ip, per esempio 179.11.2.1 e dico che quello è il router di default. A differenza degli altri due indirizzi ip, questo indirizzo è virtuale. Corrisponde al router r1 o r2, a seconda del processo di elezione. Il **processo di elezione del router master** avviene in questo modo: ogni router che viene acceso, manda un messaggio periodicamente su un indirizzo broadcast, 224.0.0.18, in cui dice "io sono colui che si propone come master". Questo messaggio viene mandato con una certa periodicità. Lo standard del vrrp, ha 1 secondo come periodicità. Se c'è un solo router attivo, dice sono il master e nessuno risponde, allora diventa il master. Dire sono il master, vuol dire "mi appartiene il virtual ip". Il proprio indirizzo mac del router, viene associato al virtual ip. Cosa succede se ci sono due o più router? Si utilizza un meccanismo di elezione distribuito. Si sceglie quello che ha una priorità configurata a mano, maggiore. Il secondo router aspetta che ogni secondo l'altro router, quello master, invii il messaggio che è il router master. Se il master non manda più messaggi ogni secondo, allora il secondo router dice "sono il master" e comincia a rispondere ai messaggi che gli arrivano e si prende l'indirizzo vip. La prima cosa che si evince è che ho due risorse, dove una funziona e l'altra ogni secondo, si aggiorna dicendo "ah c'è l'altro che risponde", ma non fa niente. Per non tenerlo inutilizzato, andrebbe implementato il load balancing, cerco di distribuire il carico. Ho due router e utilizzo due vip:

- Per il **vip1** il router1 è il master e il **router2** è lo slave.
- Per il **vip2** il router2 è il master e il **router1** è lo slave.

LOAD BALANCING

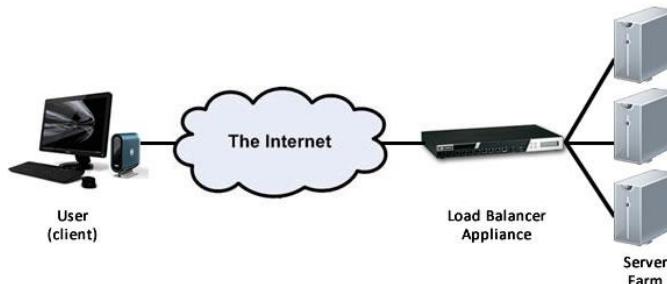
Come distribuisco il carico?

A livello WAN:

- MPLS traffic engineering funziona in maniera perfetta e permette di distribuire il traffico fra diversi percorsi. L'unico difetto è che ci sia una rete mpls per farlo funzionare. Il secondo difetto è che si tratta di un meccanismo rigido perché un tunnel mpls è qualche cosa che funziona se tutti i nodi del percorso hanno mappa delle label nelle tabelle.
- SW Define networking

A livello interno di distribuzione di traffico su server:

- DNS Load Balancing: quando facciamo una risoluzione dns (disco.it si trasforma in un indirizzo ip), se utilizza più di un indirizzo ip corrispondente a più di un server, crea distribuito su tutti i client del mondo, una visione di un server logico, distribuito su tanti server logici. Funziona con tempo di allineamento molto lungo.
- Soluzioni applicative: ci sono molte tecnologie che permettono di effettuare questo.
- Load balancer hardware



FIREWALL

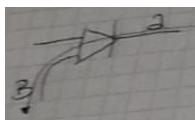
Il firewall si basa su una serie di regole. Queste regole sono abbastanza elementari. È un oggetto attraverso cui passa tutto il traffico. Il firewall decide in tempo reale se il pacchetto deve essere accettato o scartato. Nessun firewall ragiona senza considerare la sequenza che transitano in entrambe le direzioni. La sequenza di pacchetti è importante per determinare l'accettabilità o no dei pacchetti. Esempio di regola:

```
set-policy <id_number_policy> from< zona_in> to
<zona_out><address_in><address_out><protocol/port>
```

- **A)** **from** mi dice da dove viene il traffico, zona di ingresso del traffico
- **B)** **to** zona di uscita del traffico

Nessun firewall è stateless, cioè nessun firewall ragiona senza considerare la sequenza dei pacchetti che transitano perché la sequenza di pacchetti di protocollo è importante per determinarne l'accettabilità. Una regola che mi posso imporre, è che io accetto traffico che proviene solo da host miei e non il traffico che proviene da host esterni. Per fare questo bisogna tracciare il protocollo tcp, cioè far passare il messaggio di sync in una direzione e non nell'altra. Le zone sono di diversi tipi:

- **untrusted**: l'esterno
- **trusted**: sistemi interni (host, server)
- **dmz**: zona demilitarizzata che contiene tutti i server che devono essere accessibili sia dall'interno che dall'esterno



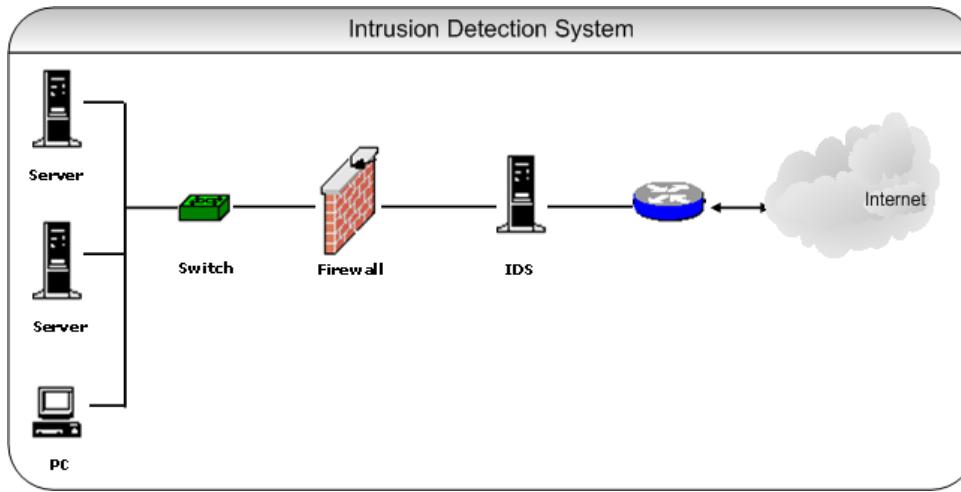
IDS (Intrusion Detection System) e IPS (Intrusion Prevention System)

L'Intrusion Detection System o IDS è un dispositivo software o hardware (o a volte la combinazione di entrambi, sotto forma di sistemi stand-alone pre-installati e pre-configurati) utilizzato per identificare accessi non autorizzati ai computer o alle reti locali. IDS e IPS possono essere online oppure offline. Posso far funzionare un sistema come questo in due modi:

- **Signature based:** in qualche modo ho una firma, caratterizzazione di tutti i più rilevanti attacchi di sicurezza, quindi sono in grado di capire che una certa sequenza di azioni provenienti da un certo indirizzo ip, sta effettuando un attacco. Io conosco il pericolo e se identifico il pattern, lo segnalo.
- **Anomaly based:** conosco i comportamenti corretti, tutto ciò che è al di fuori, lo registro come anomalia.

Entrambe i sistemi hanno punti deboli:

- Il signature based è simile all'antivirus; in caso di attacco di un nuovo virus, mai visto, non avendo la sua firma, non sa come comportarsi e agire.
- La normaly based, butta via ogni volta che non capisco. Perché la cosa funzioni devo conoscere le mie applicazioni e ambiente.



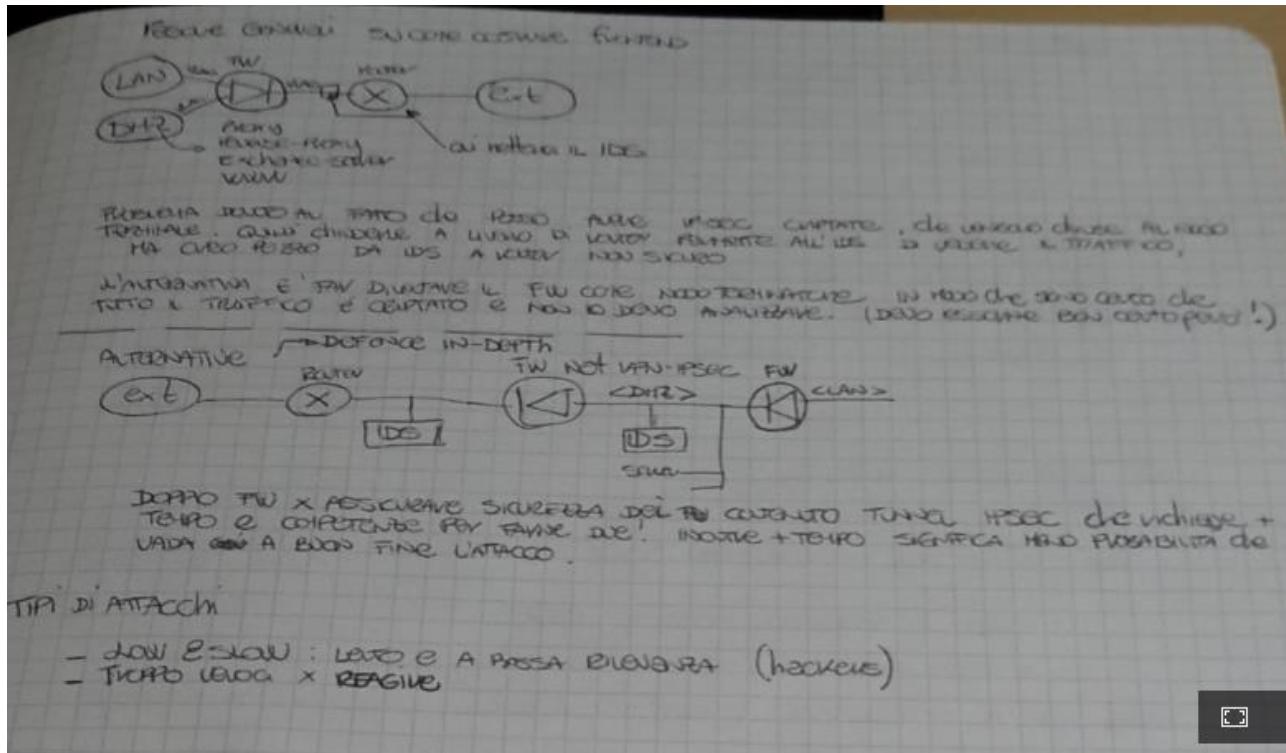
Un esempio di Network Intrusion Detection System è Snort, uno degli IDS più conosciuti. consiste essenzialmente in un uno standard, per descrivere e definire i database di regole degli intrusion detection

system. Sono regole che hanno struttura molto semplice. Sono regole che definiscono un'azione che deve essere applicata dato un certo protocollo e su una coppia ingresso uscita. <Ip/Port>. Le opzioni possibili sono il payload, non-payload, post detection. Gli IDS basati su regole, sono sistemi che sfruttano database, librerie e firme di attacco (o signature) per rilevare le intrusioni. Quando il traffico di rete oppure un'attività di rete corrisponde a una regola ben nota all'ids, questi segnala il tentativo di intrusione. Il limite principale è che l'affidabilità di tale strumento dipende interamente dalla tempestività con cui il database degli attacchi viene aggiornato.

Regole di costruzione di un frontend

Il frontend più semplice, è costituito da una zona esterna (zona untrusted), un povero router che fa da frontend, un firewall che dà accesso a due zone:

- zona interna
- dmz, zona in cui abbiamo tutte le funzioni come sito web, il server della posta elettronica, dns.



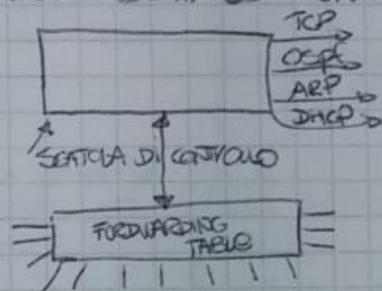
8.0 Software defined networking

Il router è una scatola di controllo in cui sono implementati vari protocolli come tcp, ospf e un'altra serie di protocolli come ARP, DHCP... Il router è collegato con una macchina multi porta che contiene al suo interno una tabella di forwarding (a volte chiamata tabella di routing). In un router l'effettiva struttura hardware non è definita in maniera esplicita. Come è fatto invece lo switch? È costituito da una scatola che svolge una funzione di controllo e che parla con il resto del mondo con vari protocolli, tra cui il rtsp che serve per creare lo spanning tree (router spanning tree protocol). Inoltre abbiamo lo switching table, che viene riempito dal meccanismo di learning bridge, meccanismo che permette di inizializzare la switching table. Come è fatto invece un load balancer? È costituito da una scatola di controllo, che oltre ad avere i protocolli visti precedentemente, ha anche dei componenti per misurare il traffico.

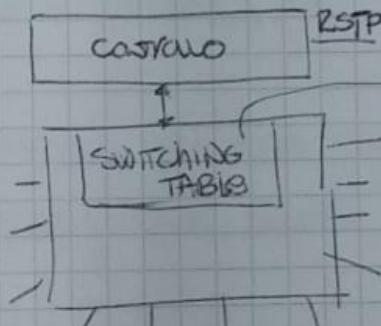
Software Defined Networking

11/04/20
Helen

ROUTER



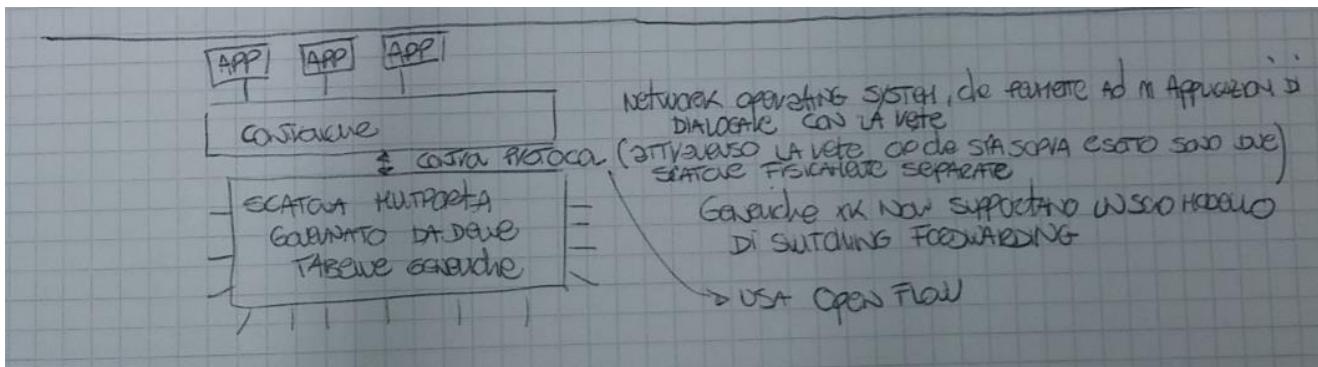
SWITCH



PVINCIPALMENTE DUE FUNZ DI CONTROLLO
OSA Router Spanning Tree Protocol

PROVINTA DAL MECCANISMO DI LEARNING BRIDGE

Molti oggetti di rete sono fatti secondo questo schema. Perché non provare a generalizzare questo concetto, ovvero scatola di controllo + tabella? Proviamo a standardizzare un'ipotetica interfaccia che sta tra il mondo controllo e il mondo forwarding. Ci immaginiamo di avere un controllore, e qualche cosa che effettua il forwarding, una scatola multi porta governata da tabelle. Sono tabelle generiche; generiche perché non supportano un solo e unico modello di switching forwarding.

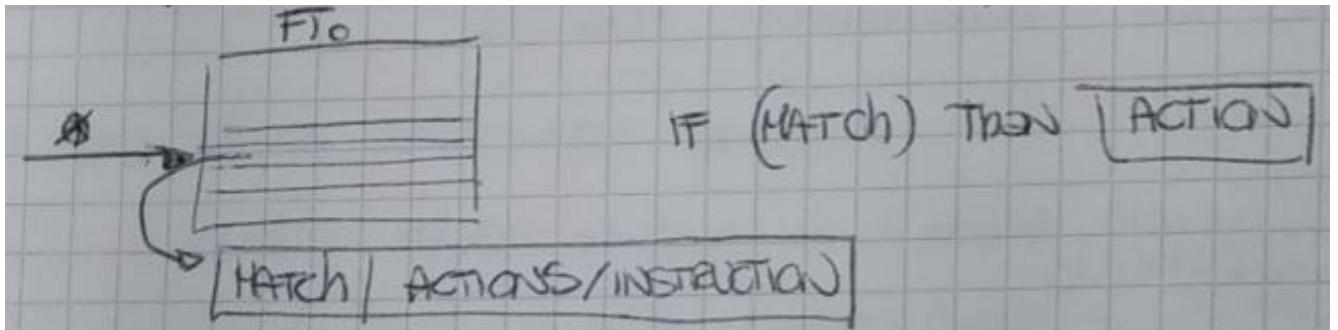


La tabella di switching deve leggere l'indirizzo di destinazione della macchina per scegliere l'uscita. Il controllore e la scatola multi porta sono scatole fisicamente separate. Tra i due ci sta il control protocol, ovvero una faccenda che può viaggiare attraverso la rete. Questo viene chiamato network operating system. Permette alle applicazioni di dialogare tramite il network operating system con la rete. L'applicazione che può girare su qualsiasi server, vede le primitive esposte dal network operating system. Le novità proposte dal network operating system è:

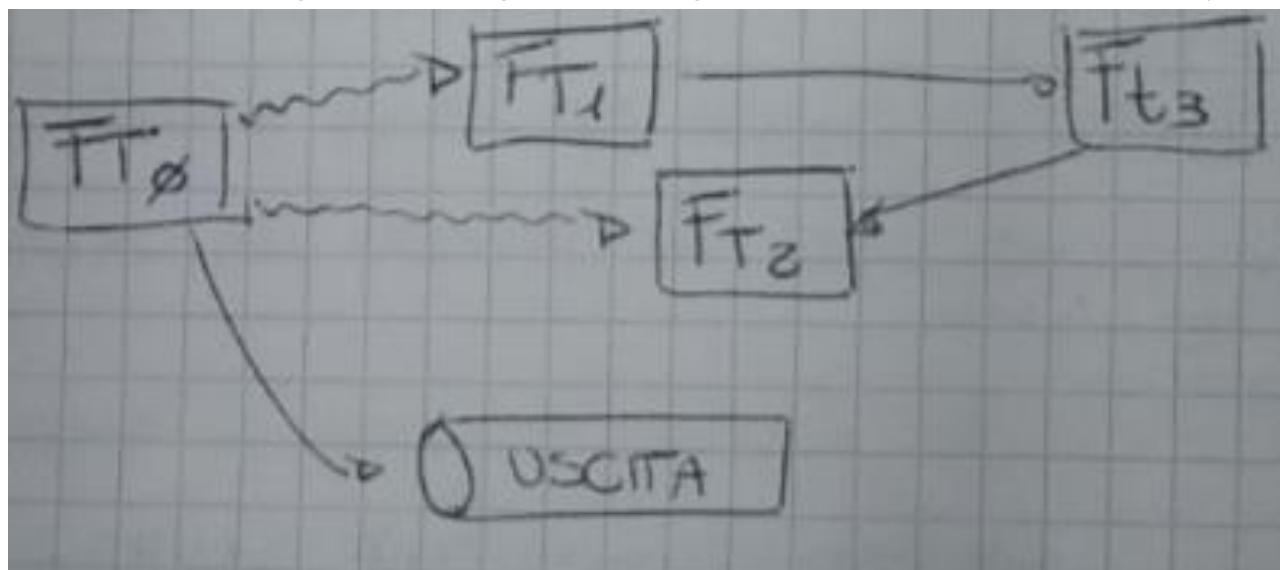
- Apertura ovvero open flow. Il protocollo è aperto. L'apertura del mercato vuol dire che c'è molta più competizione, prezzi che calano...
- Centralizzazione delle informazioni e degli algoritmi. Se io ho una rete grande e questa rete utilizza un algoritmo di routing grande avrò difficoltà nell'utilizzare il mio traffico. L'unica cosa è utilizzare l'mpls, con l'unico problema che i nodi mpls non sono flessibili.
- Accesso diretto alla rete da parte delle applicazioni

Flow table

La chiave di tutto sono le tabelle di forwarding. Dal punto di vista strutturale, una generica riga della tabella, comprende dei campi, delle regole di match e delle azioni da intraprendere e o istruzioni conseguenti, ovvero la riga della tabella di forwarding, contiene una regola che mi dice se questa riga si applica a quel pacchetto che è arrivato e se coincide che cosa devo fare: **If condition then action**.



Queste tabelle si chiamano flow table. Il protocollo open flow permette di installare dei flussi sulle tabelle. Un flusso è un insieme di pacchetti che matchano questa regola. Identificato il flusso dal fatto che la regola scatta, si intraprendono delle azioni. Con l'evoluzione, si è pensato di averne più di una di flow table. La prima tabella si chiama Flow table 0, poi abbiamo la flow table 1, ... flow table n. oltre a queste tabelle abbiamo la **GROUP TABLE** che serve per gestire il multicast, i gruppi multicast. Come funziona? Il singolo pacchetto arriva alla flow table 0, e se matcha, scatta una certa regola, effettua un'azione. Il traffico che entra viene smazzato dalle varie flow tables e poi attraverso le varie flow table passa. Dalla flow table 1 posso andare alla tre e dalla tre alla due. Prima o poi dovrò uscire, il pacchetto dovrà uscire da qualche porta di uscita. non è detto che io esca dallo switch. Può darsi che ci siano delle condizioni per cui io vado al controller. Questo è importante perché mi permette di realizzare le flow table in maniera incrementale. Se dovessi mandare un pacchetto a un'uscita, avrei la necessità di definire il percorso del pacchetto. Io posso anche dire che il mio pacchetto va al controller. Supponiamo che la prima flow table mi dica di mandare il pacchetto alla flow table 2 e la flow table 2 mi dica di mandare il pacchetto alla flow table 3 e così via e poi va al controller. Il pacchetto va al controller; esso sa che il pacchetto non è stato gestito per vari motivi, ed è in grado di riconfigurare la configurazione delle flow table in modo da poterlo



gestire alle volte successive. Su che cosa posso effettuare il match? Posso specificare per il matching un particolare campo del pacchetto; i campi obbligatori sono parecchi:

- **import** ovvero porta di ingresso
- **ethernet source** è l'indirizzo MAC
- **ethernet destination** è l'indirizzo MAC
- **ethernet type** è il campo lunghezza della trama eternete
- **Ipv4 source**
- **Ipv4 destination**
- **Ipv6 source**
- **Ipv6 destination**
- **Tcp source**
- **Tcp destination**
- **Udp source**
- **Udp destination**

Per ciascun di questi campi obbligatori, posso dare un set di valori che devono matchare. Con questi campi obbligatori definisco un flusso. Ci sono altri campi che sono **implementation dependent**. Ciò significa che posso realizzarli o meno. Posso costruire uno switch conforme al protocollo open flow che non ha queste cose. Chi ci garantisce che il pacchetto matcha su una sola regola? Bisogna avere una regola che mi dice quale è la priorità. La priorità nella tabella è la prima regola che prevale sulle altre. La regola che scatta per prima è quella che ha priorità. Cosa succede se arriva in fondo e non è scattata nessuna regola? La **table miss entry** mi dice cosa devo fare nel caso in cui non ho delle regole che matchano con il mio pacchetto. Ci sono dei default. Il default è lo scarto.

9.0 DATA CENTER

Quando faccio un data center che domande mi faccio? Posso migliorarne uno vecchio o metterne uno nuovo, o fare outsourcing, quanto farlo grande, quali sono i livelli di sicurezza, ciclo di vita... In termini di spesa, i costi di acquisto sono il 10% della spesa IT, mentre i costi di esercizio sono il 90% della spesa IT.

Tier

Ci sono diversi tipi di data center a seconda dell'utilizzo da fare. L'Uptime Institute ha stabilito quattro livelli di servizio (tolleranza ai guasti) per i Data center. Tier 1 rappresenta il livello più basso e il Tier 4 il livello più alto, dotato di impianti di distribuzione elettrica multipli, impianto per la generazione elettrica e gruppi di continuità (UPS).

In base al livello sono previsti i seguenti tempi di downtime / anno:

- **Tier 1:**
 - singolo impianto di alimentazione elettrica e di raffreddamento
 - nessuna ridondanza nei componenti

- downtime minore di 28,8 hh/anno
- **Tier 2:**
 - singolo impianto di alimentazione elettrica e di raffreddamento
 - ridondanza nei componenti
 - downtime minore di 22 hh/anno
- **Tier 3:**
 - impianti multipli di alimentazione elettrica e di raffreddamento
 - ridondanza nei componenti
 - possibilità di effettuare manutenzione durante l'attività
 - downtime minore di 1,6 hh/anno
- **Tier 4:**
 - Impianti multipli di alimentazione elettrica e di raffreddamento,
 - ridondanza nei componenti
 - continuità di servizio in caso di guasto
 - downtime minore di 0,4 hh/anno (o una disponibilità del 99,995%)



L'identificazione del livello di «toleranza al guasto», guida la fase di progettazione del data center; infatti tanto più alto sarà il livello, tanto maggiori saranno gli investimenti che dovranno essere effettuati. Tale livello sta diventando sempre più un elemento critico su cui competere. Nel mercato della finanza, una elevata disponibilità dei Data center (tipicamente Tier 3 / Tier 4) è fondamentale per garantire la continuità delle transazioni finanziarie 24/24 x 7/7. L'Uptime Institute mette in guardia sul fatto che le sole specifiche di progettazione, non possono garantire un'elevata affidabilità del data center: molte interruzioni di servizio accadono infatti a causa di errori umani. In tal senso una attenta selezione del personale, investimenti sulla formazione e un ambiente di lavoro positivo e motivante possono contribuire a una riduzione degli errori e, di conseguenza, una elevata disponibilità.



5 elementi principali in un data center

Nella costruzione di un nuovo data center (o nell'upgrade di uno pre-esistente) sono stati identificati cinque diversi elementi / ambiti, che richiedono competenze specifiche in fase di progettazione:

- **Impianto elettrico:** tale sistema include l'impianto di distribuzione, gruppi di continuità UPS, generatore di corrente secondario, PDU e unità di distribuzione intermedie)
- **Impianto di raffreddamento:** questi sistemi possono prevedere unità di raffreddamento disposte sul tetto, che provvedono un raffreddamento localizzato. La principale sfida degli attuali Data Center è quella di mantenere una temperatura adeguata, contrastando l'elevato calore generato dai moderni blade-server e DASD

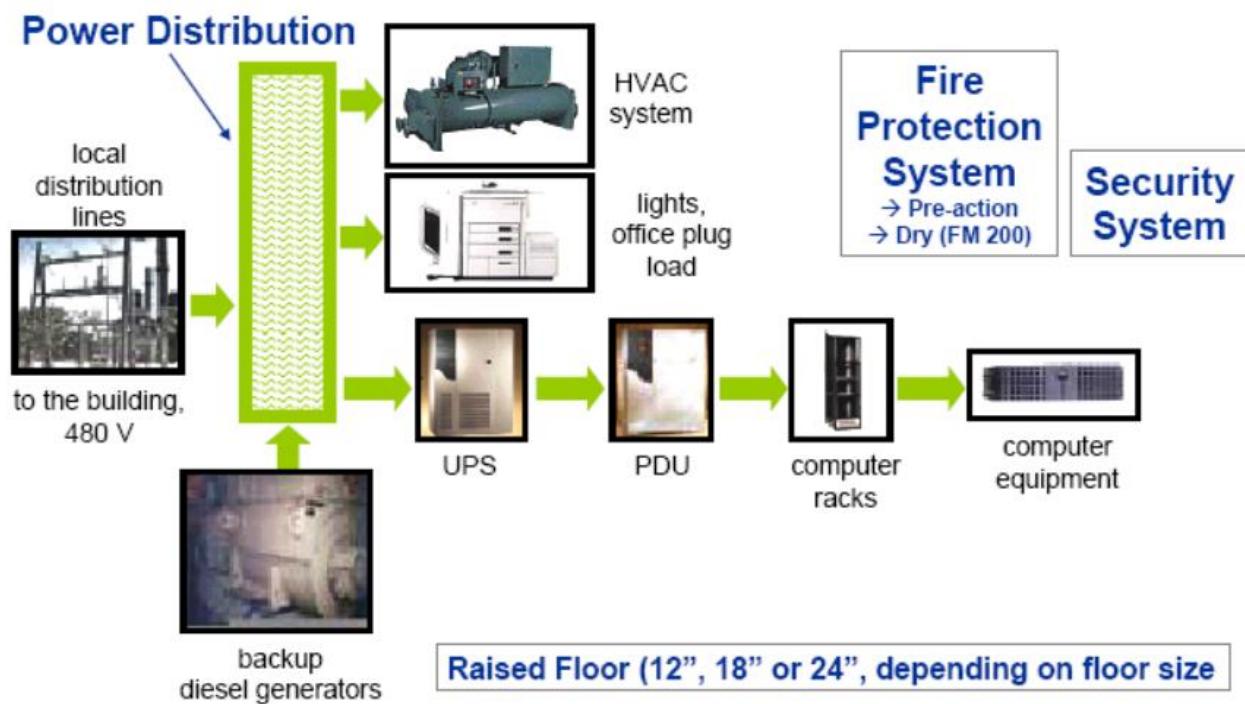
- **Sistemi anti incendio:** questi sistemi includono sensori di incendio e soluzioni di abbattimento / riduzione delle fiamme, in grado di combinare sistemi di prespegnimento (wet-systems) con sistemi anti-incendio (dry-systems) – come l'FM 200 – per aree specifiche (i.e., aree di storage)
- **Sistemi di pavimentazione sopraelevata / flottante:**
 - circa 30cm, per superfici fino a 100mq
 - da 30 a 45cm, per superfici comprese tra 100 e 500
 - da 45 a 60cm, per superfici comprese tra i 500 e i 1.000mq
 - circa 60cm, per superfici maggiori di 1.000mq
- **Sistemi di sicurezza centrale e locale**

Criteri di scelta localizzazione datacenter

La scelta del luogo geografico in cui costruire un Data Center ha un elevato impatto sulla sicurezza, sull'efficienza operativa e sui costi operativi. I criteri di selezione del sito dovrebbero valutare che:

- la distanza media dalle abitazioni degli operatori e dai siti di supporto/manutenzione non sia eccessiva;
- Sia disponibile un parcheggio adeguato;
- Siano garantiti acqua e rifornimenti di carburante, nonché spazi necessari a eventuali camion per l'accesso.
- Inoltre i siti non devono trovarsi in aree ad alto rischio geologico, caratterizzate da elevati rischi di alluvioni / frane, o elevato rischio sismico. Per garantire una maggior sicurezza il sito dovrebbe trovarsi in una zona isolata, non contornato da altre costruzioni, ma comunque collegata da autostrade / strade principali al fine di garantirne l'accessibilità.
- Nel caso di struttura condivisa, sarebbe opportuno non collocarsi in una posizione in cui si è esposti a possibili danni causati dagli altri «inquilini». In ottica di futura espansione, sarebbe opportuno prevedere sufficienti spazi per l'allargamento della struttura e dei parcheggi annessi. Infine è importante accertarsi che le normative locali / regionali, eventuali ordinanze o restrizioni di zona, non impediscano la regolare operatività del data-center

Rete elettrica



La progettazione dell'impianto di generazione e di distribuzione dell'energia elettrica è fondamentale per garantire un'elevata affidabilità ed efficienza del Data Center. Per la fornitura di corrente elettrica, è meglio avere due cavi perché uno dei due potrebbe essere tranciato o andare in disuso. Sarebbe anche meglio avere due fornitori di corrente elettrica diversi, così qualora uno dei due non dovesse riuscire a fornire corrente, c'è sempre l'altro che la fornisce.

Le nuove tecnologie blade-server necessitano di una enorme quantità di energia, destinata sia all'alimentazione dei server stessi, sia all'alimentazione dei sistemi ausiliari di raffreddamento. In tal senso ci sono diversi principi che devono essere rispettati in fase di progettazione dell'impianto:

- Predisposizione di interruttori in tutti i punti di ingresso del sito;
- Un sistema di «messa a terra» che rispetti la normativa in materia (National Electrical Code, Art.250, e/ o eventuali codici locali qualora applicabili);
- La predisposizione di una SRG (Signal Reference Grid) per ridurre l'impedenza ad alte frequenze;
- Utilizzo di sistemi di distribuzione (i.e., cavi, quadri, etc.) sovradimensionati, per supportare eventuali future espansioni;
- Utilizzo di unità di distribuzione (PDU) per garantire la presenza di interruttori nelle connessioni; sono punti di accesso alla rete elettrica. Dopo ci stanno i server.
-
- Utilizzo di «Power Conditioner» o di gruppo di continuità (UPS), insieme di batterie che garantiscono la continuità. Le batterie hanno durata limitata, e solitamente un ups dura massimo 1a o due ore
- Considerare infine l'utilizzo di supporti ad-hoc per i cavi elettrici nel pavimento rialzato, separare i cavi «dati» da quelli «elettrici», migliorare la circolazione dell'aria attraverso il pavimento

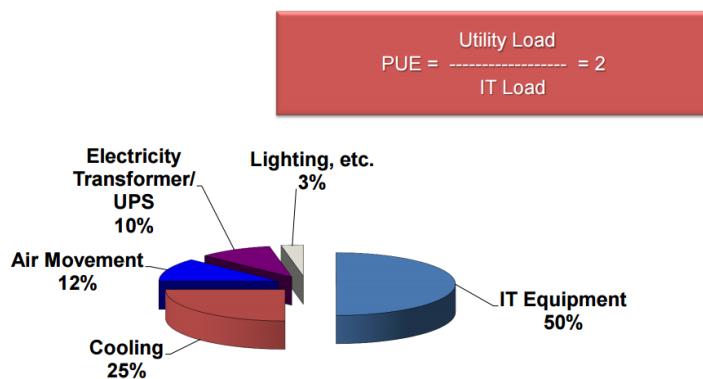
Sia i gruppi di continuità (UPS), sia – in molti casi – i generatori diesel secondari sono elementi cruciali per garantire la continuità della corrente in caso di guasti sulla rete di distribuzione pubblica

della corrente. Ci sono diversi principi base che dovrebbero guidare il dimensionamento e la scelta degli UPS:

- Gli UPS dovrebbero essere dimensionati per garantire la corrente a TUTTI i sistemi (i.e., computer/server, sistemi HVAC, altri sistemi che in caso di emergenza devono avere il 100% delle funzionalità per i 15/20 minuti successivi all'interruzione della corrente)
- Gli UPS dovrebbero essere dimensionati tenendo conto dei picchi di carico o eventuali condizioni di sovraccarico (condizioni che si generano durante il periodo «transitorio» di avvio di un dispositivo elettrico). Come regola empirica si può prevedere un dimensionamento dell'UPS sul 150% dell'assorbimento rilevato a regime.
- Gli UPS dovrebbero essere mantenuti sempre attivi, per filtrare e modulare eventuali picchi/abbassamenti di corrente. In caso di UPS non funzionanti / spenti, la protezione da eventuali sbalzi dovrebbe essere garantita da appositi pannelli schermanti / trasformatori.

Per far fronte a interruzioni di corrente con durata superiore ai 20 minuti è comunque auspicabile installare dei generatori secondari a diesel, in grado di garantire autonomia per lunghi periodi (se alimentati). Solo per i livelli Tier 3 e Tier 4 è richiesta l'installazione di un ulteriore generatore di back-up. Infine è fondamentale considerare eventuali normative locali in merito alla disposizione di serbatoi di carburanti e all'emissione di rumori

Il tasso di efficienza del data center, è dato dal PUE. Più basso è il PUE, più è green il nostro datacenter. Più alto è, più è inquinante il nostro datacenter.

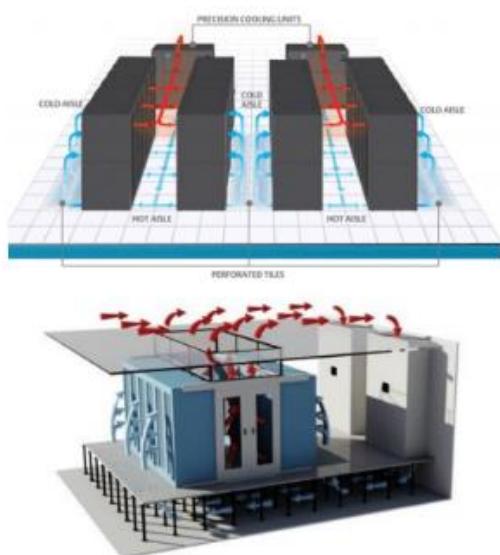


Sistema di raffreddamento HVAC

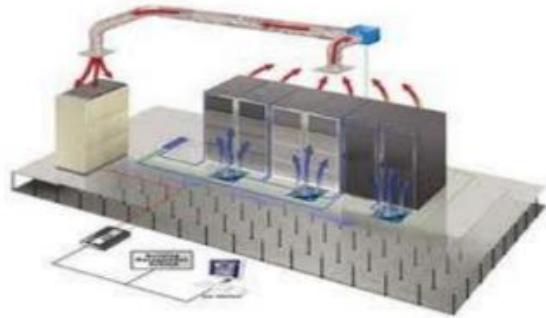
I nuovi impianti di raffreddamento permettono di risparmiare energia. Racchiudo il sistema di raffreddamento in uno spazio molto piccolo e questo fa risparmiare energia.

Impianto di raffreddamento

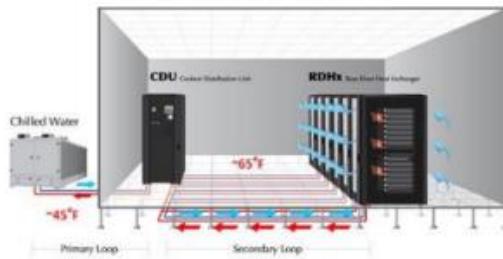
IN THE HOT-AISLE/COLD-AISLE ARRANGEMENT, RACKS ARE PLACED IN ROWS FACE-TO-FACE, WITH A RECOMMENDED 48-INCH AISLE BETWEEN THEM. COLD AIR IS DISTRIBUTED IN THE AISLE AND USED BY RACKS ON BOTH SIDES. HOT AIR IS EXPELLED AT THE REAR OF EACH RACK INTO THE "HOT AISLE."



11



LiquiCool® System



L'impianto di raffreddamento è diventato un sistema cruciale per garantire la corretta operatività del data Center, a causa del sempre maggiore calore emesso dai server di ultima generazione. Di seguito vengono quindi presentate le linee guida da seguire nella progettazione di sistemi HVAC (Heat Ventilation Air conditioning and Cooling):

- Garantire una temperatura compresa tra i 20 e i 23 gradi.
- Garantire un'umidità compresa tra il 45 e il 50%.
- Installare sistemi di raffreddamento ridondanti, installando diverse unità HVAC, anziché affidarsi ad un unico sistema di raffreddamento centralizzato
- Disegnare un sistema di raffreddamento che massimizzi la circolazione dell'aria tra tutti gli elementi dell'ambiente. Questo richiede un flusso che percorra gli elementi dal basso verso il basso e da davanti a dietro, attraversando il rack. Disporre dei corridoi che separino i flussi di aria calda da quelli di aria fredda, può facilitare il controllo della temperatura nell'ambiente.
- Mantenere una pressione all'interno del pavimento sopra-elevato del 5% superiore rispetto all'area sopraelevata in cui risiedono i server. In tal modo sarà possibile predisporre dei fori sul pavimento per garantire un'areazione diretta all'interno dei rack

- Predisporre delle barriere di vapore intorno al perimetro del Data Center per minimizzare il rischio di condensa, dovuto alla presenza di umidità

Sistema anti incendio

A causa dell'elevato rischio di incendio dovuto ai numerosi componenti elettrici presenti nel Data center, installare un sistema antincendio comprensivo di rilevatori di fumo/fiamme e sistemi di spegnimento è fondamentale per garantire la sicurezza del data center e un rapido ripristino in caso di guasto. I sistemi di rilevazione dovrebbero essere installati al di sotto della pavimentazione rialzata, in ottemperanza alla normativa NFPA 72°. Il sistema di rilevazione dovrebbe provvedere sia rilevatori di calore, sia rilevatori di fumo, entrambi interconnessi con il sistema di spegnimento dell'incendio, con il sistema di allarme locale, e il sistema di monitoraggio/allarme centrale. I rilevatori devono essere disposti in relazione ai flussi d'aria (garantiti dal sistema di



raffreddamento) per garantire la massima sensibilità rispetto a eventuali picchi di calore e/o principi di incendio. Il sistema di spegnimento prevede quattro categorie:

- Predisposizione di pareti antincendio.
- Installazione di ugelli erogatori (sprinkler).
- Installazione di un sistema di spegnimento che utilizzi agenti chimici «clean agent» come prima linea di difesa.
- Predisposizione di sistemi/postazioni manuali attrezzate con materiali antincendio.

BIA/RPO/RTO

L'analisi BIA/RPO/RTO si focalizzano sui requisiti che devono possedere i sistemi, così da classificare i Data Center secondo una importanza relativa. Il sistema di classificazione viene tradotto in requisiti tecnici e policy. I seguenti elementi devono essere compresi appieno per ogni sistema:

- **Recovery Point Objective (RPO)** definisce il carico di dati che è possibile gestire in fase di recovery, determinando il più recente punto di ripristino.
- **Recovery Time Objective (RTO)** è il tempo necessario per ripristinare i sistemi a seguito di un disastro, o il tempo per il quale il business può «sopravvivere» in caso di assenza dei sistemi.
- **Network Recovery Objective (NRO)** definisce il tempo necessario per ripristinare il funzionamento delle reti in caso di disastro.

È importante considerare che il «livello di recovery» non sarà mai completo qualora i Clienti non possano accedere ai sistemi a causa di problemi di rete. Molti dei livelli (tiers) descritti definiscono l'abilità di recuperare i dati in caso di disastro. La distinzione tra i livelli si basa sulla velocità di recupero dei dati (RTO), sui tempi di ripristino dei servizi e sulla quantità di dati che viene recuperata (RPO). Tuttavia, una soluzione di disaster-recovery dovrebbe essere selezionata in base a dei criteri connessi allo specifico business, tenendo conto dei potenziali costi dovuti al downtime (i.e., perdita di dati, mancati ricavi, etc.). Tanto minore sarà il periodo necessario per ripristinare i dati/servizi, tanto maggiore sarà il costo della soluzione. Di contro, tanto maggiore sarà il tempo impiegato dalla società per ripristinare il proprio Data Center, tanto più alti saranno i costi che dovrà pagare per l'interruzione del servizio. Inoltre è fondamentale comprendere che i costi di una soluzione devono essere proporzionali al valore del business. Sarà quindi auspicabile non spendere per una soluzione di DR una cifra superiore alla potenziale perdita derivabile dal disastro. L'importo di tale perdita può essere determinata da esperienze passate, da Business Impact Analysis (BIA), da risk-assessment e da piani di sicurezza. Non vi è dubbio che il valore dei dati è molto elevato e per questo i downtime possono avere un costo molto elevato. In molti casi, ad esempio per le istituzioni finanziarie, le società devono dotarsi di altissimi livelli di servizio per far fronte a eventuali disastri, sia in termini di protezione, sia in termini di capacità di recupero.

ANALISI FORCSS

L'analisi FORCSS fornisce un metodo per individuare e confrontare i vantaggi, i costi e gli impatti che presentano varie alternative per la progettazione di un Data Center

F	FINANCIAL	<ul style="list-style-type: none">• Impatto sui ricavi• Costi di gestione• Necessità di finanziamenti e di denaro
O	OPPORTUNITY	<ul style="list-style-type: none">• Time to value• Scalabilità• Sinergie col Business
R	RISK	<ul style="list-style-type: none">• Costi di inattività vs disponibilità• Livelli di sicurezza• Flessibilità della fornitura
C	COMPLIANCE	<ul style="list-style-type: none">• Governo delle decisioni• Politiche aziendali• Certificazioni e adeguamento agli standard
S	SUSTAINABILITY	<ul style="list-style-type: none">• Emissioni di CO₂ e consumo di acqua• Certificazioni in ottica «green»• Indice PUE*
S	SERVICE QUALITY	<ul style="list-style-type: none">• Disponibilità di servizio• Performance di servizio• Customer satisfaction

L'analisi FORCSS offre alle aziende gli strumenti per sviluppare risposte concrete e flessibili rispetto alle diverse esigenze organizzative.

Architettura 3 TIER

CARATTERISTICHE DEL MODELLO AS-IS

Architettura composta da 3 livelli
(three-tier)

Utilizzo dello spanning tree protocol per
eliminare i loop

Ethernet

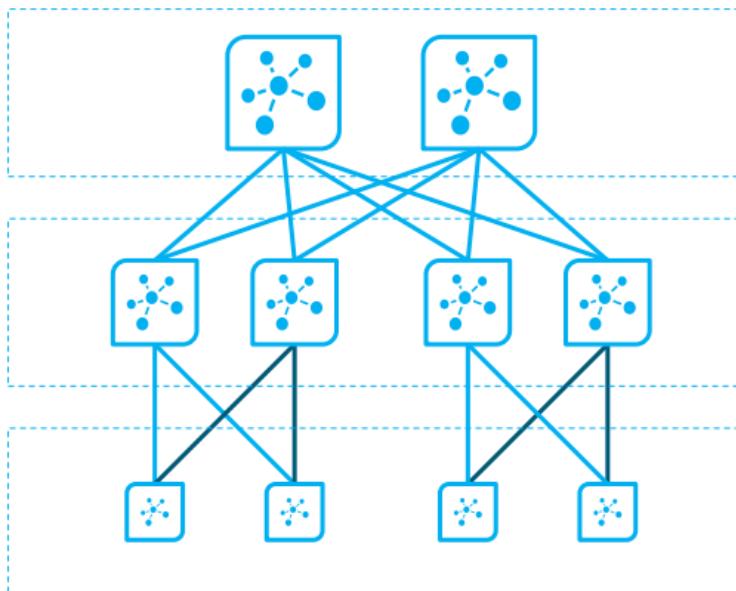
Separazione del data network dalla storage
network

DRIVER DI CAMBIAMENTO

- Uno dei primari fattori che guidano il cambiamento dei Data Center LAN è la **virtualizzazione dei server**
- Adozione di **iniziativa specifiche per le organizzazioni IT** in grado di fornire comunicazioni ad alta affidabilità, bassa latenza, ad elevata larghezza di banda sia tra server fisici che virtuali

UN APPROCCIO INNOVATIVO PER IL MIGLIORAMENTO DELLE COMUNICAZIONI SERVER-TO-SERVER È CARATTERIZZATO DALL'EVOLUZIONE DELL'ARCHITETTURA DA 3 A 2 LIVELLI (ACCESS LAYER E AGGREGATION/CORE LAYER SWITCHES)

L'architettura a 3-tier è quella maggiormente utilizzata dagli attuali data center ed è ancora il principale framework per il design dei nuovi network



CORE SWITCHES

Questi switch smistano il traffic verso i server da una intranet a internet, attraverso gli aggregation switches

AGGREGATION SWITCHES

L'ampiezza di banda può essere saturata, causando un aumento della latenza e la riduzione delle performance

ACCESS SWITCHES

Questi switch sono connessi ai server e agli storage di rete, nonchè agli Aggregation Switches tramite ethernet

Evoluzione Data center networking

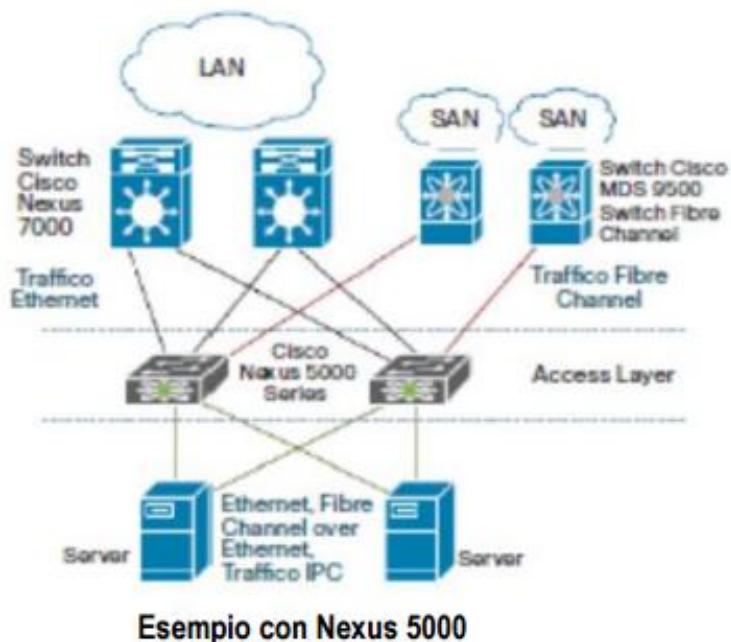
I tradizionali switch enterprise avevano già un primo concetto di virtualizzazione:

- venivano utilizzate le VLAN, che sono un sistema utilizzato per dividere una subnet da un'altra e far sì che non comunichino tra loro.
- Attualmente l'architettura degli switch può fornire oltre 15 Terabit al secondo (Tbps) e in futuro supporterà Ethernet a 40 Gbps e 100 Gbps.

I nuovi switch hanno ripreso tutte le funzionalità degli switch precedenti e in più hanno elevato il livello di virtualizzazione:

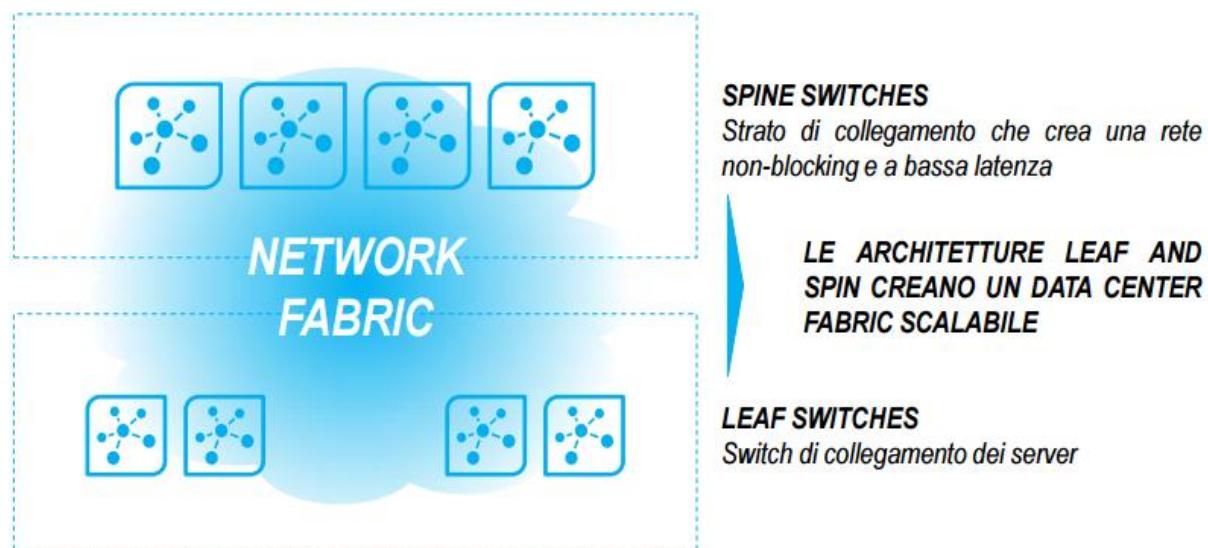
- la Virtual Device Context, che serve a suddividere a livello logico lo switch in più parti. Vengono divise non solo le porte ma anche i prompt di comando. In definitiva è come se si disponesse di due apparati diversi ed autosufficienti aventi in comune solamente il fatto che nel caso in cui la CPU venga attaccata ne risentono tutte le VDC create.
- In definitiva a livello di rete vi è quindi una semplificazione e una riduzione degli apparati. Gli switch possono essere segmentati in dispositivi virtuali secondo le esigenze aziendali. I Virtual Device Contexts (VDC) garantiscono una reale segmentazione del traffico di rete, isolamento e gestione dell'errore a livello di contesto attraverso la creazione di partizioni hardware e software indipendenti.
- I VDC riducono le spese di investimento e di gestione ottimizzando il consumo di energia elettrica, le esigenze di spazio, l'utilizzo dei dispositivi, le operazioni di manutenzione e la velocità del sistema.

I nuovi switch offrono un'architettura innovativa per semplificare la trasformazione dei Data Center, abilitando una standard-based Ethernet unified fabric ad elevate prestazioni. La nuova tecnologia permette di consolidare ambienti separati di rete Local Area Network (LAN), Storage Area Network (SAN) e server cluster in un'unica unified fabric.



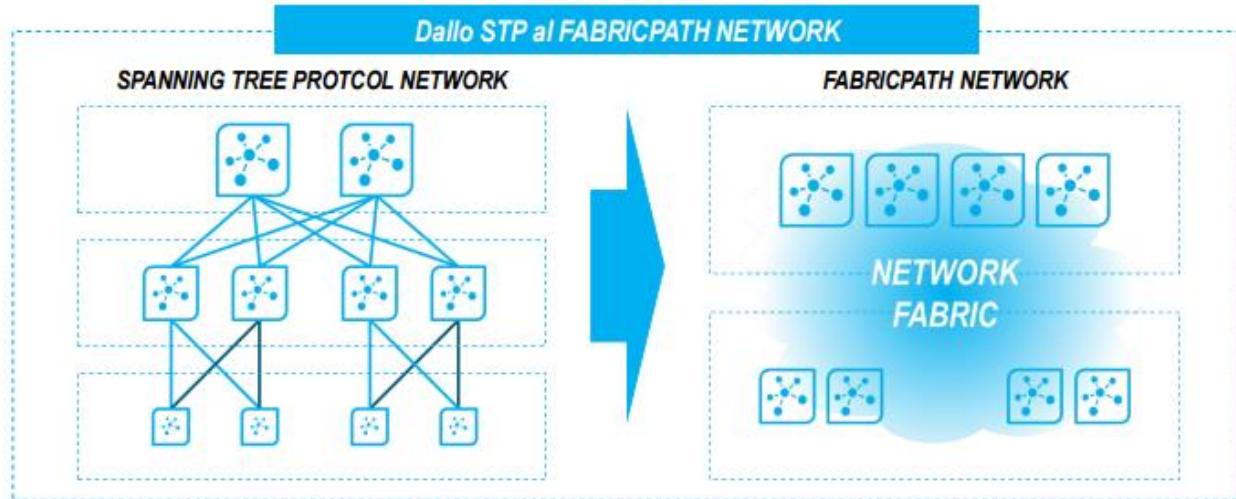
Architettura a due livelli: Leaf-Spine Network Fabric

AL FINE DI PROGETTARE UN'ARCHITETTURA CHE INCONTRI UNA DOMANDA EMERGENTE, MOLTI RESPONSABILI HANNO BISOGNO DI UN DATA CENTER FABRIC SPESSO CHIAMATO «FAT-TREE», BASATO SU DUE TIPI DI SWITCH:

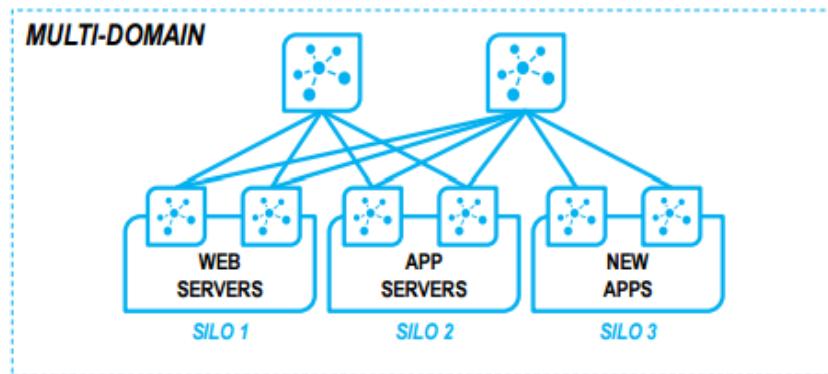


Dallo Spanning Tree Protocol al FabricPath

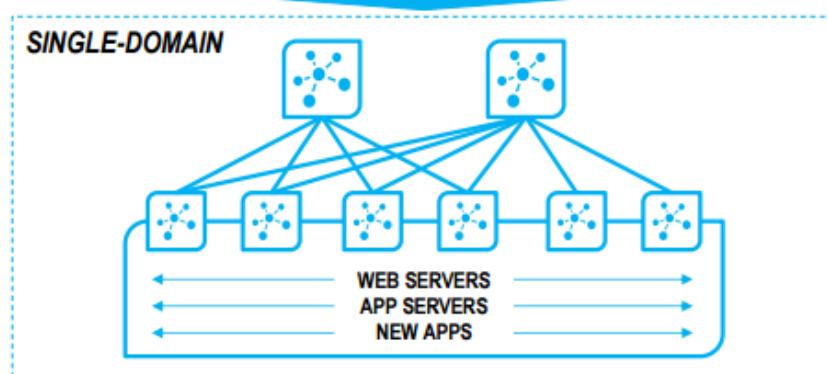
FABRICPATH offre un'alta disponibilità in quanto elimina lo SPANNING TREE PROTOCOL (STP), che permette un solo percorso, e lo sostituisce con percorsi multipli



Workload Mobility: dal Multi-Domain al Single-Domain



In un multi-domain network, molti architetti IT segmentano le applicazioni come ad esempio i web servers, CRM, etc. Questo approccio incrementa la cross-sectional bandwidth grazie a 3 livelli di demarcazione (silos) ma è poco flessibile.



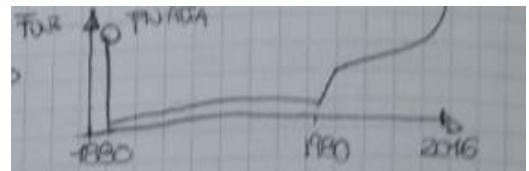
Un single-domain layer connette tutti i server, offrendo un network fabric più scalabile e flessibile. Gli Architetti IT sono così in grado di scalare in modo più ampio con le barriere di sottorete eliminate, permettendo ad una VLAN di estendersi su tutta l'infrastruttura fisica.

10.0 SERVIZI MULTIMEDIALI – VOCE SU IP

Come codifico la voce, quanti bit servono e come sono i server che permettono di far viaggiare la voce in rete?

VOCE

Le prime reti per le voci sono state le reti telefoniche, nate alla fine dell'800. Dal punto di vista della ricchezza della funzionalità, facendo un grafico, negli anni 80 ha una rapida crescita perché prima la commutazione per telefonare, veniva fatta manualmente dalle operatrici; dopo la commutazione divenne automatica.



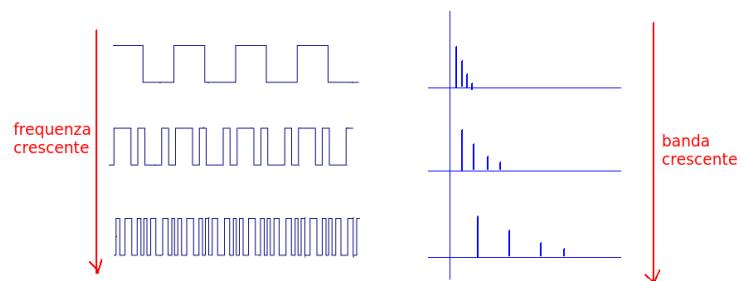
Una cosa è rimasta uguale: la gente parla, bisogna trasportare un segnale in fonia. Il segnale in fonia è rimasto per gran parte del tempo analogico. Oggi il segnale che proviene dalla nostra voce, viene raccolto da un microfono, trasformato in un segnale elettrico, campionato trasformato da segnale analogico in numerico, pacchettizzato e trasferito su una linea digitale. Nella rete analogica, il segnale si degrada in maniera significativa e i disturbi nel lungo percorso portano alla degradazione del segnale. Gli amplificatori lungo il percorso amplificano il rumore ma anche il rumore. In una rete analogica quando entra il rumore non si toglie più.

In una rete numerica, il rumore può essere eliminato. Il segnale può subire disturbi, ma comunque ricostruisco lo stesso segnale di partenza. Come trasformo il segnale analogico in digitale?

1. **CAMPIONAMENTO:** prendo dei campioni di segnale a ogni t (tempo). Il tempo che passa tra due campionamenti, lo chiamiamo t_c ed è il tempo di campionamento. La frequenza di campionamento è uno dei parametri fondamentali che caratterizzano il processo di conversione analogico-digitale nei sistemi elettronici di elaborazione dell'informazione.

Il dispositivo che realizza la conversione da segnale analogico a segnale digitale viene detto convertitore A/D. La frequenza di campionamento indica il numero di campioni registrati in un secondo. Qual è il rapporto tra velocità di cambiamento di segnale e la frequenza di campionamento? A cosa è legata la velocità con cui cambia il segnale? Alla banda¹ del segnale. Maggiore è la banda del segnale, più variazioni ci sono e più campioni devo fare. Esiste un teorema, **teorema del campionamento** e dice che la frequenza di campionamento $F_c = 1/T_c$ deve essere almeno grande quanto 2 volte la banda in Hertz.

Ad esempio, un segnale audio ha uno spettro compreso fra 20 Hz e 20 kHz: per poter registrare il segnale su un supporto digitale (come, un CD audio) la frequenza di campionamento deve essere almeno di 40 kHz. Usualmente, tale campionamento viene effettuato a 44.1 kHz, valore che soddisfa appieno il teorema e che consente di ricostruire fedelmente il segnale analogico di partenza.

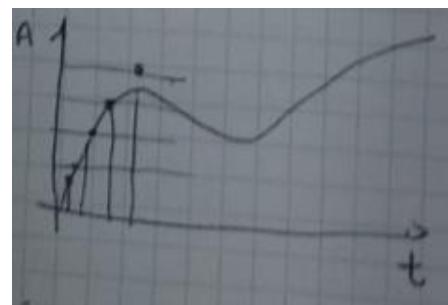


¹ In informatica e in telecomunicazioni, il termine banda indica la quantità di dati informativi che possono essere trasferiti, attraverso una connessione, in un dato periodo di tempo, e la cui ampiezza è in analogia con l'ampiezza di banda in campo fisico. In generale, più alta è la frequenza, più alta è la larghezza di banda disponibile.

Le reti telefoniche sono nate avendo come idea di base, quella di trasmettere la voce umana, che ha una banda che va da 300Hz a 3400Hz. La F_c nelle reti telefoniche è: $F_c = 8000 \text{ Hz} = 8 \text{ KHz}$ quindi il tempo di campionamento è di $T_c = 125 \text{ Microsecondi}$; ogni 125 microsecondi io prendo un campione del mio segnale voce. Questo campione è un livello di ampiezza. Il livello di ampiezza deve essere trasformato in un numero e quindi procedo con una quantizzazione.

2. **QUANTIZZAZIONE:** se ho un segnale che varia nel tempo e ho un'ampiezza, devo stabilire dei livelli rappresentati da un numero finito di bit, che costituiscono i miei livelli di quantizzazione.

Assegno a ogni campione effettuato a un certo istante, un valore discreto. C'è un errore introdotto, che è il **rumore di quantizzazione** (pallino al di sopra dell'onda). È un qualcosa di inevitabile. Avendo un segnale che varia continuamente di ampiezza, avremo sempre un'imprecisione. Tuttavia se definiamo un numero sufficientemente grande di livelli, avremo un errore che non è percepibile. Si potrebbe assegnare a ogni livello 8 bit e con 8 bit significa che posso avere 2^8 (256) livelli.; mai usato un metodo così "stupido". Si è pensato subito di inserire qualcosa tale che permetesse di dividere meglio: i livelli non sono a una stessa distanza, ma partono fitti per distanziarsi man mano. Normalmente la soluzione più semplice per catturare la voce è questo: io ho un campione a 8 KHz e utilizzo 8bit/campione. Ottengo un segnale a 64 Kbps, che è il segnale voce numerica, il famoso standard **PCM**.



Un **Codec**, ovvero un codificatore voce che utilizza PCM, corrisponde a uno standard G711, con qualità molto elevata.

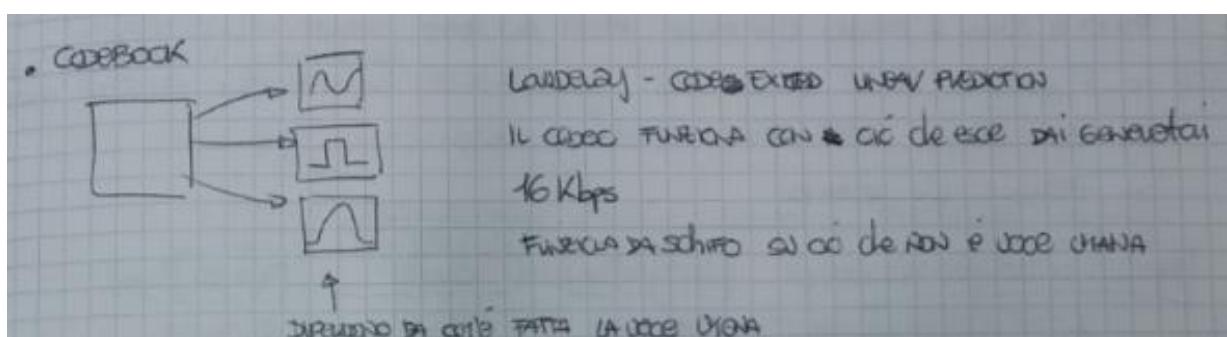
Si sono studiati meccanismi di codifica sempre più complessi. Possiamo ridurre i 64 Kbps in qualche maniera? La prima tecnologia utilizzata per ridurre la banda del segnale, è stata l'**ADPCM**. Conviene dal punto di vista della codifica, non codificare il livello del segnale, ma le differenze tra un campione e l'altro. Codificare come fa l'ADPCM porta a un certo degrado della qualità.

Un altro standard è il **G726**. Mi vengono date diverse opzioni: il segnale può essere campionato a 16, 24, 32, 40 Kbps; 32 Kbps, la metà dei 64, è quello più utilizzato.

Sia l'ADPCM che il G726 hanno una cosa in comune: **waveform codecs**.

I waveform codecs è un codificatore che prende il segnale con la sua forma d'onda e cerca di replicarlo al destinatario. È in grado perfettamente di trasportare un segnale audio purché sia di un determinato formato.

Successivamente vennero definite delle **primitive**: esse sono un insieme di possibili



generatori di forme d'onda di un certo tipo a frequenze diverse, sempre nel range vocale. Ognuno di questi generatori, caratterizza una componente presente nel segnale vocale umano. Inoltre io ho una parola di codice che mi permette di attivare o spegnere ognuno di questi generatori di segnale. La parola di codice che fa parte di un **codebook**, è un insieme

di bit che attivano e disattivano questi generatori per un certo periodo. Il primo di questi codici è il lowdelay-codec exited-linear prediction.

Altri codec sono:

- **G729**: produce un segnale a 8 Kbps di qualità molto elevata. È utilizzata da Skype.
- **G723.1**: può codificare la voce a 5.3 Kbps e/o 6.3 Kbps

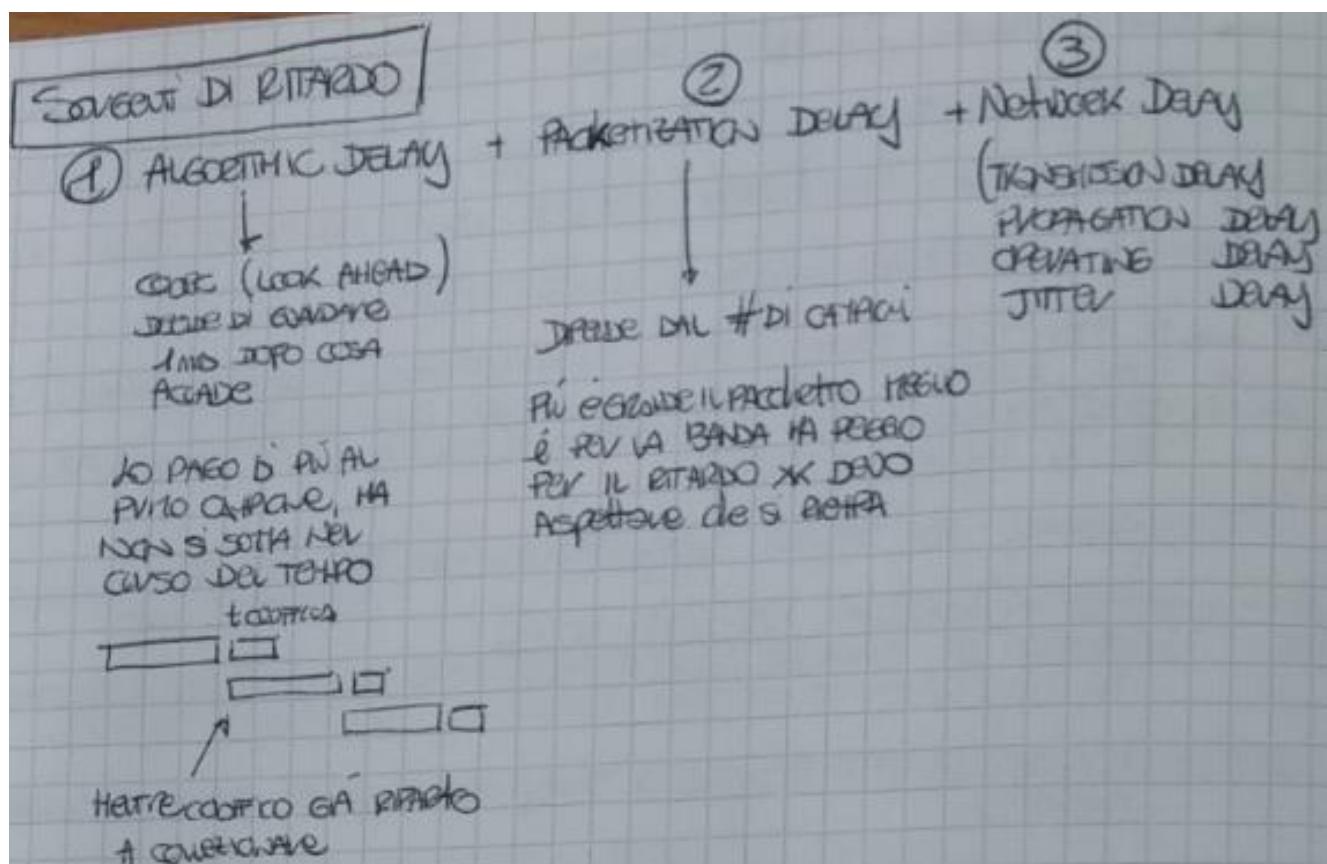
QUALITA' DEI CODEC

Come valuto la qualità dei codec? Ci sono due modi:

- **Misura oggettiva della qualità** (modello di distanza tra segnale originale e cod/decod).
- **MOS (Mean Opinion Score)**: si prende un gruppo di persone e faccio ascoltare un segnale e mi dai un feedback. È una misura percettiva della qualità della voce.

CODEC	CAMPIONAMENTO	SCORE
G711	64 Kbps	4.3-4.4
G726	32 Kbps	4.0-4.2
G728	16 Kbps	4.0-4.2
G729	8 Kbps	4.2
G723.1	6.3 Kbps	3.8

SORGENTI DI RITARDO



3 tipi di ritardi:

- **Algorithmic delay** dipende dal codec. È il ritardo che io devo considerare perché venga eseguito l'algoritmo del codec. Il ritardo non diventa nullo con il progresso della tecnologia. Alcuni codec hanno dentro un look ahead: se codifico quello che succede in questo istante

di tempo posso guardare quello che è successo prima, ma posso guardare anche quello che succederà dopo perché c'è continuità del segnale. Se quando codifico, aspetto un po' e guardo cosa succede qualche millisecondo dopo, posso avere una codifica migliore di quella che succede in questo momento. Quel ritardo è ineliminabile.

- **Packetization delay:** dipende dal numero di campioni in un pacchetto. È legato alla codifica. Più grande è il pacchetto meglio è per la banda, ma peggio per il ritardo perché devo aspettare che il pacchetto si riempia.
- **Network delay:**
 - transmission delay
 - propagation delay
 - operating delay

Qualsiasi dispositivo per riprodurre un segnale, ha una parte analogica che non è perfettamente bilanciata e spesso genera un segnale all'indietro che ritorna a me. Se il ritardo end to end è molto basso io non sento la mia voce che ritorna indietro e non nessun disagio. Tuttavia se il ritardo è grande, la mia voce la sento e provoca un disagio. Per ovviare a questo, si utilizzano dei dispositivi che confrontano il segnale, cancellano, attenuano questo segnale. Quindi:

- Fino a 25 ms no cancellatori DECO
- Tra i 25 ms – 150 ms di ritardo devo usare un cancellatore DECO
- Sopra i 150 ms la qualità del segnale è tale da provocare un disagio

Blocco di dati	Su cui lavora	Look Ahead	Pacchetto con quanto?	Payload (byte)
6.711	0,125 ms	Nullo	20 ms	160 byte
6.726	0,125 ms	Nullo	20 ms	80 byte (30Kbps di air)
6.728	10 ms Prede 10ms e fa 10ms	0,625 ms	20 ms	40 byte (16Kbps)
6.729	10 ms	5 ms	20 ms	20 byte (8Kbps)
6.723,1	30 ms	7,5 ms	30 ms	20 byte (5,3Kbps)

↳ Pacchetti + header, periodo di codifica
ad una fine del pacchetto + header

Dove \rightarrow e \rightarrow indica i campioni di voce e ci fa pensare che:

Il payload dove sta? nel pacchetto, che può essere intestazioni relative a determinati protocolli

① Pacchetto P \rightarrow intestazione 20 byte

② ~~ma~~ UDP \rightarrow 8 byte

③ RTP QUANDO APP VOIP INIZIAVA IL PROPRIO PAYLOAD DI PROPRIO HEADER, PER ESEMPIO

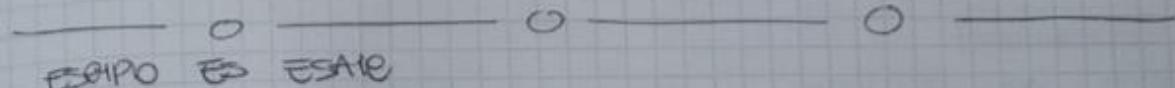
60 byte che sono trochi ma non troppo trochi

G.711	64Kbps \rightarrow overhead $\cdot \frac{200}{160} = 80\text{Kbps}$	}
G.726	$32\text{Kbps} \cdot \frac{120}{80} = 48\text{Kbps}$ e non più 32	
G.728	$16\text{ Kbps} \cdot \frac{80}{40} = 32\text{ Kbps}$ e non più 16	
G.729	$8\text{ Kbps} \cdot \frac{60}{20} = 24\text{ Kbps}$ e non più 8	

velocità che aumenta
a livello 3

ALTERNATIVE:

① ATTIVARE LA SOPPRESSIONE DEI SILENZI (il sov. della chiamata unica velocità è zitti)



Se 20 conversazioni contemporanee usi codec G728, overhead L2 da 10%.
Quanti byte usano insieme?

$$\begin{array}{rcl}
 50 \cdot 16\text{ Kbps} \rightarrow \text{traffico utile} & \rightarrow & 800\text{ Kbps payload} \\
 + \text{overhead } @ 10\% & & \rightarrow 800\text{ Kbps} \\
 & & \hline
 & & 1600\text{ Mbps} \quad L_3 \\
 & + & \\
 & & 0,16\text{ Kbps} \\
 & & \hline
 & & 1,76\text{ Mbps}
 \end{array}$$

se ci fosse soppressione silenzio farei un 50%.

Attenzione: sopra sono 64 Kbps di payload, non 64 Kbps di overhead!

Nelle reti di telecomunicazioni, il termine "overhead" si riferisce a quella parte di banda di trasmissione che viene utilizzata per spedire, anziché l'informazione utile, dati aggiuntivi necessari per i protocolli di trasmissione stessa (per esempio SDH o PDH) e per il monitoraggio, la gestione e il controllo della rete stessa, sia da parte di meccanismi automatici (per esempio, protocolli di protezione di rete) che da parte di sistemi di gestione esterni, per esempio per segnalare condizioni di guasto o per consentire la configurazione della rete tramite sistemi remoti centralizzati. Il contenuto e il significato delle informazioni di overhead dipende dal tipo di protocollo di trasmissione utilizzato.

Quando la banda è poco costosa codifico con G 711. Diversamente quando la banda costa e le distanze sono lunghe dobbiamo considerare altre codifiche. Possiamo ridurre i Kbit trasmessi utilizzando i soppressori di silenzi (50% risparmio) ed effettuando compressioni sull'header (da 40 byte a 5 byte).

All'esame verrà data la tabella sottostante per poter risolvere gli esercizi:

Alcuni codec utilizzabili in applicazioni VoIP

	Blocco di codifica		Lookahead	Pacchetti generati	Payload	Overhead	Banda IP
	ms	byte	ms	pps	byte	%	kbps
G.711 (64 kbps)	0,125	1	0	50	160	25%	80
G.726 (32 kbps)	0,125	1	0	50	80	50%	48
G.726 (24 kbps)	0,125	1	0	50	60	67%	40
G.728 (16 kbps)	10	20	0,625	50	40	100%	32
iLBC (15,2 kbps)	20	20	5	50	38	105%	31,2
iLBC (13,3 kbps)	30	30	10	33,33	50	80%	24
G.729 (8 kbps)	10	10	5	50	20	200%	24
G.723.1 (6,3 kbps)	30	24	7,5	33,33	24	167%	17,07
G.723.1 (5,3 kbps)	30	20	7,5	33,33	20	200%	16

La percentuale di overhead è data dal seguente rapporto: 40 byte (overhead)/xx byte (payload).

VIDEO

Il video è del tutto diverso dalla voce. Al video corrisponde generico audio. Il segnale video utilizza dei meccanismi di compressione. Noi vediamo il video come una serie di immagini, una dietro l'altra. Dobbiamo ragionare su due parametri:

- Parametro temporale, frequenza con cui trasmetto il mio segnale, ovvero gli fps (frame per second).
- Quanto è dettagliata l'immagine, quanti pixel io trasmetto e con che definizione.

La terza dimensione che utilizzo è il numero di bit che utilizzo per ciascun pixel. I video viaggiano normalmente fra i 30 e i 100 Hz (immagini al secondo). I 100 Hz sono migliori dei 50 Hz dal punto di vista percettivo.

Il video può essere:

- **Interallacciato (I)**
- **Progressivo (P)**

Se io trasmetto un video a 25 fps si vede lo sfarfallio. Ma se trasmetto le righe pari in un quadro e le dispari nel quadro successivo, l'occhio percepisce un segnale quasi pari a 50 fps. In termini di bit trasmessi è importante. Il progressivo trasmette il quadro completo a ogni passo.

Quanti sono i pixel di un video? 1920x1080.

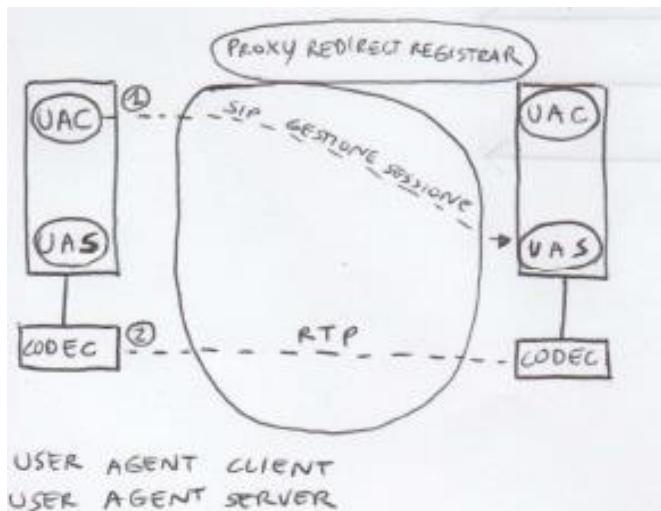
Quanti bit al pixel? 24 bit (3 colori, RGB, e per ciascuno 8 bit -> 3 x8=24).

Questo è il mio video grezzo. Se faccio: 1920x1080x24x50 = roba assurda 2.5 Gbps di video grezzo. Devo comprimere e il livello di compressione è molto superiore a quello del segnale audio. Come si fa a comprimere?

Ridondanza spaziale: quello che ho un pixel è molto legato a quello che ho nel pixel affianco. Posso utilizzare delle tecnologie che mi permette di tener conto di questa ridondanza spaziale. Taglio quindi frequenze spaziali. Prendo il segnale e lo trasformo e lavoro in uno spazio di trasformate:

1. **DCT** (Discrete Cosine transform)
2. **Quantizzazione** dei coefficienti che non è di tipo lineare, cioè i coefficienti corrispondenti alle alte frequenze vengono codificati con meno bit rispetto alle basse
3. **Codifica a blocchi** tipo non lossy. Se un segnale ha ridondanza, ci sono meccanismi di codifica, di comprimerlo senza perdere informazioni.

VOIP E SIP



Per il voip utilizzo il **Session Initiation Protocol** per iniziare una sessione voip. La voce a pacchetto, abbiamo visto prima come viene codificata, con più varianti. Come gestisco le sessioni? Questo problema è diverso da come gestisco una sessione con il server. Quando parliamo con un server abbiamo un indirizzo. Quando applichiamo il concetto alla persona, essa può non essere nello stesso posto. Non mi basta il server, la richiesta deve andare verso l'utente che sta dall'altra parte. Il soggetto terminale della sessione può aprire a sua applicazione voip su un altro dispositivo. Esempio: skype. La rete capisce quando ci connettiamo e disconnettiamo da un'altra parte. Qua si applica il concetto di **nomadismo**: possibilità di avere più postazioni e deve tenere traccia di dove finisce l'utente. Gli elementi architetturali sono:

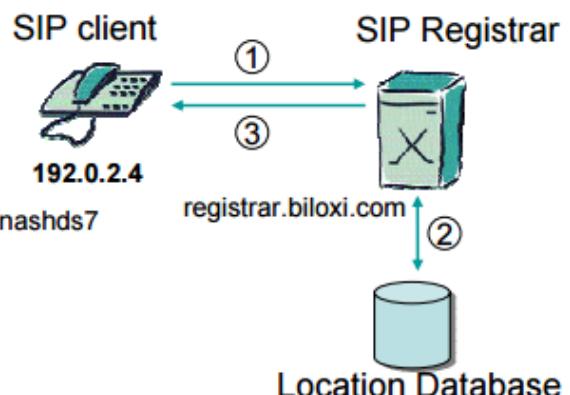
- User agent costituito da due componenti:
 - **UserAgent Client (UAC)**: entità che genera le Request e che invia la richiesta allo User Agent Server
 - **UserAgent Server (UAS)**: entità che riceve Request e può generare Response per accettarle, respingerle o indirizzarle altrove.

SIP: esempio di registrazione

1. Il client SIP invia una *Request REGISTER* a registrar.biloxi.com

```
REGISTER sip:registrar.biloxi.com SIP/2.0
Via: SIP/2.0/UDP bobspc.biloxi.com:5060;branch=z9hG4bKnashds7
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Bob <sip:bob@biloxi.com>;tag=456248
Call-ID: 843817637684230@998sdasd09
CSeq: 1826 REGISTER
Contact: <sip:bob@192.0.2.4>
Expires: 7200
Content-Length: 0
```

2. Il SIP registrar associa la URI del "Contact:" all'address-of-record presente nell'Header "To:"
3. Il SIP registrar risponde al client SIP comunicando la lista dei contact-address associati

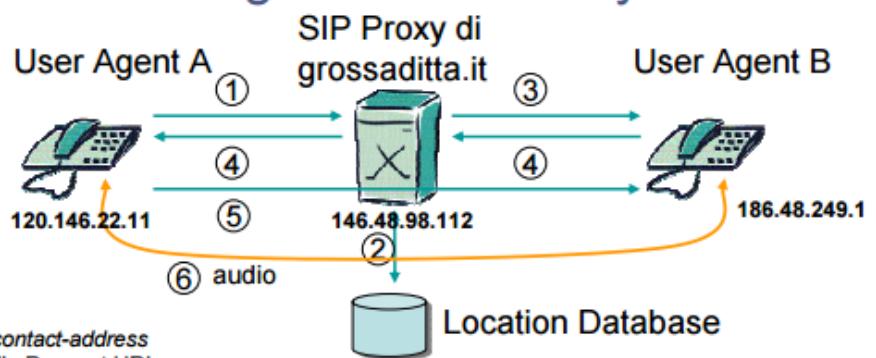


```
SIP/2.0 200 OK
Via: SIP/2.0/UDP bobspc.biloxi.com:5060;.....
.....branch=z9hG4bKnashds7;received=192.0.2.4
To: Bob <sip:bob@biloxi.com>;tag=2493k59kd
From: Bob <sip:bob@biloxi.com>;tag=456248
Call-ID: 843817637684230@998sdasd09
CSeq: 1826 REGISTER
Contact: <sip:bob@192.0.2.4>;expires=7200, ...
...<sip:robert@192.0.3.10>;expires=1320
Content-Length: 0
```

Attivazione di dialogo via SIP Proxy

- l'UAC di A invia una INVITE al SIP Proxy "grossaditta.it" (l'indirizzo di trasporto viene ricavato dal DNS)

```
INVITE sip:bob@grossaditta.it SIP/2.0
Via: SIP/2.0/UDP 120.146.22.11:5060;...
To: sip:bob@grossaditta.it
From: sip:alice@grossaditta.it;tag=aaa...
Call-ID: ccc...
CSeq: 1 INVITE
Contact: sip:alice@120.146.22.11:5060
.....
```



- Il SIP proxy cerca nel location database i *contact-address* associati all'*address-of-record* presente nella Request URI: `sip:bob@grossaditta.it`

- Il SIP proxy inoltra l'INVITE all'unico *contact-address* di B trovato nel location database: `sip:bob@186.48.249.1`

```
INVITE sip:bob@186.48.249.1 SIP/2.0
Via: SIP/2.0/UDP 146.48.98.112:5060;...
Via: SIP/2.0/UDP 120.146.22.11:5060;...
To: sip:bob@grossaditta.it
From: sip:alice@grossaditta.it;tag=aaa...
Call-ID: ccc...
CSeq: 1 INVITE
Contact: sip:alice@120.146.22.11:5060
.....
```

- Quando l'utente B alza la cornetta, l'UAS di B invia una Response "200 OK", che raggiunge l'UAC di A, transitando da tutti gli hop presenti nei "Via:" Header. Lo UserAgent A apprende dalla Response il *contact-address* dello UserAgentB

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 146.48.98.112:5060;...
Via: SIP/2.0/UDP 120.146.22.11:5060;...
To: sip:bob@grossaditta.it;tag=bbb...
From: sip:alice@grossaditta.it;tag=aaa...
Call-ID: ccc...
CSeq: 1 INVITE
Contact: sip:bob@186.48.249.1:5060
.....
```

- L'UAC di A invia un ACK all'UAS di B mandandolo direttamente al *contact-address* presente nel "Contact:" Header della FinalResponse

```
ACK sip:bob@186.48.249.1:5060 SIP/2.0
Via: SIP/2.0/UDP 120.146.22.11:5060;...
To: sip:bob@grossaditta.it;tag=bbb...
From: sip:alice@grossaditta.it;tag=aaa...
Call-ID: ccc...
CSeq: 1 ACK
.....
```

- Le sessioni audio/video fluiscono come concordato nella negoziazione SDP

12/44

- Registrar Server** tipo speciale di UAS che accetta le Request REGISTER e memorizza le informazioni in esse contenute in un "location service"
- Proxy Server** entità che instrada le Request verso gli UAS e le Response verso gli UAC può rispondere direttamente ad una Request (in tal caso opera come UAS)
- Redirect server**

I codec servono per far passare un flusso della voce, video, ovvero il **media stream**. Qui viene utilizzato il protocollo RTP/UDP/IP. Il collegamento tra user agent, è il collegamento di controllo della sessione. Il protocollo che utilizzo a livello applicativo è il protocollo che utilizzo, è il protocollo SIP. Ormai è usato in tutte le reti telefoniche fisse e mobili. Il SIP è un protocollo Text based. La sessione viene creata tramite messaggi, chiamati **metodi**; abbiamo 3 messaggi:

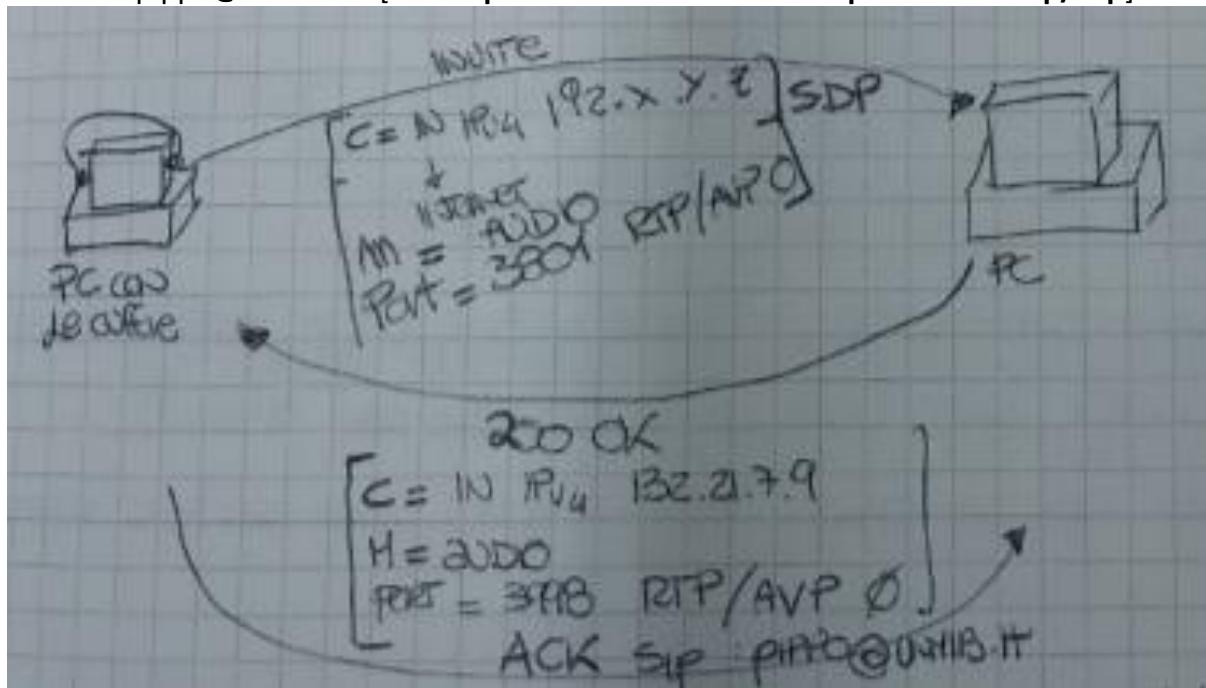
- `Invite()`: invitare un soggetto a partecipare alla sessione;
- `Ack()`: presa conoscenza della conversazione;
- `Bye()`: abbandono conversazione;

Esempio: abbiamo due terminali (**situazione semplice**). Supponiamo che io sappia già dove si trova il destinatario, ovvero mando il messaggio di invite. Il messaggio invite è così costituito:

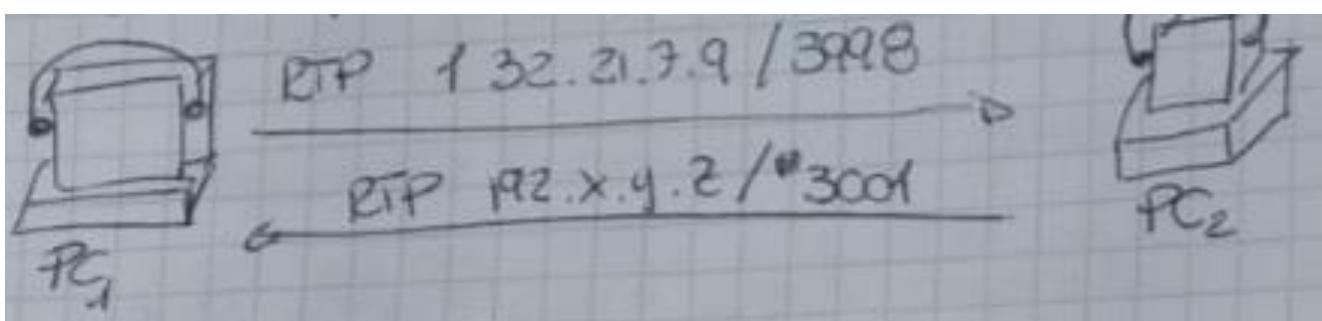
- Ha come prima indicazione una url sip. Una url sip assomiglia a un indirizzo di posta elettronica: `pippo@hotmail.it`
- All'interno ci sono tante cose, ma in particolare un payload che fa parte di un protocollo SDP (Session Description Protocol). Qui dentro troviamo alcune caratteristiche tra cui:

- **C = IN ip4 191.2.170.7**: mi sta dicendo che il codec è su internet (IN), utilizza un protocollo ipv4 e ha l'indirizzo 191.2.170.7. significa che sono in grado di dire in maniera precisa dove si trova il mio codec.
- **M = audio porta =3001 rtp/avp**: mi sta dicendo che M è il media, qual è il media che stiamo trasmettendo. Port, la porta dalla quale sto trasmettendo.

INVITE: pippo@hotmail.it [C = IN ip4 191.2.170.7- M = audio porta =3001 rtp/avp]

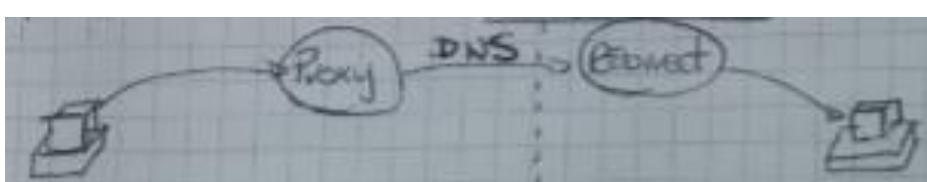


Successivamente devo rispondere all'invite e le risposte possono essere **Bye** oppure **200 OK**. Semando un messaggio 200 OK, ho bisogno dell'ack finale perché devo rispondere ed essere sicuro che l'altro riceva (esempio: ok avvio comunicazione). A questo punto attivo due flussi RTP nelle due direzioni come nell'immagine sotto.



Uno dei due prima o poi manda un messaggio all'altro di tipo **BYE** con risposta **200 OK**.

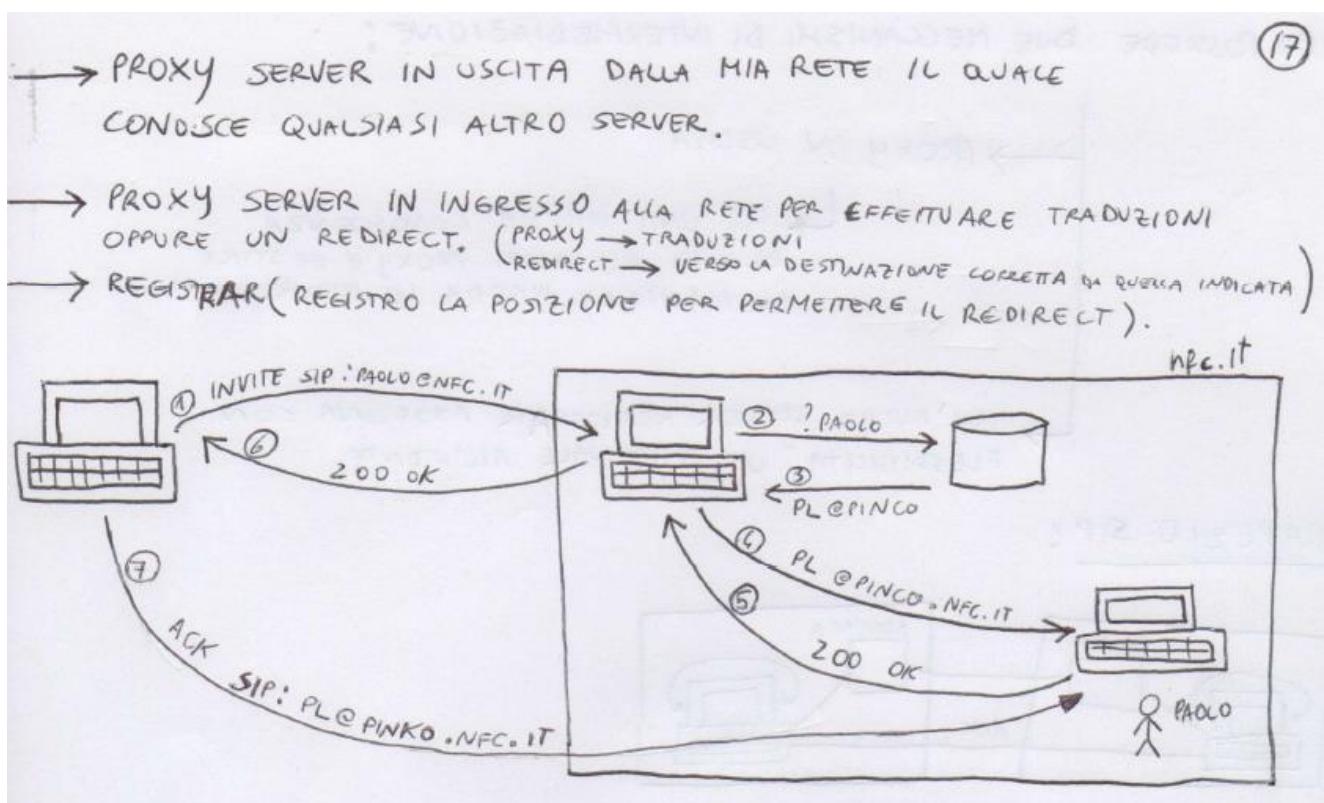
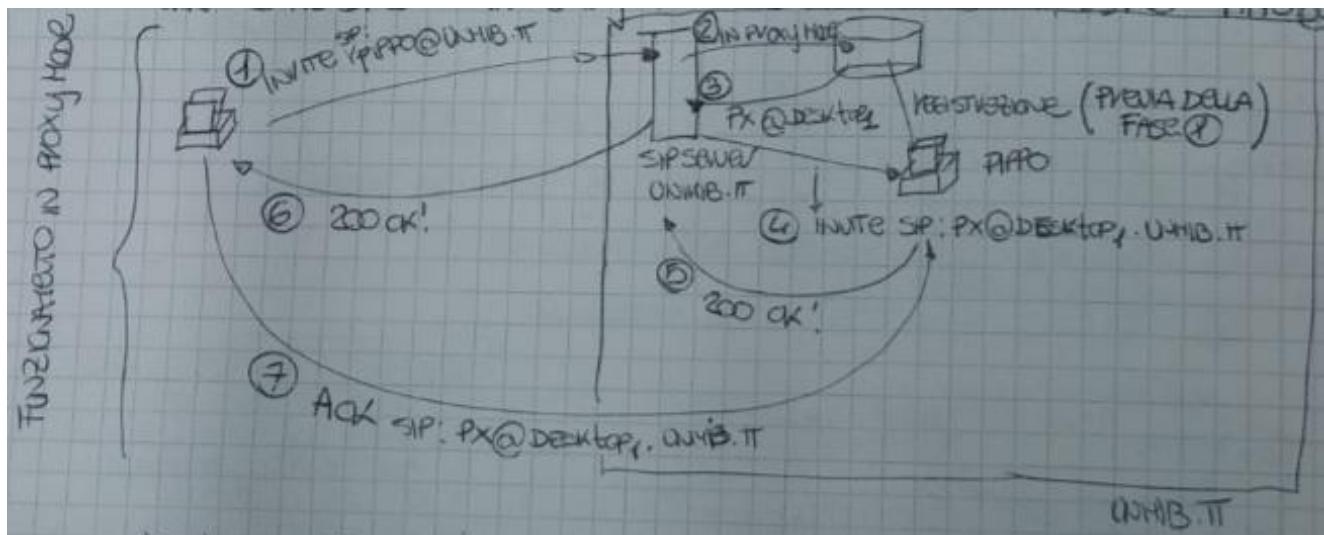
Fin qua tutto bene se sono due client in una rete piccola. Fin qua tutto bene se sono due client in una rete piccola. Se le reti sono più grandi, avrò bisogno di un **Proxy server**, quindi l'invite non lo mando più al destinatario, ma a un intermediario e per trovare il relativo redirect server, usa il **DNS**.



Però ho anche necessità di un **Redirect server** che abbia la stessa funzione del proxy in uscita. Infine ci serve il **Registrar server** che serve per gestire il nomadismo dei client queste 3 macchine (Proxy Server, Redirect Server, Registrar server) sono in un oggetto solo, chiamato **Sip Server**.

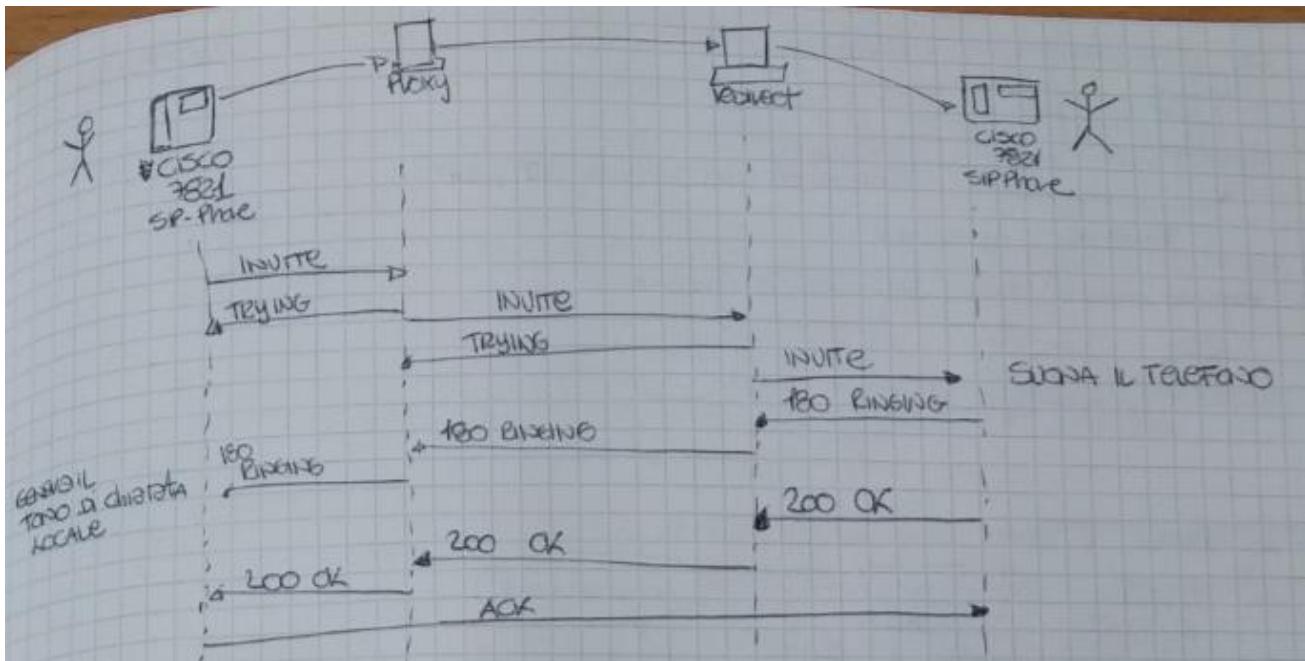
nomadismo dei client queste 3 macchine (Proxy Server, Redirect Server, Registrar server) sono in un oggetto solo, chiamato **Sip Server**.

Esempio: supponiamo di voler invitare alla nostra conversazione pippo@unimib.it:



Dall'punto 7 (ack) in poi, i due parlano direttamente (anche il **BYE** viene mandato tra loro). Il che va bene finchè sono in una lan dove le telefonate non costano. Ed è un problema perché il sip-server non sa quando termina il tutto, quindi non ho il contatore di ciò che ho speso. Nella fase 2 potrei aver risposta "non so il soggetto dove sta" oppure "guarda che si è mosso da un'altra parte e la risposta è **302 moved temporary** con campo "contact pippo@nfl.

Gli schemi di messaggi che ci sono nella telefonia tradizionale sono i seguenti:



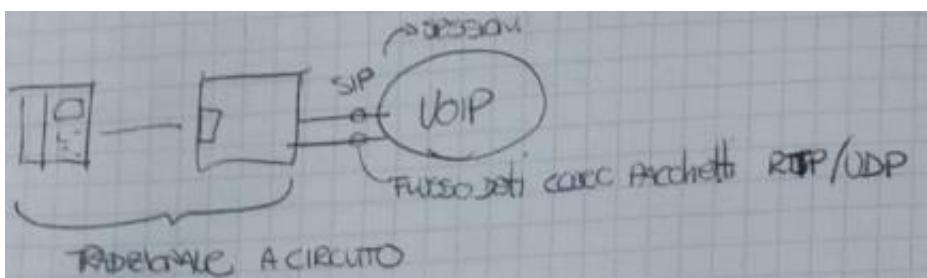
Il trying avvisa il chiamante che la telefonata è partita, mentre i ringing indicano che il telefono del chiamato sta suonando. Abbiamo alcuni problemi:

- Iterlavoro con la rete a circuito
- Terminali non Ip. Il problema attuale è che molti telefoni sono ancora analogici.
- Accounting. Problema da gestire perché le reti telefoniche non sono totalmente gratuite ho bisogno di un registro dei contatori
- Controllo dei media. In lan banda costa zero, in wan non costa zero. Non posso permettere che il link venga sprecato. Se sip dice audio, devo certificare che sia audio.
- Servizi telefonici. Centralini che sembrano stupidi, ma utili, un ambiente ufficio; deviazione, avviso chiamata, inoltro chiamata, melodia d'attesa

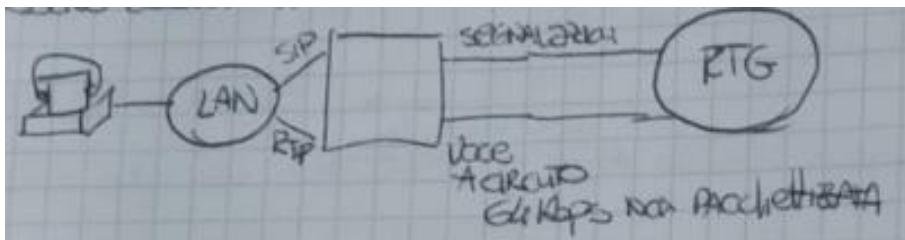
TERMINALI SIP

Abbiamo un tipo di interazione con telefono che si basa sul digitare delle cifre. Ha un'interfaccia analogica in cui le cifre vengono trasmesse in multifrequenza sopra lo stesso collegamento della voce e da qualche parte all'interno della rete le cose cambiano. Possiamo distinguere il problema in due sottoproblemi:

- **Iterlavoro:** terminale di tipo analogico collegato a un dispositivo che capisce la segnalazione e il mondo voip. L'interfaccia deve gestire un flusso di segnalazione di tipo sip, e un flusso dati.

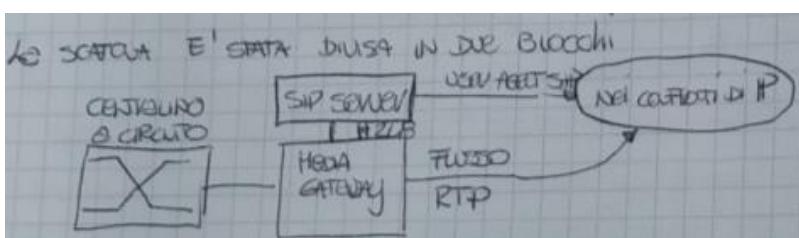


- Caso in cui abbiamo un dispositivo nativo voip. Avremo due flussi, uno sip, e un altro che è ip e dall'altra parte avremo una rete telefonica generale che ha due tipi di segnali: flusso voce circuito e segnalazioni

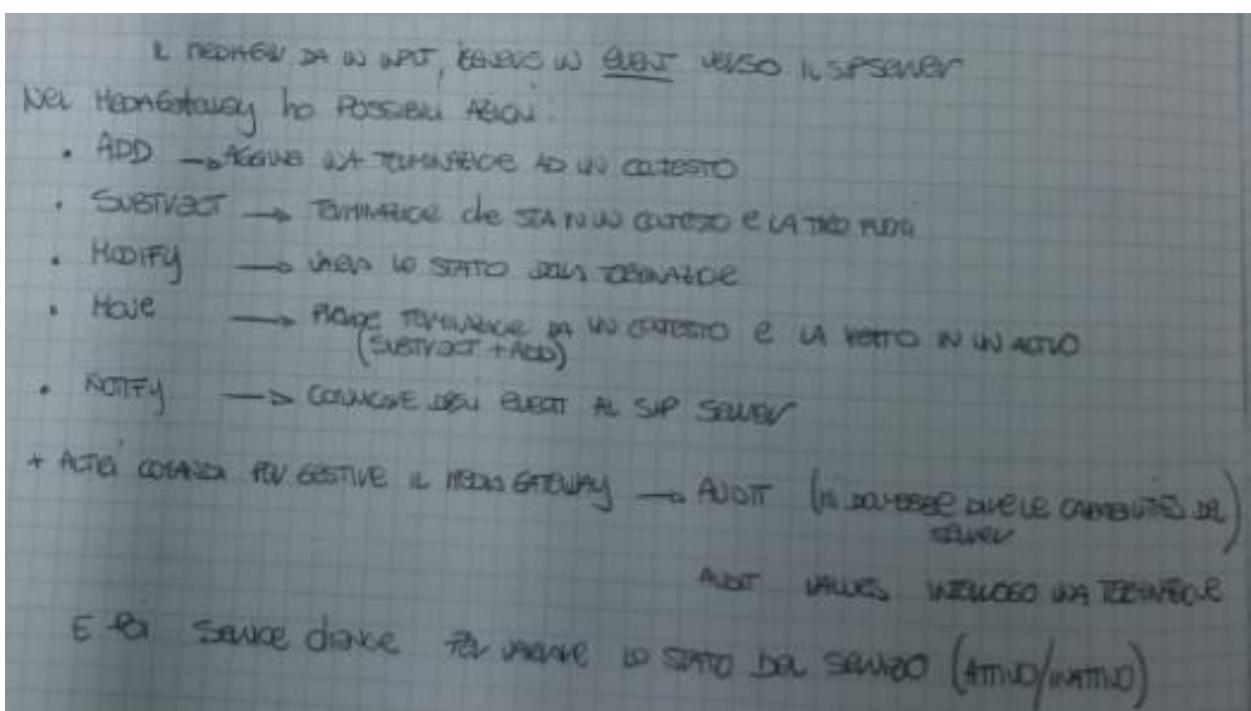
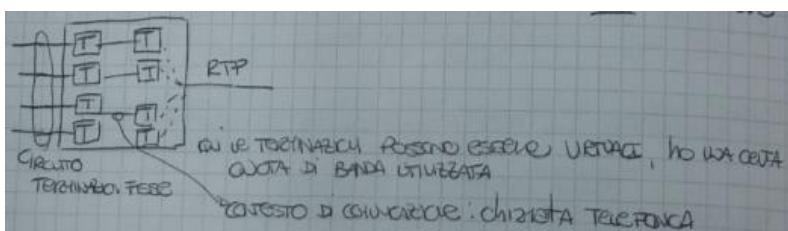


INTERAZIONE TRA TECNOLOGIE DI RETE

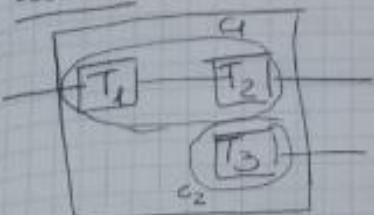
Esiste uno standard, che permette di distinguere le funzioni di interfaccia di due blocchi. Supponiamo di avere un centralino a circuito, che tramite collegamento invia la mia voce. Il media gateway, trasformerà la voce a circuito in voce a pacchetto.



Sip parla con media gateway tramite H248. All'interno del media gateway ho due parti: una a circuito e una a ip. Il modello basato sul concetto di terminazione. Il modello non è hardware.



ESSEMPIO



Supponiamo chiamata in arrivo su T3 destinata a T1, che è già in comunicazione con T2. (Contesto C1)

HGW → MGW contiene un evento NOTIFY (event, T3) in arrivo su T3, quindi

→ MediaGatewayController
esegue il suo behav per due a T1 decide un
CALL IN ATTESA, quindi invia:
Notify (T1)

→ ora T1 manda un INFO avendo il MediaGateway in lista
il MediaGateway controller con una
Notify (e, T1)

→ ora il MediaGatewayController modifica il MediaGateway
modificando il contesto di T4 ~~con~~ da C1 a C2
Hence (T1, C2)

→ Punto 3: stanno di parlare, ancora
MediaGateway dice al controller che la conn. è chiusa
Notify (event, T3)

→ E qui il HEC avendo una MAPPA delle GATE IN SOBREO,
EFFECTUA lo switch dalla terminazione T1 al contesto
C1, si procede
Hence (T1, C1)

Contatto DAI UNO PLAN → ~~sezione~~ sezione definisce direzione uscita (esterno)
" " " centro.

Teléfono (Protocolo interfazante)

Pc / SIP Phone



Pc sono SIP phone
TUTTE VITE

Ora che 1. Dalla rete
Dopo ogni punto
copia un BIDI!

Ora che 2. USO VITE

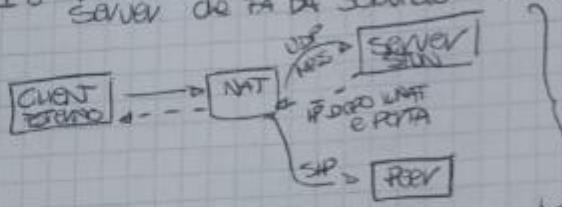
Per il TAK invece ho dei TAKUAL ADAPTER, sono un po' FANCIUO \rightarrow DOPPIO
e converto è scattate, così se una rete è scattata, costa.

Accordatela è rendere un PBX IP e una scheda analogica x fare traduzione
inadattabile

Net TRaversal (caso specifico VoIP)

- È UNA FACCIENDA Peer TO Peer e chi ha messo il NAT e la parte VoIP possono essere fatte da persone differenti. Inoltre, non è detto che interagisca per il suo apparato voce nello stesso momento.

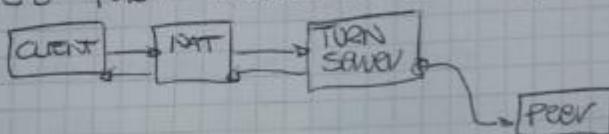
Soluzione 1: io faccio di client di un servizio che sta dentro il NAT e poi un server che fa da servizio STUN (Session Traversal Utility for NAT)



Soluzione semplice che non serve più funzionare
X se suppone che la traslazione IN-NAT e OUT-NAT ha assegnato lo stesso IP esterno.

E' RFC - 5389

Soluzione 2: TURN TRaversal using relay NAT



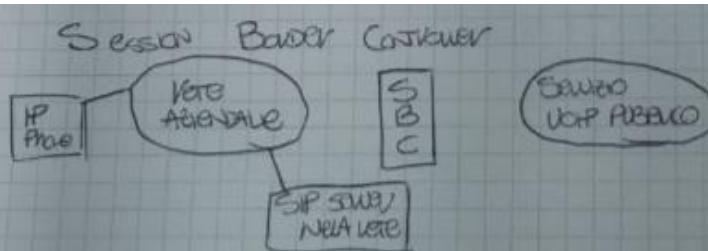
IL modo x fare il refresh sfrutta x esempio
il fatto che alcune operazioni hanno un timer

RFC - 5560

Soluzione che funziona molto spesso

L'unica cosa che bisogna considerare è che il NAT ha un tetto di associazioni che può scadere se non transita nulla per un certo periodo.

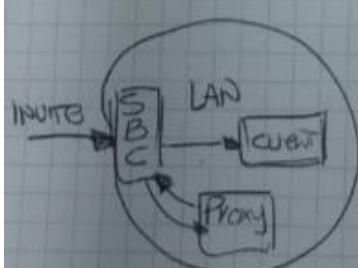
Soluzione 3: Net TRaversal



è comunque necessaria
in questo di mantenere le sessioni,
può più fare una soluzione

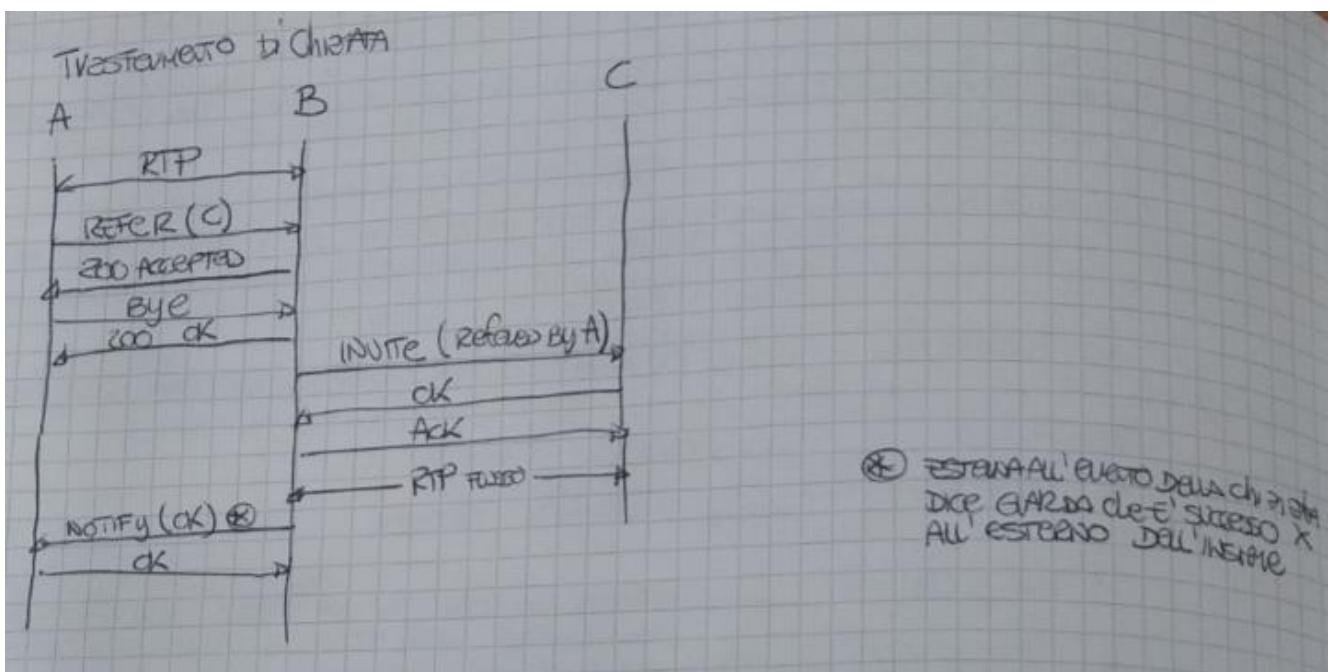
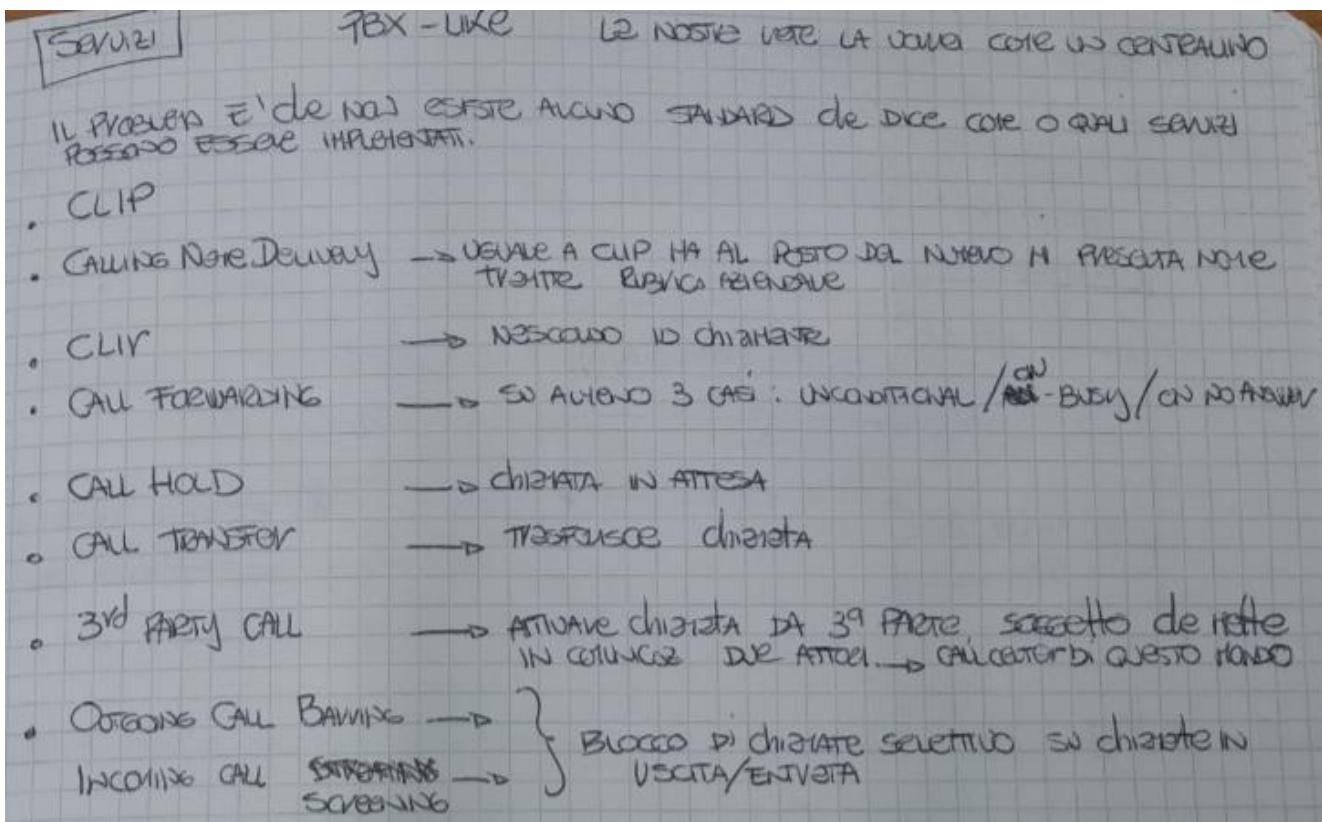
- ① risolvere il problema di NAT
(passa tutto attraverso di lui)

comunque sono usato l'esterno
che fa da NAT
ma anche da Firewall, accounting
e contratti sicure.

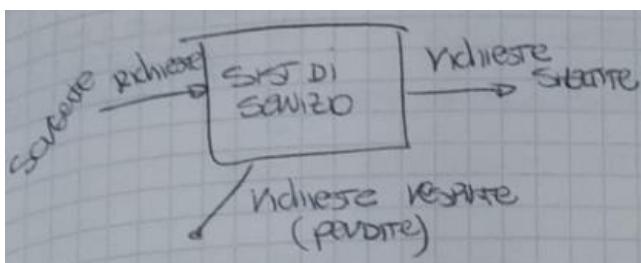


In più può fare il Topology hiding
che verso l'esterno nasconde
la rete interna

Potrebbe una sequenza fissa di messaggi più facile capire la struttura
della rete, in maniera diretta (attacco informatico) e indiretta
x capire l'organizzazione (spionaggio)



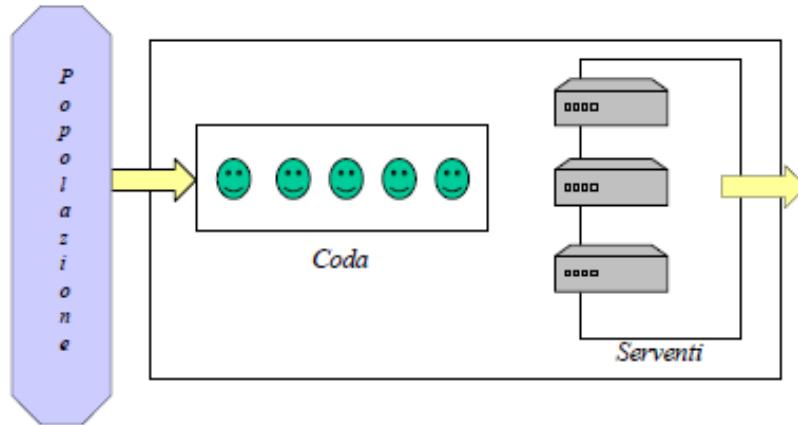
11.0 SISTEMA DI SERVIZIO



Il sistema di servizio modella qualsiasi cosa che si può intendere come una sorgente di richieste che smaltisce dopo averle masticate per un certo tempo. Alcune richieste possono essere respinte quando non ha risorse per gestirle. Il fenomeno di "non smaltimento" si chiama "perdita".

Da un punto di vista fisico, un sistema di servizio è composto da:

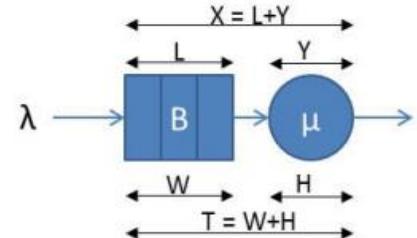
- insieme (non vuoto) di serventi, che indicheremo con **N**. In generale, vi possono essere uno o più serventi e nel caso di più serventi è necessario distinguere se lavorano “in parallelo” o “in serie”.
- insieme (non vuoto) di aree di attesa (chiamate anche buffer) che indicheremo con **B** che accolgono i clienti in attesa di essere serviti.



Il processo base che avviene in un sistema a coda è il seguente: le sorgenti che richiedono un servizio entrano nel sistema e raggiungono la *coda*. Ad un certo momento, una sorgente viene selezionata dalla coda secondo la *disciplina della coda* (*FIFO*, *LIFO*...). Il servizio richiesto è effettuato da un servente e successivamente a ciò, la sorgente lascia il sistema.

Il tempo richiesto per un servizio è $T = H + W$ dove:

- **W** è il tempo di attesa in coda
- **H** è il tempo di attesa in servizio



Notazione di Kendall

È stata definita una notazione per indicare sinteticamente le caratteristiche principali di un sistema di servizio (o a coda); la notazione, chiamata notazione di Kendall, consiste in sigle separate dal simbolo /, del tipo **A/B/s/c/p/Z**, dove:

- **A** rappresenta lo schema di arrivo, ovvero la distribuzione di probabilità degli intertempi di arrivo;
- **B** rappresenta lo schema di servizio, ovvero la distribuzione di probabilità dei tempi di servizio;
- **s** rappresenta il numero di serventi;
- **c** rappresenta la capacità del sistema (dimensione del buffer);
- **p** rappresenta la dimensione della popolazione;
- **Z** rappresenta la disciplina della coda.

Le ultime tre componenti possono non essere specificate, assumendo, i seguenti valori di default: in mancanza della componente **c** si assume che la capacità del sistema sia infinita; se non è specificata la componente **p** si assume che le sorgenti siano infinite; se non è presente la componente **Z** si assume che la disciplina della coda sia FIFO.

Le componenti **s**, **c** e **p** sono numeri interi non negativi. Per quanto riguarda le distribuzioni di probabilità dello schema di arrivo e di servizio, quelle che vengono più frequentemente assunte sono la distribuzione *esponenziale*, la distribuzione *costante* (degenere) o tempi deterministici, la distribuzione *di Erlang* di ordine *k*.

Queste vengono indicate in termini delle componenti **A** e **B**, nel seguente modo:

- **M** indica la distribuzione *esponenziale*;
- **D** indica la distribuzione *costante* (degenere) o tempi deterministici;

- E_k indica la distribuzione di Erlang di ordine k ;

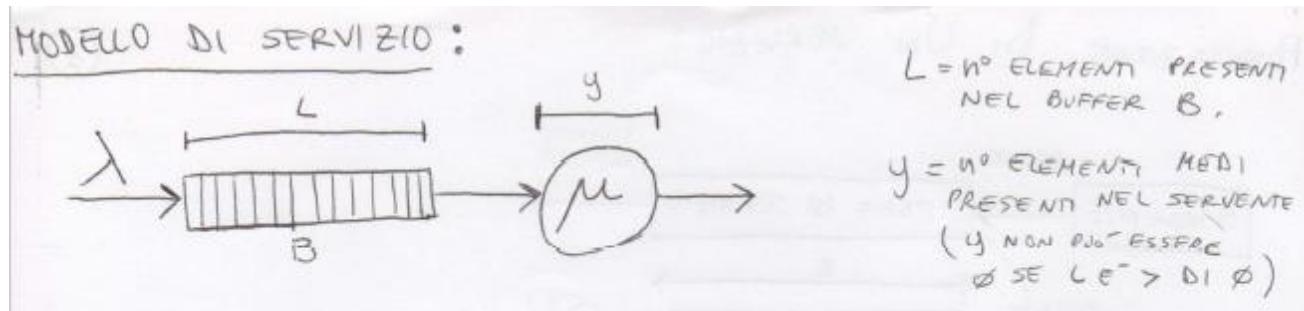
Molto frequente è l'uso di notazioni del tipo M/M/1 (ovvero con solamente tre sigle) che, come abbiamo già detto, corrisponde ad avere la capacità del sistema infinita, le sorgenti infinite e la disciplina della coda basata sul criterio FIFO (ovvero corrisponderebbe a scrivere M/M/1/1/FIFO); tale modello M/M/1 assume che sia gli intertempi di arrivo (tempi di attesa), sia i tempi di servizio hanno distribuzione esponenziale e che è presente un solo servente. Tale modello M/M/1 assume che sia gli intertempi di arrivo, sia i tempi di servizio hanno distribuzione esponenziale e che è presente un solo servente. La notazione M/G/1 indica, ad esempio, un modello con intertempi di arrivo distribuiti esponenzialmente e non pone nessuna specificazione sulla distribuzione dei tempi di servizio.

DEFINIZIONI

Introdurremo ora alcune definizioni e notazioni standard che vengono di solito adottate nell'analisi delle prestazioni di un sistema a coda e che utilizzeremo nel seguito.

- λ richieste di servizio secondo.
- μ richieste smaltite al secondo.
- ρ fattore di utilizzazione dei serventi $\rho = \frac{\lambda}{N \cdot \mu}$

MISURE DI PRESTAZIONE



$\lambda = \text{FREQUENZA DI ARRIVO} \quad (\text{RICHIESTE DI SERVIZIO AL SECONDO})$

$\mu = \text{RICHIESTE SMAILTITE AL SECONDO}$

TEMPO DI ATTRaversamento = $W + H = T$

$H = \frac{1}{\mu} \quad \text{TEMPO DI SERVIZIO}$

FORMULA DI LITTLE :

$$\bar{X} = \lambda \cdot \bar{T}$$

n° MEDIO DI ELEMENTI DEL SISTEMA = TASSO DI ARRIVO • TEMPO MEDIO DI ATTESA

$$\bar{Y} = \lambda \cdot \bar{H} \quad \text{UTILIZZAZIONE}$$

Nell'analisi di un sistema di servizio vengono prese in considerazione alcune grandezze fondamentali come misure di prestazione.

Nella maggior parte dei casi di interesse si è interessati a valutare queste grandezze assumendo che il sistema abbia raggiunto una situazione di regime e ciò avviene quando il sistema è stato in funzione per un tempo sufficientemente grande.

Infatti, quando un sistema ha iniziato da poco ad essere operativo, lo stato del sistema sarà fortemente influenzato dallo stato iniziale e dal tempo che è trascorso dall'attivazione. In questo caso il sistema è detto in **condizioni transitorie**. Tuttavia, in molti casi, trascorso un tempo sufficientemente grande, il sistema diviene indipendente dallo stato iniziale e si dice che il sistema ha raggiunto condizioni stazionarie o equilibrio (steady-state).

Si osservi subito che questo non può accadere se risulta $\rho \geq 1$ nel qual caso lo stato del sistema cresce indefinitamente nel tempo. Per un sistema in condizioni stazionarie la distribuzione di probabilità dello stato del sistema rimane la stessa nel tempo. La teoria delle code analizza principalmente sistemi in condizioni di stazionarietà.

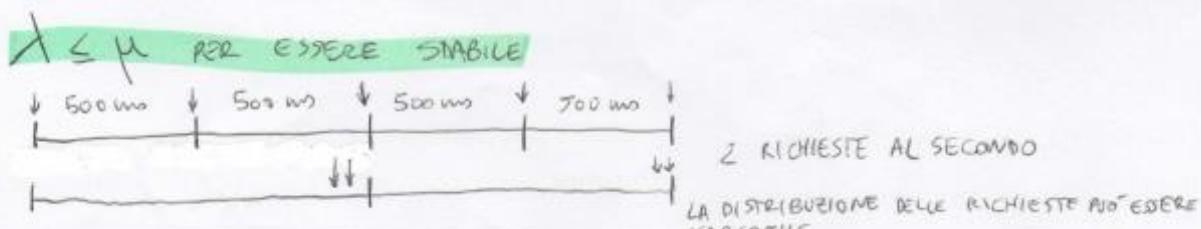
IN ASSENZA DI PERDITA:

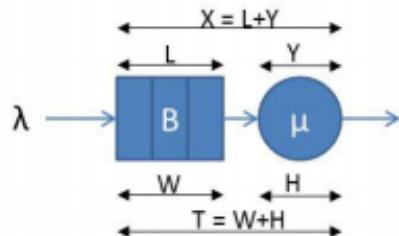
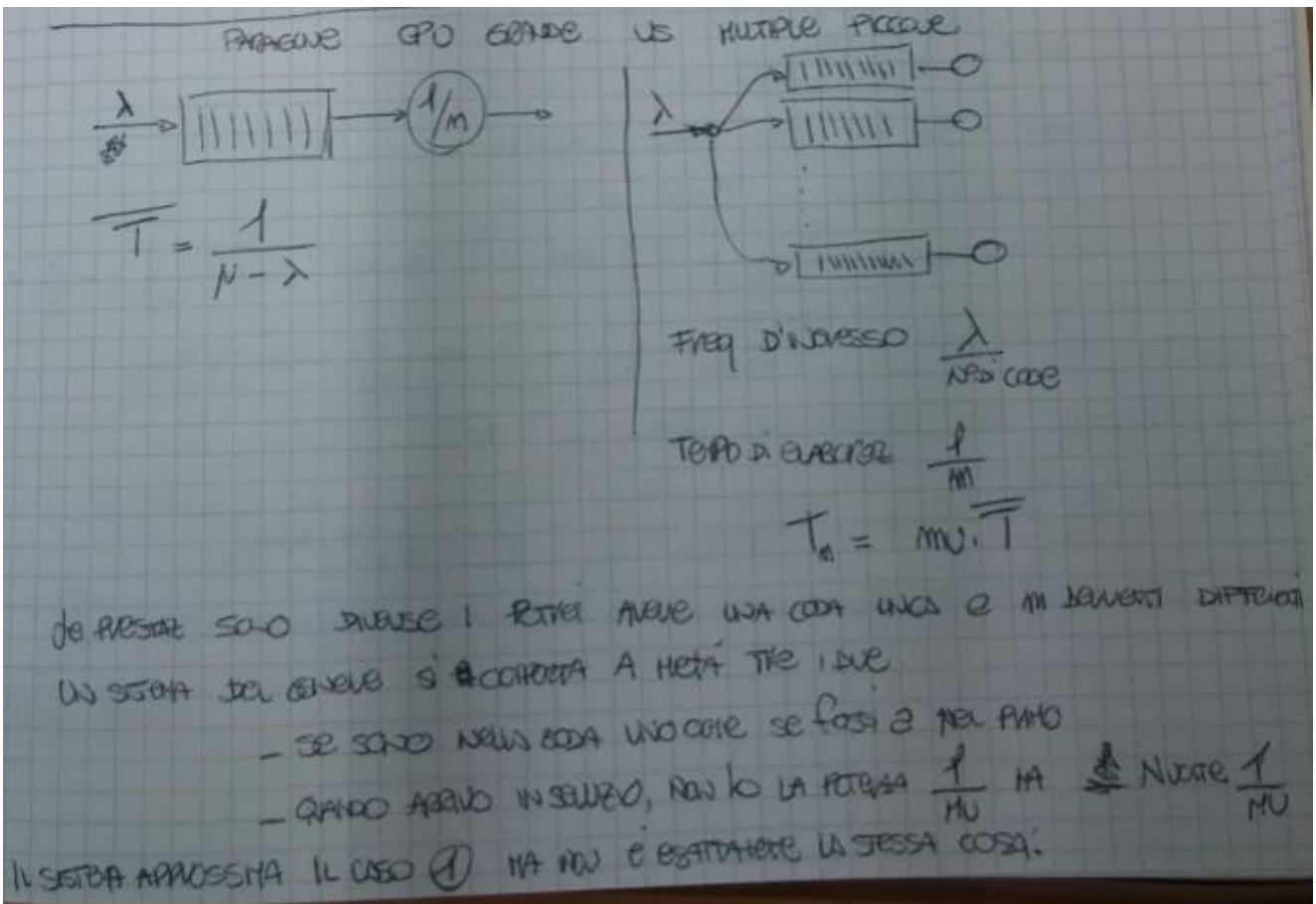
$$\overline{H} = \frac{1}{\mu} \quad \overline{Y} = \frac{\lambda}{\mu} = P_{RHO} = \text{ATTUAZIONE}, \text{ OVVERO TEMPO CHE UN SISTEMA DI SERVIZIO PASSA A GESTIRE RISORSE LAVORANDO.}$$

SE $P > 100\%$, LA CODA CRESCE ALL'INFINITO. (IL SISTEMA NON È STABILE)

STABILE = NON È INTRANSITORIO (HA MEDIANTEMENTE LO STESSO COMPORTAMENTO).

IL SISTEMA DI SERVIZIO DETERMINISTICO È NELLA MEDIA PIÙ AFFIDABILE.





M/M/1 (tempi di interarrivo e di servizio distribuiti esponenzialmente, $\rho = \frac{\lambda}{\mu}$)

$\bar{X} = \frac{\rho}{1 - \rho}$	$\bar{T} = \frac{1}{\mu - \lambda}$		
$\bar{L} = \frac{\rho^2}{1 - \rho}$	$\bar{Y} = \rho$	$\bar{W} = \frac{1}{\mu} \frac{\rho}{1 - \rho}$	$\bar{H} = \frac{1}{\mu}$

M/D/1 (tempi di interarrivo esponenziali, servizio deterministico, $\rho = \frac{\lambda}{\mu}$)

$\bar{X} = (1 - \frac{\rho}{2}) \frac{\rho}{1 - \rho}$	$\bar{T} = (1 - \frac{\rho}{2}) \frac{1}{\mu - \lambda}$		
$\bar{L} = \frac{\rho^2}{2(1 - \rho)}$	$\bar{Y} = \rho$	$\bar{W} = \frac{1}{\mu} \frac{\rho}{2(1 - \rho)}$	$\bar{H} = \frac{1}{\mu}$

M/M/N/0 (sistema con N serventi a pura perdita, B = probabilità di perdita con A erlang di traffico)

$$B(N; A) = \frac{A^N}{N!} \sum_{i=0}^N \frac{A^i}{i!}$$

AFFIDABILITÀ E DISPONIBILITÀ DI SISTEMA

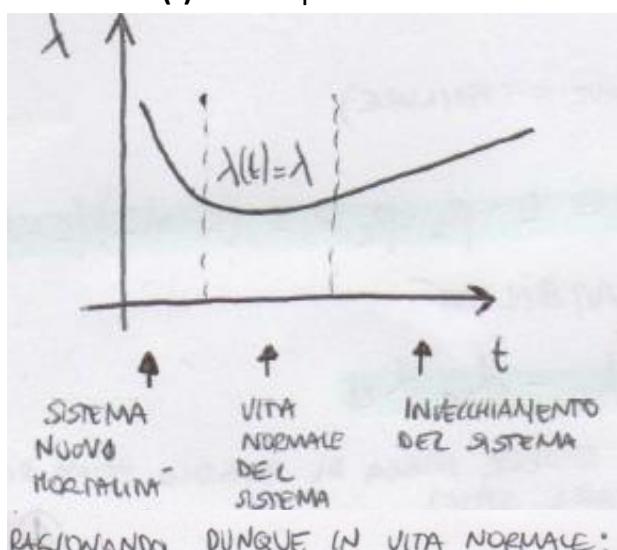
- **Affidabilità di sistema:** È la misura della probabilità che il sistema non si guasti in un determinato lasso di tempo. È una probabilità che dipende dal tempo ed è quella che funziona in un certo istante. Con guasto (fault) si intende un evento per cui un sistema viola le specifiche di funzionamento, interrompendo la disponibilità dei servizi che fornisce.

RDT -> probabilità che il sistema funzioni fino a t. Viene indicato con $R(t)$.

La **guastabilità** è complementare: **Guastabilità=1-R(t)**; probabilità dell'evento complementare, ovvero che il sistema si guasti prima del tempo t. La guastabilità fa parte di una normale vita di un sistema.

- **Disponibilità di sistema:** misura l'attitudine di un sistema di essere in grado di svolgere una funzione richiesta in determinate condizioni ad un dato istante o durante un dato intervallo di tempo. Può essere definita come il rapporto tra il tempo effettivo di funzionamento e il tempo totale (dunque è minore o uguale a 1). La disponibilità non dipende dal tempo t; è importante sia il tempo di funzionamento prima del guasto che il tempo di riparazione che ci vuole.

$\lambda = \lambda(t)$ è la frequenza con cui il sistema esce dallo stato funzionante. $R(t)$ è la probabilità che il sistema funzionava fino al tempo t.



$$R(t) = e^{-\lambda t}$$

$$F(t) = 1 - e^{-\lambda t}$$



$F(t)=$ probabilità che il sistema si guasti prima del tempo t (guastabilità=F(t)=1-R(t)).

L'immagine affianco rappresenta la cosiddetta "curva a vasca da bagno":

- 1° parte: mortalità precoce\infantile. Esiste, ma dura pochissimo e viene rilevata durante la fase di testing iniziale.
- 2° parte: frequenza di guasto quasi costante.
- 3° parte: deterioramento, invecchiamento del sistema.

MTTR, MTBF

Il **tempo medio fra i guasti** (in inglese *mean time between failures*, spesso abbreviato in **MTBF**), è un parametro di affidabilità applicabile a dispositivi meccanici, elettrici ed elettronici e ad applicazioni software; sarebbe il periodo in cui il sistema è disponibile.

Il significato dell'acronimo **MTTR** è **Mean Time To Repair**, traducibile in italiano come **Tempo medio di riparazione**.

L'MTTR comprende il tempo per la diagnosi, quello per l'arrivo del tecnico di manutenzione, l'arrivo del componente da sostituire e la riparazione vera e propria, incluso un piccolo collaudo: è il tempo medio per riparare il sistema.

$$\text{Disponibilità } d = \frac{\text{MTBF}}{\text{MTTR} + \text{MTBF}} = 1 - p \text{ dove } p \text{ è l'indisponibilità}$$

Per avere più disponibilità, o aumento il MTBF o diminuisco il MTTR. Il MTBF lo fornisce il costruttore mentre il MTTR devo saperlo io dato che è il tempo di riparazione.

COMBINAZIONI:

SERIE:

CONDIZIONI: FUNZIONA SOLO SE ENTRAMBI (FRONT-END & BACKEND) FUNZIONANO CONTEMPORANEAMENTE.



$$d = P(S_1) \cdot P(S_2)$$

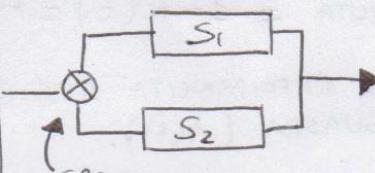
ONVERO

$$d = d_1 \cdot d_2$$

ONVERO E' IL PRODOTTO DELLA PROBABILITA' DI FUNZIONAMENTO DI S_1 CON LA PROBABILITA' DI FUNZIONAMENTO DI S_2 .

PARALLELO:

CONDIZIONI: FUNZIONA SE ALMENO UNO DEI DUE FUNZIONA.



SPoF
(SINGLE POINT OF FAILURE)

$$d = 1 - p = 1 - p_1 \cdot p_2 = 1 - (1 - d_1)(1 - d_2)$$

p = INDISPONIBILITÀ

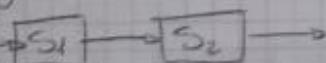
$$d = d_1 + d_2 - d_1 d_2$$

NON CI DEVE ESSERE NULLA DI SINGOLO PRIMA DEL PARALLELO (EVITARE SPoF).

$$d = d_x \cdot (d_1 + d_2 - d_1 d_2)$$

PRIMO TIPO DI COMBINAZIONE

• IN SERIE

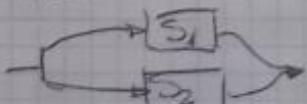


$$\text{disponibilità complessa} = d_1 \cdot d_2$$

• E' il prodotto di cui sopra. E disponibile se S_1 e' disponibile AND S_2 è disponibile

• IN PARALLELO

OR



$$\text{disponibilità complessa} = \frac{1}{d_1 + d_2 - d_1 d_2}$$

$$= 1 - \text{INDISPONIBILITÀ}$$

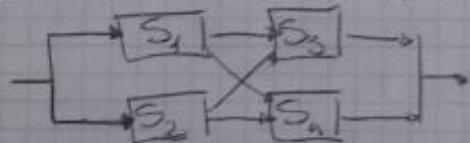
e l'indisponibilità è data dalla rotura di entrambi

$$L_d = p_1 p_2 = (1 - d_1)(1 - d_2)$$

$$d = d_1 + d_2 - d_1 d_2$$

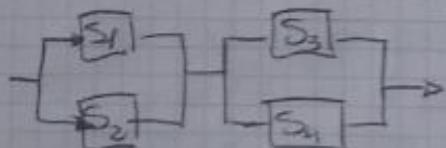
SIA LA SEQUELLE CHE IL PARALLELO LI POSSO TRAVERSI

IN PARALELO INCROCIO (BUTTERFLY)



S_3 e S_4 sono IN PARALELO ESTINTAMENTE come S_1 e S_2

IL DEGENDO PUÒ DIVIDERSI



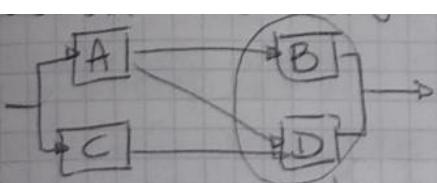
disptotale = $\frac{\text{disp primo blocco}}{\text{IN SEQUELLE}} - \frac{\text{disp secondo blocco}}{\text{IN SEQUELLE}}$

$$\text{essendo IN PARALELO SARÀ} \Rightarrow [d_1 + d_2 - d_1 d_2] \cdot [d_3 + d_4 - d_3 d_4]$$

Faccendone un esempio: LA DISPONIBILITÀ ha il DIRITTO DI PARTIRE REPENTIMENTE AD ESSERE
ATTIVATA MA NON PUÒ DIVIDERSI

FAULT TREE ANALYSIS

La FTA è una tecnica che correla, usando porte logiche, gli eventi che provocano un determinato malfunzionamento. Nella FTA si procede in maniera top-down prendendo in considerazione tutti i guasti verificabili in un impianto/sistema cercando di verificare le possibili cause nei componenti di gerarchia via via inferiore. Si inizia con la definizione dell'EVENTO TOP O INDESIDERATO che di solito è combinazione di varie cause.



SISTEMA HA 3 INPUT, DUE BLOCCI SEP, HA MA NON SI POSSOC

AUORA DEVO CONSTRUIRE RIGUARDANDO TEOREMA:

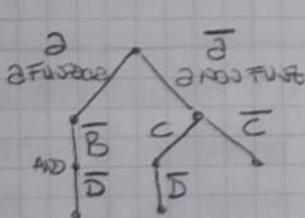
$$P_A = P_A | b + P_A | \bar{b}$$

b = BLOCCATO

costruire un

Posso avere Fault Tree: LA VEDICE È L'EVENTO: IL SISTEMA NON FUNZIONA

MI DA MOGLI DI CALCOLARE L'INDISPONIBILITÀ



NE HOGESTO IN CI HO DIVISO, HO DUE INSISTEMI DI EVENTI CHE SONO INDIPENDENTI.

LE FOGLIE SONO IL SISTEMA NON FUNZIONANTE E IL FAULT TREE COMPLETO DI QUESTO SISTEMA

La radice dell'albero è "il sistema non funziona". Si devono sviluppare tutte le casistiche tali per cui il sistema non funziona. L' **OR** è rappresentato con la biforcazione, mentre l'**AND** è il proseguimento del ramo precedente.

QUA' E' LA DISPONIBILITA DI TUTTA SUA ROBA?

$$\begin{aligned}
 d &= 1 - \left\{ [d_A (1-B)(1-D)] + [(1-A)[(1-C) + C(1-D)]] \right\} \\
 &= 1 - (A - AB)(1-D) + (1-A)[(1-C) + C - CD] \\
 &= 1 - [A - AD - AB + ABD + (1-A)[1 - C + C - CD]] \\
 &= 1 - [A - AD - AB + ABD + 1 - CD] \\
 &= 1 - [ABD + ACD - AD - AB - CD + 1] \\
 &= -ABD + ACD + AD + AB + CD
 \end{aligned}$$

RISOLVO COSÌ A CALCOLARE LA DEP DI QUAISIASI PROBLEMA COMPUTATO QUANTO VOGLIO.

ESERCIZIO

→ CALCOLI SISTEMI SEUE PARAVERO

→ CREATIV FAULT-TREE

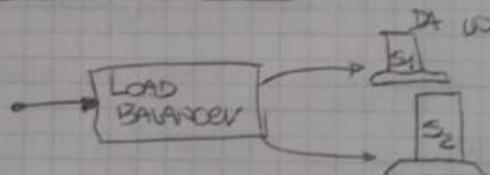
→ DATO FAULT TREE → ESTRAE FORMA come quella sopra

NON PRESSIONATO come se la FAULT UNIT = REPAIR UNIT.

(non è sempre così)

ESERCIZIO ESERCIZIO

SUPP DI AVERE UN SERVIZIO WEB DEI 24 IN FRATTO DATO



Supponendo che il LB abbia HTBF = 5 ANNI e che il web server abbia HTBF = 3 MESI e che il HTTR = 2 GIORNI

Qua' e' la disponibilità di tutto?

PRIHA CALCOLATO DI OGNI SINGOLO WEB SERVER

$$d_{ws} = \frac{90}{92} = 97,8\%$$

$$d_{tot} = d_{LB} (2d_{ws} - d_{ws}^2)$$

$$\frac{\text{HTBF}}{\text{HTBF} + \text{HTTR}}$$

$$d_{LB} = \frac{360}{360+2} = \frac{1800}{1802} = 99\%$$

$$= 99\% (2 \cdot 97,8 - (97,8)^2) = 0,998 \rightarrow 99,8\%$$

Se volessi aumentare d_{tot} bisogna mettere d_{ws} a 3?

No! XK vedo ad aumentare il secondo de' e' più alto del d_{LB} .

Quindi aggiungendo un WS non ottengo un grande risultato.

Mentre può essere conveniente ridurre il HTTR a un solo

FINE

SERVIZI

GESTIONE DELLA RETE

Un modo di vedere le cose è quello di suddividere la rete nelle seguenti categorie:

- **Configuration management**
- **Performance management**
- **Fault management (gestione dei guasti)**

Queste sono suddivisioni funzionali. Il livello a cui intervengo sono:

- Servizi (livello 1)
- Rete (livello 0)
- Business (livello 2)

	CONFIGURAZIONE	PERFORMANCE	FAULT
RETE (Livello 0)	Immaginiamo che la rete sia già costruita, già collegata, tutti i nodi sono collegati. La configurazione è più complicata di quella che sembra.*	Nella rete, per quanto riguarda le prestazioni, ho il ritardo o il jitter del ritardo (variazione). Se faccio web browsing e ho 50 ms di jitter di ritardo, non me ne frega nulla. Se sulla stessa rete ho 50 ms di ritardo e la mia comunicazione è voce, l'impatto è negativo e devo intervenire. Non tutte le applicazioni hanno la stessa tollerazione di jitter del ritardo.	Quando ho un guasto sulla rete, vuol dire che avrò un nodo che non mi funziona più bene. Ragiono a livello di rete. Identifico il nodo che non funziona, capire come sostituirlo, attivare dei meccanismi per far continuare ad andare la rete, come ad esempio creare percorsi alternativi.
SERVIZI (Livello 1)			Quando un nodo non funziona, lui sta fornendo una serie di servizi. Io devo intervenire, cercare di capire i servizi che non vengono più forniti. Devo individuare delle strategie per fornire i servizi prioritari. Ex: faccio passare del traffico prioritario per primo. Il modo di ragionare in termini di servizi, è diverso dai modi di ragionare in termini di rete.
BUSINESS (Livello 2)			

* il 40% dell'effort (sforzo) sta nella direzione, configurazione, e di questo 40%, buona parte sta nella configurazione di apparati. Perché questo?

Immaginiamo di avere una scatola che è un router, di averlo collegato, di accenderlo. Cosa devo fare ora? Ecco i passi:

1. Devo partire da un punto di accesso sicuro al router (console) oppure precaricare codice che mi consenta di avere una sessione sicura; devo poi definire utenti, password, la tipologia di utenti, a seconda di quello che possono fare sul router; abbiamo livelli di utenti, come gli admin e non admin.
2. Dare un nome alle interfacce fisiche o logiche.
3. Devo definire per ogni interfaccia, la sub network e indirizzo ip.
4. Funzioni del nat. Non mappo uno a uno gli indirizzi. Dico quali sono gli insiemi di indirizzi di tipo privato e quelli di tipo pubblico.
5. Inizializzare DHCP server
6. Mi serve fare il ruting. La tabella di routing è vuota e non passa nulla. Inizializzo le tabelle di routing con i protocolli di routing. Posso avere tanti protocolli di routing a seconda delle interfacce.
7. Devo salvare la configurazione! save running cnf.

Ora posso attivare i protocolli di funzione, il più utilizzato è il **SNMP**. Questo protocollo ha i suoi utenti e permessi di accesso.

Esistono due tipologie di apparati:

- **Plug and Play** (richiedono poca configurazione)
 - Host
 - Switch
- **Non Plug and Play** (richiedono configurazioni abbastanza complicate):
 - Router
 - Dns server
 - Intrusion detection system- Intrusion prevention system e tutti gli apparati di sicurezza
 - Firewall

Serve qualcosa che aiuti la configurazione automatica dei sistemi. Il modello standard per la configurazione di apparati standard complessi si basava sul fatto che io utilizzavo protocolli **FTP**, **SFTP**, **NETCONF**, **PRE_CARICATA**.

FAULT MANAGEMENT

Il **fault management** è un processo che ha al suo interno varie componenti che hanno come obiettivo finale quello di abbassare il **MTTR**. Ricordiamo che la disponibilità è:

$$\text{Disponibilità } d = \frac{MTBF}{MTTR + MTBF} = 1 - p \text{ dove } p \text{ è l'indisponibilità}$$

Cose da fare:

1. Prima cosa da fare è identificare il fault, che può essere estremamente complicato se la rete è sufficientemente grande. Dobbiamo distinguere l'identificazione del fault in due parti:
 - a. Prima parte: identificazione della componente non funzionante. C'è un blocco che non funziona e io sono in grado di riconfigurare la rete, che nonostante il blocco non funzioni, tutta la rete funziona.
 - b. Seconda parte: Identificazione della componente riparabile o sostituibile. Può esserci un guasto hardware

2. Seconda cosa da fare: riconfigurare la rete. Se la rete era duplicata non c'è bisogno di far nulla, altrimenti devo provvedere.
3. Terza cosa da fare: effettuare riparazione.
4. Quarta cosa da fare: ripristino dello stato prima del guasto
5. Quinta cosa da fare: verifico che sia effettivamente up to date

Al fine di calcolare quale sia il tempo di ripristino devo verificare il tempo impiegato tra guasto e risoluzione; il tempo si misura dall'apertura del **trouble ticket** fino a quando è risolto. Quando c'è un cliente devo essere preciso nel definire quando inizia un guasto e quando termina. Il guasto c'è quando viene assegnato un numero di trouble ticket (il famoso ticket remedy ibm). Le attività che venivano svolte in Banca Intesa nel servizio AM quando cadevano i servizi e si aprivano i ticket per l'attività (si potrebbe raccontare la propria esperienza del lavoro in Intesa). L'identificazione dei guasti è interessante. È stata una delle prime applicazioni di intelligenza artificiale nel mondo delle telecomunicazioni. Quello che abbiamo sull'identificazione di guasti è la creazione locale di un allarme: ci sono alcune condizioni verificate in un sistema che mi dicono non funziona. Quando creo questo allarme localmente, sono in grado di inviare l'allarme a un sistema di correlazione dei guasti. Io non devo inviare allarmi continui se il guasto continua a esserci; ne basta uno. Devo trovare la **root cause analysis** perché una rottura può incidere su più nodi e generare molteplici messaggi di errore. Solo allora posso definire l'unità riparabile e definire l'intervento di manutenzione. La definizione di queste azioni è parte critica perché potrei peggiorare la situazione con l'intervento che vado ad eseguire.

PERFORMANCE MANAGEMENT

Da capire subito qual è la configurazione di riferimento (il limite). Esempio: stiamo parlando di banda. La banda disponibile è qualcosa di molto concreto, quanti Mbps passano ma è anche qualcosa di sfuggente. Devo capire da dove a dove misuro. Quindi:

- Va misurata end to end (VPN). Ho un ambiente chiaro e determinato. Qualsiasi end point per esempio è in grado di smaltire 100 Mbps
- Banda verso internet. Dire su internet "ho 100 Mbps", non vuol dire nulla perché sulla linea d'accesso posso anche arrivarci a quella velocità, mentre è dopo che posso avere traffico. Allora devo selezionare un'uscita (Internet exchange points), quella che più mi conviene e misurare tra me e quell'uscita quale conviene. Devo dire qual è la banda misurata dopo che ho fatto il ping. Preso il più breve degli IExchange, e mi misura la banda che ho in questo momento.

Come misuro le perdite?

- TCP: è molto più tollerante alle perdite
- UDP: non è tollerante alle perdite perché non recupera

Nella compressione, la perdita è meno visibile perché butto già via. Dipende quanto comprimo. Se ho poca compressione, magari la sento; se la compressione è tanta, è probabile che non me ne accorga.

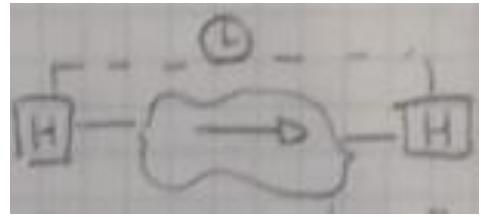
PARAMETRI PERFORMANCE MANAGEMENT

Vediamo gli indicatori che ci permettono di capire le performance:

- **Delay (ritardo):**

- **One way delay:** ho un host collegato alla rete. E dall'altra ho un altro host collegato che riceve la roba che il primo invia. Il delay è il tempo che intercorre tra il primo bit che entra nella rete e la ricezione dell'ultimo bit del messaggio. Porto dentro anche il ritardo di trasmissione. Il ritardo di una rete è costituito da varie componenti: ritardo di propagazione (tempo necessario al segnale fisico per propagarsi lungo la linea di trasmissione fino al nodo successivo e da qui alla destinazione finale), elaborazione e accodamento, e trasmissione che dipende dalla velocità della linea e dalla lunghezza del pacchetto. Il sistema di misurazione è basato sul SW del ricevente (economico). In questo schema manca un orologio che sincronizzi con grande precisione i due host, perché se non sono sicuro che il tempo visto da una parte è uguale dall'altra parte, non posso fare misurazioni precise. Per la sincronizzazione posso usare:

- **NTP (Network Time Protocol):** precisione che non è mai migliore dei millisecondi, quindi ho questo delta di errore.
- **GPS:** migliora la precisione, che è quattro volte superiore; sta sotto al microsecondo



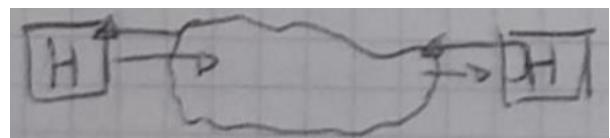
Determinato lo schema di misurazione, devo decidere alcuni dettagli:

- Dimensione pacchetto. È un fattore molto importante.
- Pacchetto frammentato oppure non frammentato
- Bit random nel contenuto. Bisogna mettere questi bit, perché in alcune tratte particolari, alcuni operatori, in specifiche situazioni effettuano compressioni sui pacchetti.
- Priorità standard (voglio misurare il ritardo di un pacchetto qualsiasi generico).
- Non considero una misura valida se i pacchetti sono persi o con errori **non correggibili**

Il protocollo utilizzato è il OWAMP per misurare il ritardo (One-Way Active Measurement Protocol)

- **Round Trip:** è più facile da misurare.

Il Round Trip Time o Round Trip Delay (acronimo RTT) è una misura del tempo impiegato da un pacchetto di dimensione trascurabile per viaggiare da un computer della rete ad un altro e tornare indietro (tipicamente, un'andata client-server ed il ritorno server-client) Il Round Trip Time o Round Trip Delay (acronimo RTT) è una misura del tempo impiegato da un pacchetto di dimensione trascurabile per viaggiare da un computer della rete ad un altro e tornare indietro (tipicamente, un'andata client-server ed il ritorno server-client)



ritorno server-client). Con il Round Trip non ho bisogno di una sincronizzazione. Il protocollo utilizzato è il TWAMP per misurare il ritardo (Two-Way Active Measurement Protocol)

- **Packet Delay Variation (Jitter):** misura derivata da una sequenza di misure di one way delay. Devono essere pacchetti di una stessa dimensione. Ho diverse definizioni:
 - Differenza tra due misurazioni: $OWD_{i+1} - OWD_i$ dove OWD sta per OneWayDelay
 - $|OWD_{i+1} - OWD_i|$
 - $|OWD_{i+1} - OWD_1|$
 - $|OWD_{i+1} - \overline{OWD}|$

Packet Loss

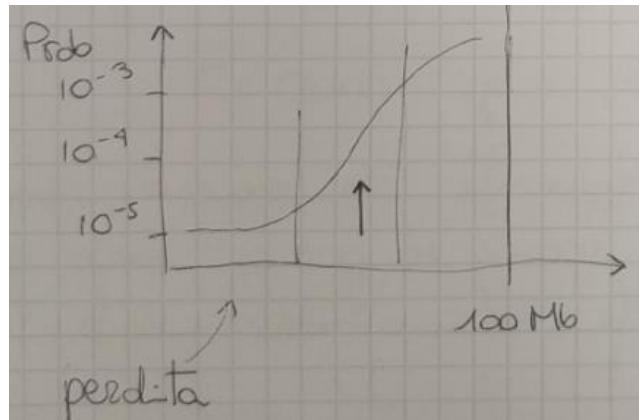
La perdita! La storia è + complicata...

Idea: li conto (magari hanno pure # di sequenza) e vedo quanti arrivano effettivamente (logica one-way)
Devo mettere un limite, e.g. $axD > T$
Ma devo stimare tipicamente un numero molto piccolo: 1 evento ogni 1000/10.000... deve generare tutti quegli eventi?! No, spazialmente...
Quanti sono sufficienti?
Supponiamo: me ne servono 100K. Come li spacco tutti di fila? Ma influenza il traffico, sforsa la congestione (e allora grazie che ce perdita, l'ho generata io!)
Insomma: la perdita è molto DIFFICILE da misurare a differenza di rete come il ritardo... devo accettare fasti APPROXIMAZIONI per necessità.
C'è comunque un modo indiretto per misurare: una misurazione di tipo PASSIVO. Osservo cioè il comportamento di app. esistenti e vedo cosa posso dedurre. e.g. le app.

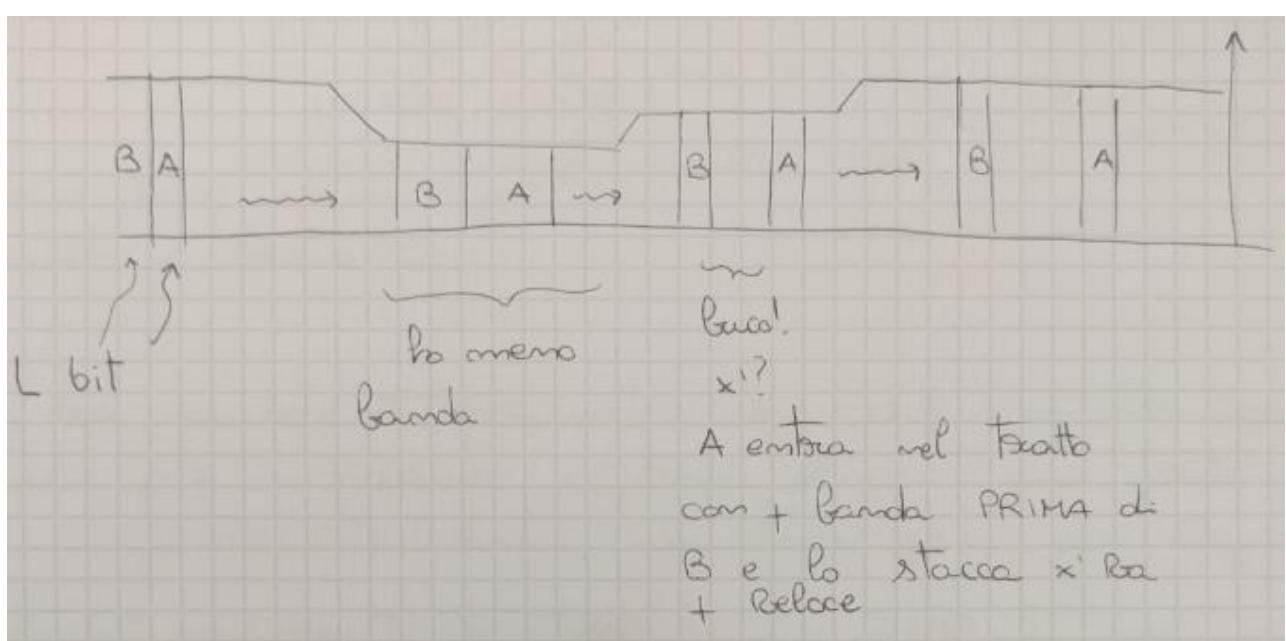
TCP misurano la perdita: posso sbatterlo. Risultato? No, devo avere app. TCP "vera", che sta operando proprio sul excesso che deve misurare! Non è mia detta.

- **Capacità disponibile:** ci sono due modalità per misurare la capacità:

- **Modalità 1:** è il massimo dell'intrusività. Ho un host. Voglio misurare la banda verso un altro host o Internet Exchange port. Fermo tutte le applicazioni. In assenza di altro traffico, sparo un treno di pacchetti in una direzione e nell'altra direzione. Cerco di misurare il massimo traffico che questo collegamento è in grado di sopportare. Questo massimo traffico non è facile da misurare. Cosa succede? Se nel collegamento sparo 4 pacchetti a 100 Mbps, quelli passano perché il router ha buffer sufficiente per accoglierli e non perdo niente; i pacchetti arrivano. Per poter fare la misurazione e raggiungere uno **stato stabile** devo sparare dati per almeno 10 secondi. Altra cosa: io vorrei misurare la capacità assoluta indipendentemente dal protocollo dal protocollo di trasporto. Per fare una cosa simile, se ho 100 Mbps di banda e ho la perdita, avrò una situazione in cui la perdita, nella situazione di congestione, avrà una crescita di perdita. devo fare tanti campionamenti e la cosa diventa alquanto intrusiva e lunga che mi massacra la rete. Utilizzo del protocollo http/TCP. Com'è vista la capacità dal TCP? Cresce, poi a un certo punto comincio a perdere e restringo la finestra. Se uso http, è in grado di aprire connessioni tcp temporanee e non avrò i picchi. Misuro in maniera più precisa.



- **Modalità 2:** la modalità 1 è banale. Vediamo la capacità in un'altra misura. Guardo la capacità sui vari livelli di rete. Mando due pacchetti uno attaccato all'altro:



pacchetto **a** e pacchetto **b** entrambe di lunghezza **I**. La ordinata è l'ampiezza di banda.

Quindi qst modo è:

- Non intuisco
- "economico": uso solo 2 pacchetti
- "mi". Non è tutto super vero e super bello

Un po' è intuisivo anche qst, e poi mi mi bastano 2 pacch. ma stream. Ma cmq qst metodo:

→ Packet Pair Text

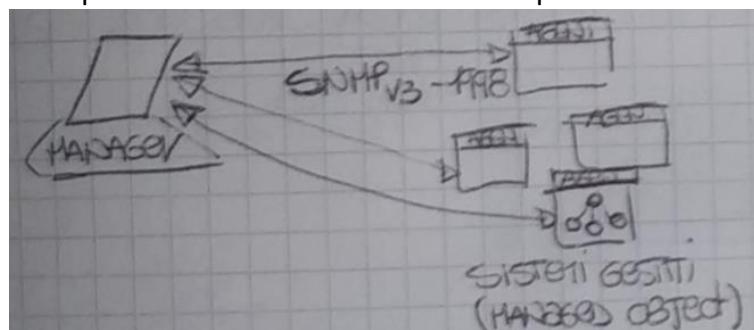
non è male ed è integrato in alcuni strumenti di misurazione. Ottimo su una VPN end-to-end.

SNMP

In informatica e telecomunicazioni **Simple Network Management Protocol (SNMP)** è un protocollo di rete. Esistono 3 versioni del protocollo: SNMPv1, SNMPv2 ed SNMPv3. Le versioni successive offrono più funzionalità, e la versione SNMPv3 offre anche ulteriori possibilità legate alla sicurezza. Esso consente la configurazione, la gestione e la supervisione (*monitoring*) di apparati collegati in una rete (siano essi nodi interni di commutazione come i dispositivi di rete e nodi terminali di utenza), riguardo a tutti quegli aspetti che richiedono azioni di tipo amministrativo (*management*). L'idea dell'SNMP è un'idea abbastanza particolare: come costruisco un'architettura di gestione della rete? I tre componenti logici fondamentali del framework SNMP per il suo funzionamento sono:

- sistema gestito (managed object);
- agente di gestione (management agent o master agent) e vari subagent (su sistema gestito);
- sistema di gestione (manager) da remoto;

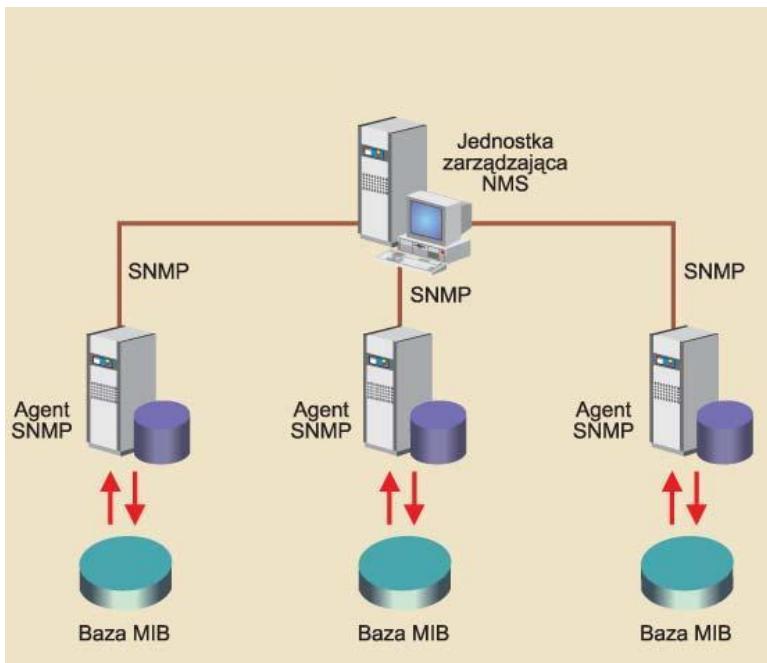
Ogni sistema gestito (per esempio un semplice nodo, un router, una stampante o qualsiasi altro dispositivo che fornisca un'interfaccia di gestione SNMP) ospita un agente di gestione (master agent) e solitamente un certo numero di subagent. Il master agent ha almeno il ruolo di intermediario fra il manager (che è l'applicazione remota che prende le decisioni di gestione, per esempio sotto il controllo diretto dell'operatore umano) e i subagent (che sono gli esecutori di tali decisioni).



Ciascun subagent è incaricato di attuare le decisioni di gestione da parte del manager nel contesto di un particolare sottosistema o relativamente a un particolare aspetto del sistema gestito. In sistemi che forniscono meccanismi di gestione particolarmente

semplici, master agent e subagent possono confluire in un unico componente software capace sia di dialogare con il manager che di attuarne le decisioni; in questo caso si parlerà semplicemente di agent. Abbiamo due elementi tecnici:

- **Protocollo di gestione:** insieme di primitive
- **Modello informativo:** MIB



Il sistema gestito è una realtà di hardware, schede, memorie, processori... (realtà fisica). Un sistema gestito può essere costituito da un nodo, un router, una stampante o qualsiasi altro dispositivo che sia in rete e fornisca una interfaccia di gestione SNMP: esso ospita un agente di gestione (master agent) ed un certo numero di subagent. L'agente funzionante nel sistema gestito ha a disposizione una base locale di dati, denominata MIB (Management Information Base).

L'agente è responsabile dell'accesso

alla base dati MIB, che rappresenta le risorse e le attività nel nodo considerato, cioè rappresenta lo stato del sottosistema gestito. Un dato di MIB (oggetto) potrebbe essere, ad esempio, il contatore dei pacchetti inviati e ricevuti dall'interfaccia nel nodo considerato, o l'indirizzo IP del sistema gestito. Il gestore può controllare il contatore dei pacchetti e monitorare il carico di rete in un determinato nodo. Un ulteriore esempio di dato di MIB è lo stato d'interfaccia. Il gestore può abilitare o disabilitare una determinata interfaccia accedendo alla MIB e modificando il relativo parametro.

L'accesso alla MIB (in lettura e scrittura) rappresenta l'interfaccia fornita al manager per gestire il sistema. Ogni MIB, pur variando nei contenuti specifici, ha la medesima struttura generale e i medesimi meccanismi generali di accesso da parte del manager (lettura e scrittura dei dati). Grazie alla connessione causale della MIB, è quindi possibile al manager agire sullo stato del sottosistema in un modo che è largamente indipendente dalle procedure concrete che devono poi essere messe in atto (dal subagent) per estrarre le informazioni di stato rappresentate nella MIB, o attuare le modifiche di stato a seguito di cambiamenti dei contenuti della MIB.

Il concetto di SNMP è sorprendentemente semplice. La piattaforma della gestione di rete invia interrogazioni (query) all'agente, e lui a sua volta risponde. Interrogazioni e risposte si riferiscono a variabili accessibili da parte del management agent. Il programma che gestisce sa anche collocare i valori delle varie variabili. I sistemi gestiti vengono monitorati e controllati mediante l'uso di semplici comandi SNMP, fra gli altri: read, write, trap.

- Il comando **read** ad esempio, viene utilizzato per il monitoraggio del sistema gestito. L'NMS (manager) può quindi verificare e modificare le diverse variabili del sistema gestito.

- Il comando **write** è utilizzato da NMS per il controllo del sistema gestito. NMS mediante write varia i parametri del sistema.
- Il comando **trap** viene utilizzato per impostare le cosiddette trap ovvero per configurare gli agent in modo da inviare un particolare messaggio al verificarsi di determinati eventi. Quando accade un certo tipo di evento, l'agent invierà il comando trap al NMS e in tal modo risulta possibile sapere, ad esempio, quando una determinata interfaccia di rete smette di funzionare. Trap consente al programma di gestione di tenere la piena conoscenza di eventi importanti, quali ad esempio, restart, errore d'interfaccia ecc.

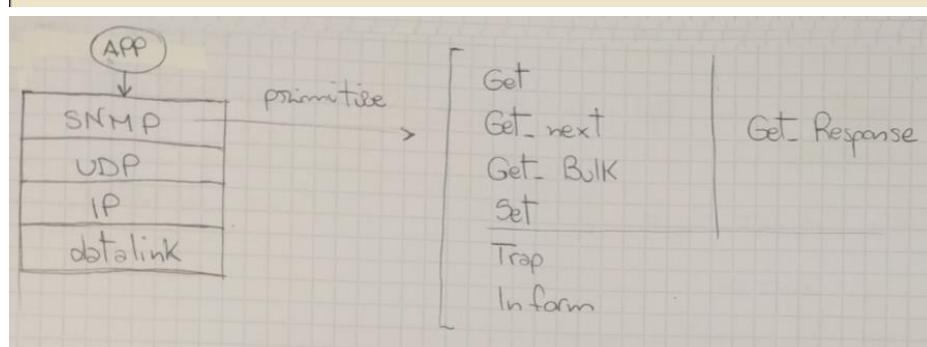
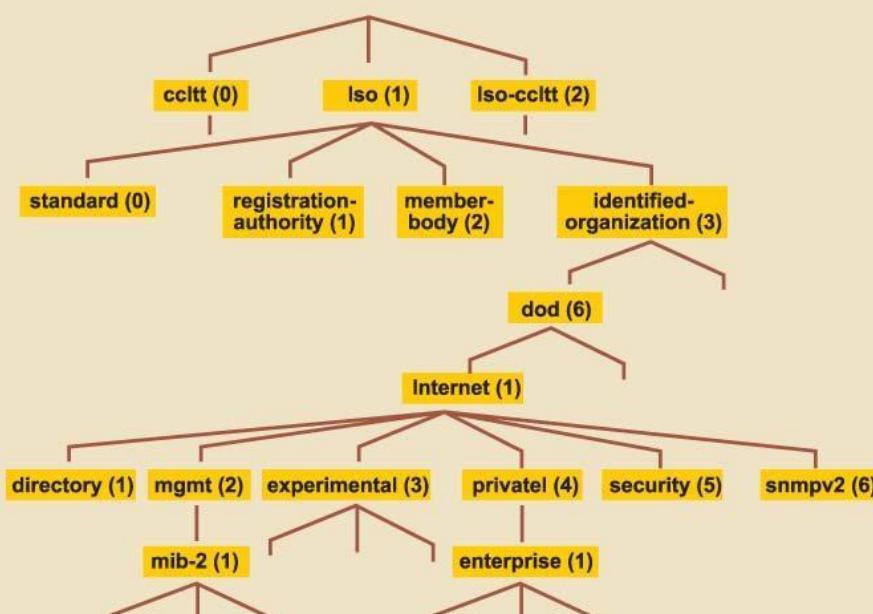
Per mantenere l'ordine e per semplificare il lavoro dell'agent, gli identificatori dell'oggetto (Object ID – OID) sono organizzati gerarchicamente.

La SMI (Structure Management Information) definisce in modo standard come devono essere strutturate le informazioni e la loro gerarchia per essere inserite nel database MIB e quindi gestite da un manager SNMP.

La gerarchia degli oggetti, è ad **albero** con una radice e vari livelli. Ogni oggetto della gerarchia viene identificato in modo univoco, attraverso il suo percorso nell'albero. Il punto rappresenta la radice (root), e i numeri rappresentano i successivi nodi nell'albero degli oggetti. Il livello più alto nella base

MIB è occupato dagli oggetti che fanno parte delle organizzazioni di standardizzazione. I vari produttori possono definire delle basi di dati private, che contengono gli oggetti, relativi ai loro prodotti. Inoltre l'insieme degli apparati di rete gestiti da SNMP appartengono ad una **comunità** (*community*). La comunità rappresenta un **identificativo** che permette di garantire la sicurezza delle interrogazioni SNMP. Un agent SNMP risponde **solo** alle richieste di informazioni effettuate da una Management Station appartenente alla **stessa** comunità. I nomi di comunità sono formati da 32 caratteri e sono di tipo case sensitive. Alcuni esempi di richieste sono:

- GET, usata per leggere uno o più dati di MIB;



- GETNEXT, usata per leggere iterativamente una sequenza di dati di MIB;
- GETBULK, usata per leggere con una sola richiesta grandi porzioni di MIB;
- SET, usata per scrivere (modificare) uno o più dati di MIB.

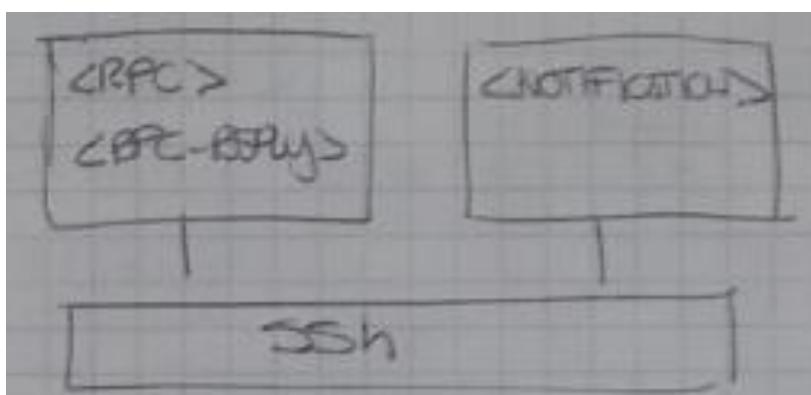
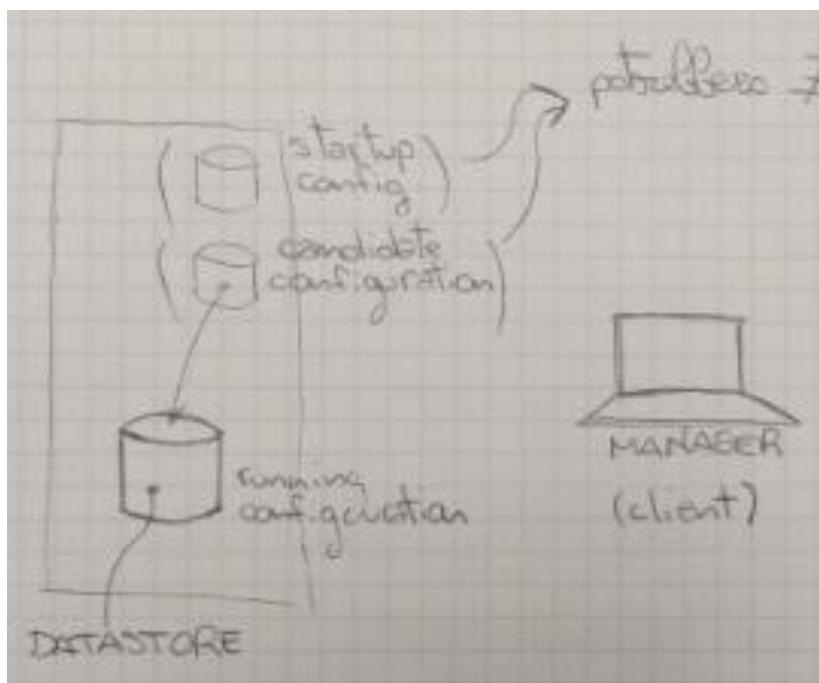
NETCONF

Il protocollo NETCONF è nato per la configurazione di rete. Netconf ha 3 parti:

- PROTOCOLLO RFC 6241
- Meccanismo di subscription delle notifiche RFC 5717
- Linguaggio YANG. È un linguaggio importante RFC 6020.

Il netconf è abbastanza complicato. Dal punto di vista della configurazione abbiamo una situazione in cui abbiamo un system manager che in funzione di client, interagisce con dei sistemi gestiti, non necessariamente solo uno. In questi sistemi gestiti manipola le configurazioni. Ogni sistema ha la sua running configuration che sta da qualche parte dentro il sistema (netconf datastore). La running configuration determina il comportamento del sistema. La vera potenza di netconf si vede quando entrano in gioco altre possibili configurazioni. Esiste un insieme di diverse possibili configurazioni che vengono indicate con le stringhe:

- **Candidate configuration**
- **Startup configuration**

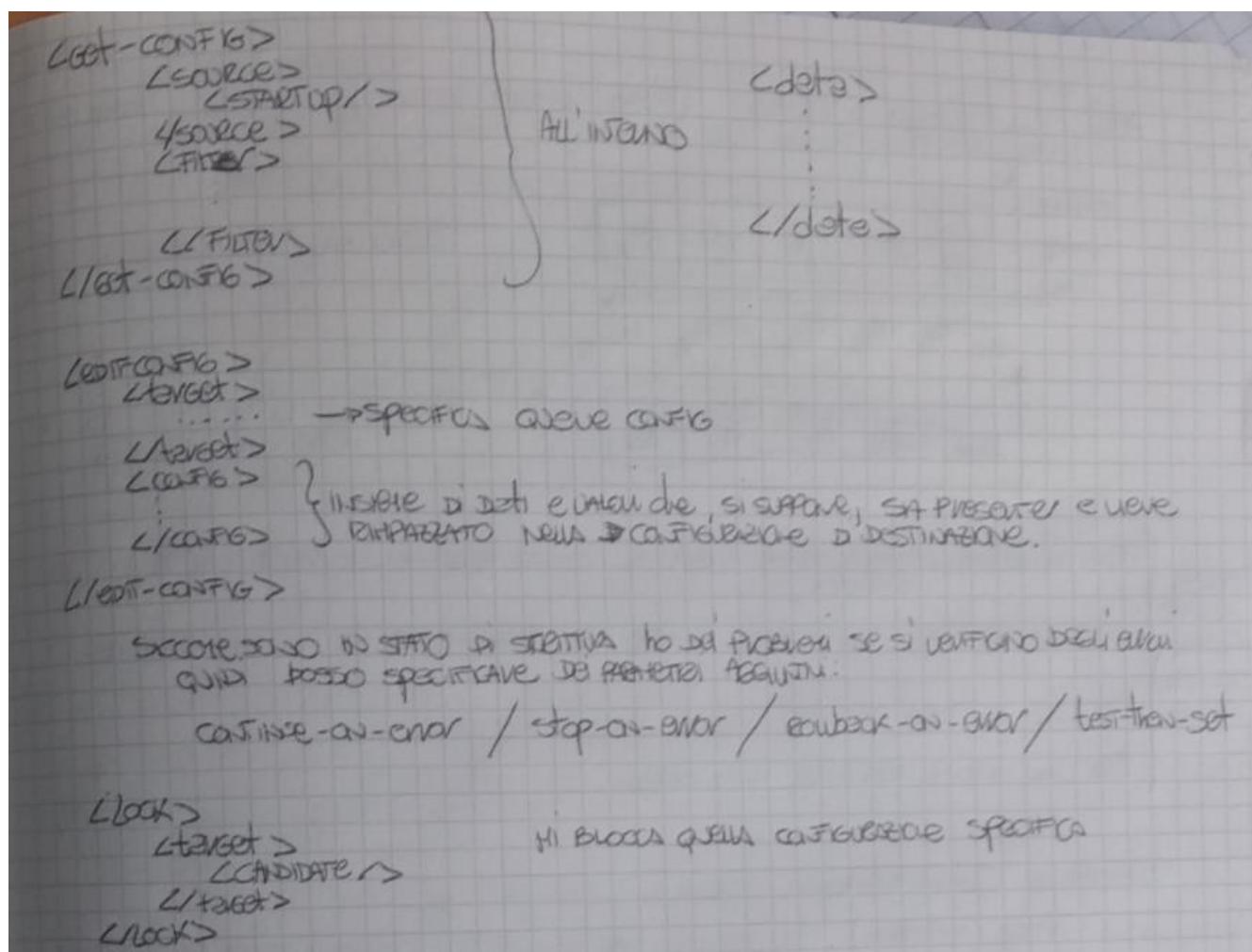


Entrambe possono essere non presenti. Ci sono sistemi che non supportano queste diverse configurazioni. La cosa interessante è che io posso disgiungere le due fasi di definizione inizializzazione della configurazione candidata del sistema, della futura configurazione del sistema, e l'operazione di attivazione della candidate configuration, cioè la startup config e la candidate config diventa la mia running configuration. Il protocollo è pensato per trasportare in maniera sicura delle RPC specificate utilizzando xml. Quando intendo trasporto sicuro, intendo il protocollo SSH o TLS. Sopra l'SSH abbiamo delle RPC, RPC Reply e notifications. Le RPC sono delle operazioni che vengono effettuate sul sistema. Abbiamo un meccanismo in cui c'è un insieme core di operazioni e delle opzioni

che possono essere attivate. queste opzioni si chiamano capabilities. Quando il nostro manager si mette in comunicazione col sistema gestito, avviene o scambio di informazioni, tra cui ci sono le capabilities che mi dicono che cosa posso fare.

Vediamo alcune protocol operations. Esse sono delle RPC che vengono invocate:

- **Hello**: serve per aprire una sessione di gestione e negoziare le capabilità.
- **Get**: legge delle informazioni provenienti dalla running configuration, informazioni di stato
- **Get-config**: legge una configurazione intera oppure utilizzare un insieme di meccanismi di filtri, posso leggere n pezzo della configurazione.
- **Edit-config**: permette di lavorare sugli elementi della configurazione tramite operazioni come merge (esiste un pezzo di configurazione che diventerà parte della configurazione del sistema), replace, create, delete, remove.
- **Delete-config**
- **Lock**: sto ottenendo accesso esclusivo alla configurazione.
- **Unlock**
- **Close session**



<lock>

<target>
<candidate/>
</target>
</lock>

mi blocca quella configurazione specifica

<close-session/>

Possibilità di fare la chiusura aspettando il termine
delle stesse

se durante la sessione avevo fatto una lock, il target
specificato viene sbloccato automaticamente

<kill-session>

<session-id>

</session-id>

</kill-session>

Ho tutto l'XML per l'achello> FASE ...

- Per le capabilities ritagli Avere:

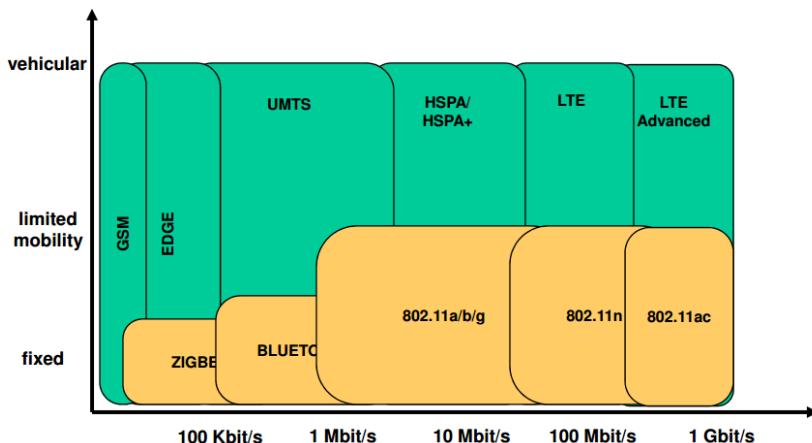
UNITABLE_RUNNING

CANDIDATE_CONFIGURATION

→ essere una candidate config è una nuova
primitiva del protocollo! La commit
oltre a questa anche la <discard-changes>
avendo di solo in grado gestire la
config di un sistema come un sistema
di transazioni distribuito.

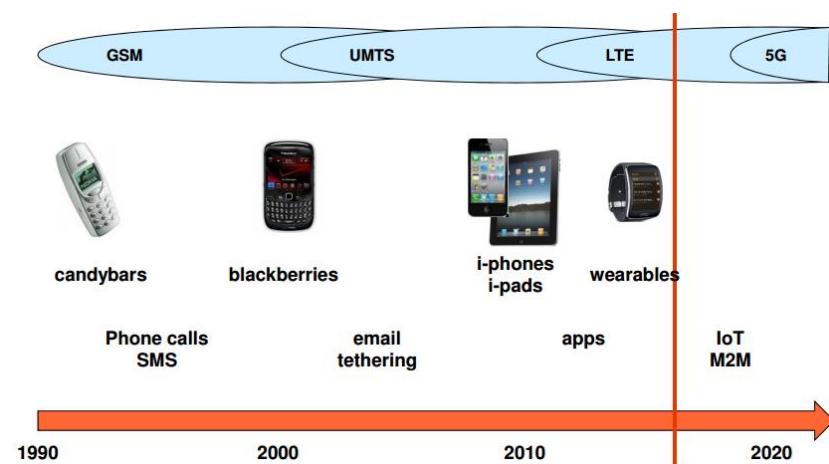
CONFIRMED-COMMIT
CANCELED-COMMIT

12.0 RETI MOBILI



Se confrontiamo le tecnologie radiomobili, la gsm ha una bassa velocità di trasmissione. La velocità porta a degli effetti significativi sulla trasmissione di dati, tipo l'effetto doppler. A certe velocità abbiamo distorsioni. Gli hspa hanno portato la velocità dei dati a livelli superiori. Non ci sono solo le tecnologie radiomobili, ma anche altre come zigbee bluetooth.

EVOLUZIONE DELLE RETI MOBILI E DEI DISPOSITIVI



Nel corso del tempo ci è stata una evoluzione delle reti, degli smartphone e dei servizi.

Negli anni 90 avevamo chiamate ed sms. Dal nokia 6800 quello classico anni 90, si è passati al Black Berry. Nel 2000 arrivano le mail su telefono e servizi di tethering. Quando esce l'Iphone, avviene la rivoluzione; ha portato alla nascita delle app; la modifica grande è stata anche per il business, non solo per i singoli utenti.

Sono nati nuovi servizi che le grosse aziende forniscono per smartphone, tablet. Successivamente sono nati i wearable. Nel 2025 si prevedono 50 miliardi di dispositivi connessi alla rete.

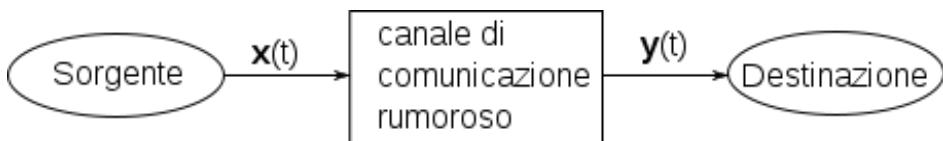
MEZZI DI COMUNICAZIONE

Il termine trasmissione si riferisce alla tecnica utilizzata per trasferire le informazioni attraverso il mezzo di comunicazione, che può essere il cavo, oppure le onde radio. Per poter trasmettere le informazioni, esse devono essere trasformate in segnali fisici, per poter essere propagati nel mezzo di comunicazione. Quando parliamo di sistema di comunicazione, parliamo di un canale. Un canale è un'astrazione. Il canale modella sia il mezzo fisico, che le sorgenti di disturbo (attenuazione del segnale...). La presenza di distorsione e rumore, limita le prestazioni del canale. Ci sono dei canali che sono più robusti al rumore e altri che sono più soggetti al rumore. Cosa significa danneggiare la qualità di una trasmissione? Nyquist, disse che io posso ricostruire un segnale, in maniera precisa, esatta, con un numero di campioni uguale due volte la sua banda. Se ho un canale che ha una banda B, io posso trasmettere 2B simboli al secondo. I simboli sono simboli discreti, configurazione di segnale diversi tra loro. Shannon, nella teoria dell'informazione, ha dimostrato che esiste un limite alla capacità del canale; questa capacità è la banda. La capacità di un canale è la quantità di informazione che può essere trasmessa in maniera affidabile su un canale. La teoria

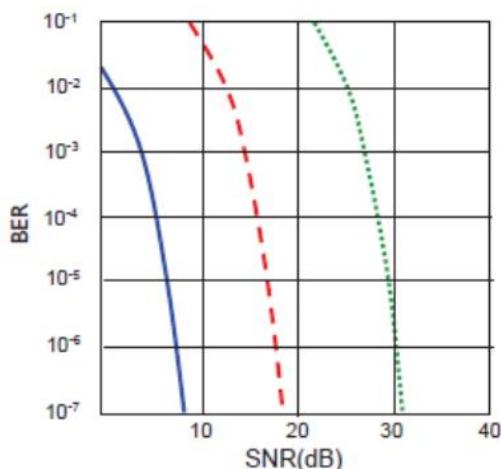
dell'informazione, sviluppata da Claude E. Shannon durante la Seconda guerra mondiale, definisce la capacità di canale e fornisce un modello matematico per calcolarla. La capacità di un canale sottoposto a rumore è:

$$C = B \log_2(1+S/N)$$

dove B è la banda, S rappresenta il segnale e N il rumore, quindi S/N rappresenta il rapporto segnale/rumore.



Maggiore è la frequenza, più è possibile trasmettere bit al secondo; ciò dipende dalla modulazione digitale, ovvero da come i bit sono rappresentati in termini di segnali. I bit non sono gli hertz. La frequenza di un segnale, è abbastanza vicina al numero di simboli al secondo che vengono utilizzati. In un sistema radio, quello che noi vogliamo alla fine, è un'alta efficienza spettrale netta. Alta efficienza spettrale = alta vulnerabilità agli errori.



- QAM256 (8 Mbps)
- - - QAM16 (4 Mbps)
- BPSK (1 Mbps)

Trasmetto piano e ho meno errore. Qam16, trasmetto 4 volte più veloce, ma ho un error bit rate superiore. Nel diagramma il BER (Bit Error Ratio), è il rapporto tra i bit non ricevuti correttamente e i bit trasmessi. Il BER è un parametro molto importante perché fornisce una misura della qualità dell'intero sistema di comunicazione.

$$BER = \frac{\text{numero bit non trasmessi correttamente}}{\text{bit totali trasmessi}}$$

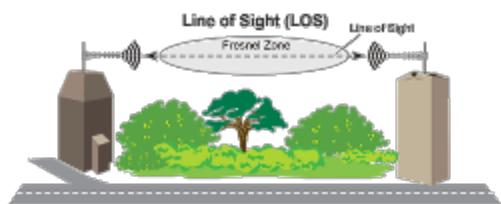
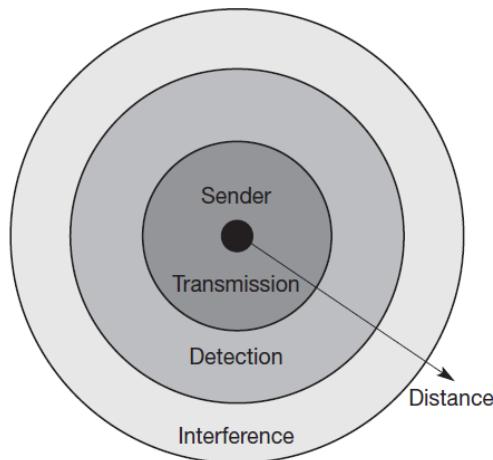
Tale indice è solitamente espresso come coefficiente di una potenza di base 10; pertanto un BER pari a 2×10^{-5} equivale a dire 2 bit errati su 100.000 bit trasmessi. SNR è il rapporto segnale rumore.

TRANSMISSION, DETECTION, INTERFERNCE RANGE

Come nelle reti via cavo, i canali di comunicazione wireless hanno un sender e un ricevitore di segnale. I fattori che

influenzano la propagazione del segnale sono diversi. La direzione di propagazione del segnale nelle reti via cavo, è una sola; nelle reti wireless, non è così. Il cavo se non ha interruzioni o è danneggiato, tipicamente ha le stesse caratteristiche a ogni punto. Si può determinare con precisione il comportamento del segnale che viaggia lungo il cavo. Per trasmissioni wireless, il comportamento prevedibile del segnale è valido solo nel vuoto. Tra il trasmittente e il ricevente possiamo distinguere 3 aree:

- **Transmission range:** entro una prima fascia di un determinato raggio, il ricevente, riceve il segnale con un error rate abbastanza basso da essere in grado di comunicare con il trasmittente.



- **Detection range:** nella seconda fascia, la rilevazione della trasmissione è possibile; la potenza è abbastanza alta per distinguere la trasmissione dal rumore di sottofondo. L'error rate è troppo alto per stabilire una comunicazione.
- **Interference range:** nella terza fascia, che ha raggio più grande, il trasmittente potrebbe interferire con altre trasmissioni, andando ad aggiungere rumore di sottofondo. Il ricevente non sarà in grado di rilevare i segnali, ma questi potrebbero interferire con altri segnali.

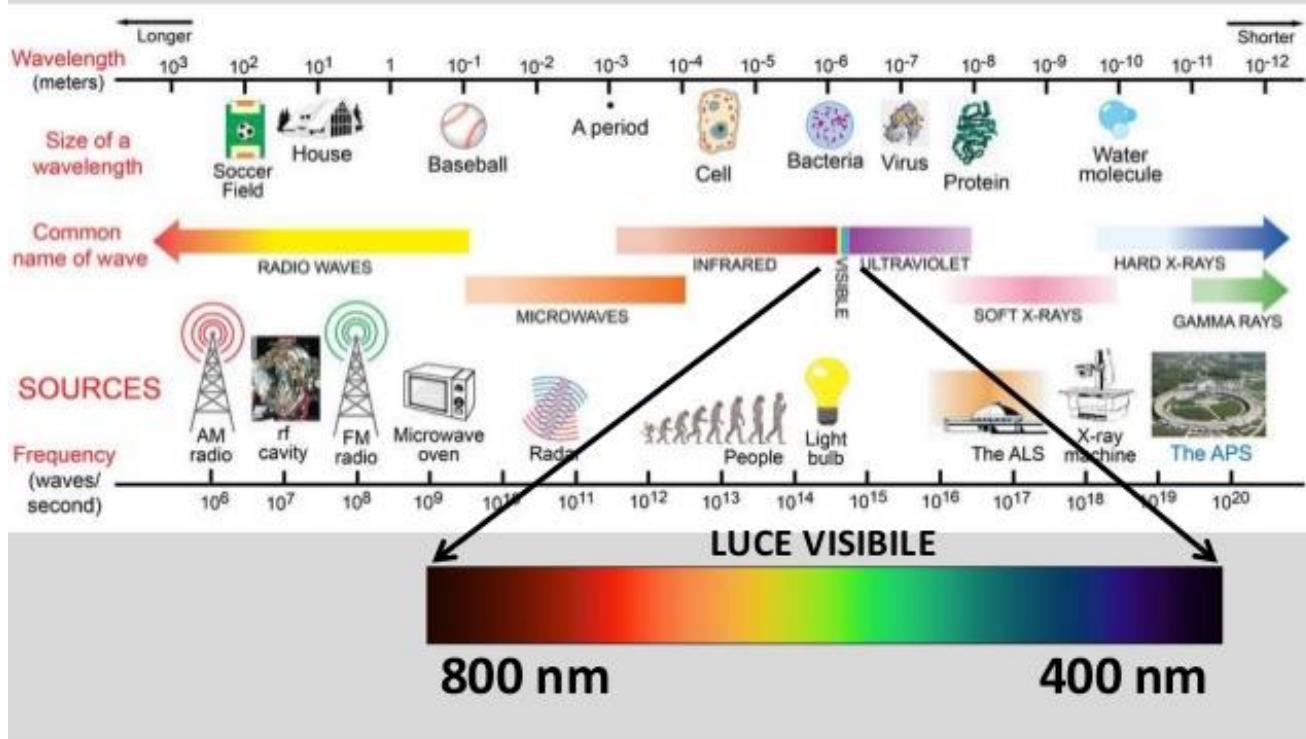
PROPAGAZIONE DEL SEGNALE

Il segnale radio, si propaga seguendo una linea retta, per di più sottoposta all'effetto della gravità. Questa linea retta tra il ricevente e il trasmittente, essa si chiama **line of sight (LOS)**. I fattori che influenzano la propagazione del segnale sono:

- **Distanza:** la potenza P_r del segnale ricevuto, è proporzionale a $1/d^2$: $P_r = \frac{1}{d^2}$ dove d è la distanza tra ricevente e trasmittente. La ragione di ciò è alquanto semplice. Supponiamo che il trasmittente sia in un certo punto dello spazio; esso trasmette un segnale con una certa energia. Questo segnale viaggia dal trasmittente verso lo spazio alla velocità della luce come un'onda con una forma sferica. Se non c'è nessun

Lo spettro elettromagnetico

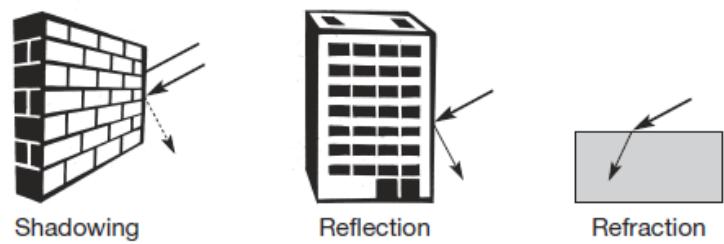
L'insieme di tutte le possibili lunghezze d'onda delle radiazioni elettromagnetiche

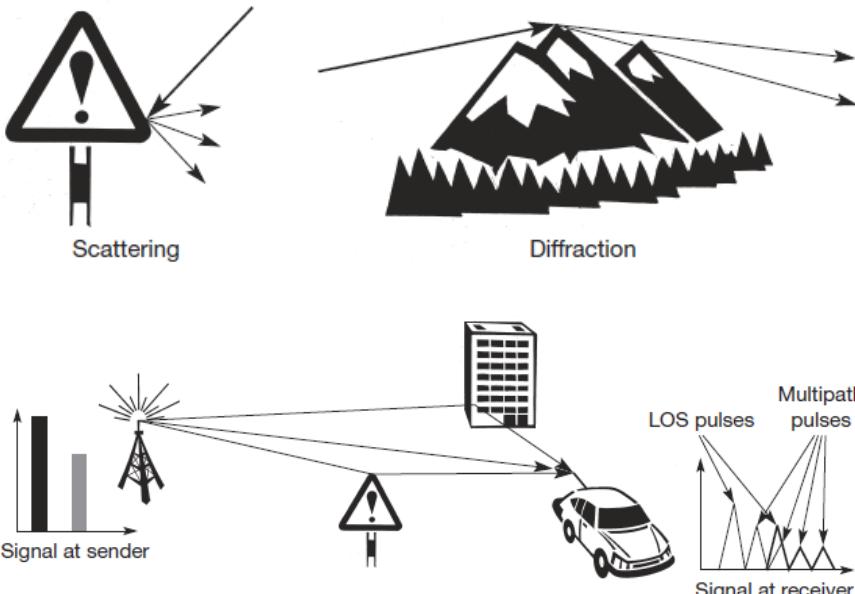


ostacolo, la sfera cresce continuamente; l'energia con cui è stato trasmesso il segnale si distribuisce equamente sulla superficie della sfera. Questa superficie s a partire dal centro, cresce con l'aumentare della distanza d : $s = 4\pi d^2$. La potenza del segnale decresce con la distanza.

- **Atmosfera e condizioni atmosferiche:** la maggior parte delle trasmissioni avviene nell'atmosfera. Essa influisce pesantemente le trasmissioni su lunghe distanze (trasmissioni satellitari...). Le trasmissioni radio mobili, quelle telefoniche, sono influenzate dalle condizioni atmosferiche come la pioggia e la neve. Esse possono assorbire gran parte dell'energia di un segnale diffuso da un'antenna.
- **Frequenza:** la frequenza influisce sulle trasmissioni. Più la frequenza è alta più essa ha un comportamento simile alla luce, e più è sottoposta a fattori di disturbo. Le onde radio possono penetrare gli oggetti. Generalmente più bassa è la frequenza, migliore è la penetrazione negli oggetti. Le onde lunghe (minore è la frequenza, maggiore è la lunghezza d'onda. Maggiore è la frequenza, minore è la lunghezza d'onda), possono essere trasmesse attraverso gli oceani, in un ambiente sottomarino, mentre le altre frequenze possono essere bloccate da un albero. Gli alberi in estate per le trasmissioni telefoniche e ad alta frequenza sono un problema in quanto le foglie, contenendo acqua, assorbono le trasmissioni ad alta frequenza. L'acqua ha un alto tasso di assorbimento delle onde elettromagnetiche. Di conseguenza pioggia, neve e nebbia assorbono le onde ad alta frequenza. A seconda della frequenza, posso avere assorbimenti diversi. A seconda delle frequenze possiamo distinguere:
 - **Ground wave (<2MHz):** le onde con bassa frequenza, seguono la superficie terrestre e si possono propagare per lunghe distanze. Queste onde sono utilizzate per le comunicazioni radio dei sottomarini oppure le AM radio.
 - **Sky wave (2-30 Mhz):** molti trasmettitori broadcast e amatori radio utilizzano queste onde corte che vengono riflesse nella ionosfera. Le onde propagandosi nell'atmosfera sono sottoposte a diffrazione. L'atmosfera, più ci si allontana dalla superficie terrestre, diventa meno densa salendo di altitudine e l'angolo di diffrazione diminuisce. Arrivate a un certo punto dell'atmosfera, l'onda subisce una riflessione e torna verso il basso. Tornando verso il basso l'onda subendo una diffrazione, avrà un angolo di diffrazione maggiore poiché tornando verso terra l'atmosfera si fa più densa. Dalle nozioni di fisica, più è denso un mezzo, maggiore sarà l'angolo di diffrazione. Minore è la densità del mezzo, minore sarà l'angolo di diffrazione.
 - **Line of sight (>30 MHz):** i mobile phone systems, i sistemi satellitari, utilizzano frequenze ancora più alte. Le onde emesse seguono una linea retta. Questo permette la comunicazione diretta con i satelliti.

Nella vita reale, raramente abbiamo una linea retta tra il ricevente e il trasmittente per le comunicazioni radio. I telefoni sono utilizzati tipicamente nelle grandi città in cui ci sono grattacieli, vicino alle montagne, dentro gli edifici, mentre si guida attraverso una valle. Questi sono fattori di attenuazione del segnale. Un fenomeno di attenuazione

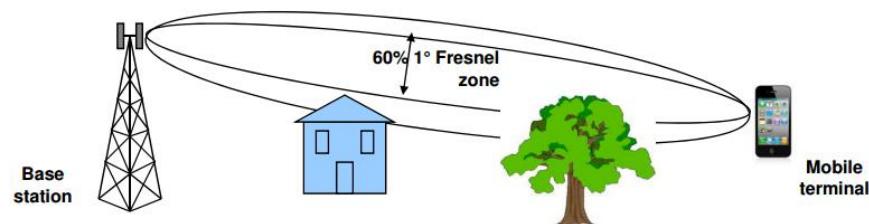




è il **blocking** o **shadowing** dei segnali radio dovuto a grandi ostacoli. Anche i piccoli ostacoli come un semplice muro o un camion nella strada o gli alberi, una montagna o una valle possono bloccare il segnale. Un altro effetto è la **riflessione** del segnale; il segnale riflesso non ha la stessa potenza prima della riflessione, in quanto una piccola parte di energia è stata assorbita dall'ostacolo su cui si è riflettuta l'onda. Più volte il segnale viene riflesso e più

debole il segnale diventa. Un altro fenomeno è lo **scattering**. Con lo scattering, il segnale dopo che ha colpito un oggetto, si divide in segnali più deboli che si propagano su percorsi diversi nel mezzo. Gli effetti sopra citati, comportano un fenomeno: **multi-path propagation**. Le onde radio emesse dal trasmittente possono viaggiare in linea retta, oppure potrebbero essere riflesse o sottoposte a fenomeni di scattering. La figura mostra solo 3 possibili percorsi, ma nella realtà è più complesso.

Nella realtà ci potrebbero essere molti più percorsi. I segnali che viaggiano su percorsi diversi arriverebbero al



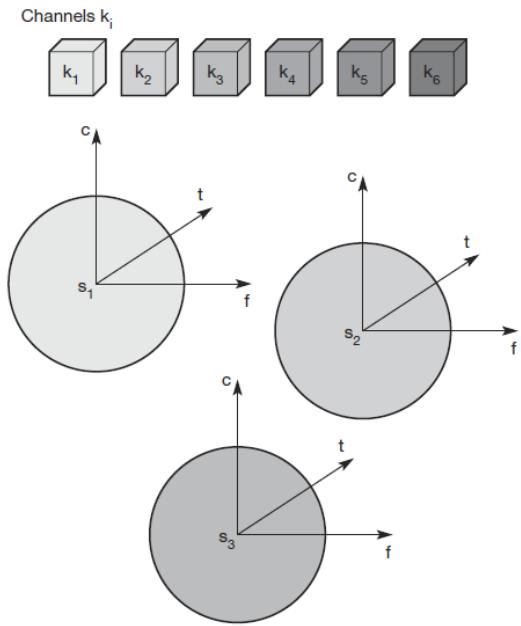
ricevente in momenti diversi. La potenza di un segnale è distribuita su un elissoide, **elissoide di fresnel**. Se in mezzo all'elissoide ho un ostacolo (dove si concentra il 60% della potenza del segnale), un segnale può rimbalzare e andare a fare un disturbo rispetto al segnale originale. Più è alta la frequenza più sono alti i disturbi. Quindi meglio trasmettere a 700 MHz che a 6 GHz.

MULTIPLEXING

Il multiplexing è un meccanismo che non viene utilizzato solo in telecomunicazioni, ma anche nella vita di tutti i gironi. Il multiplexing descrive come molti utenti possano condividere una risorsa con una minima oppure totale assenza di interferenza. Un esempio è l'autostrada e le auto che la percorrono: il motivo per cui non ci sono interferenze (incidenti) è dovuto all'utilizzo di strisce (Space division multiplexing) che separano il traffico. Inoltre le macchine utilizzano una stessa corsia in tempi diversi (time division multiplexing). Per le comunicazioni wireless il multiplexing può essere:

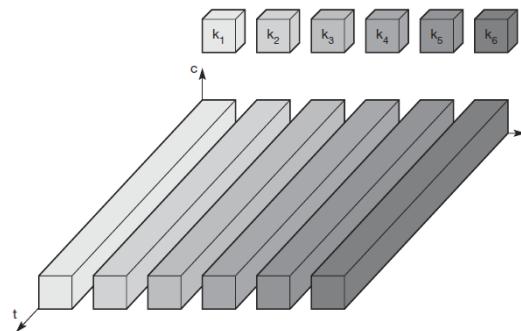
- **spaziale**
- **temporale**
- **frequenza**
- **codice**

MULTIPLEXING SPAZIALE SDM



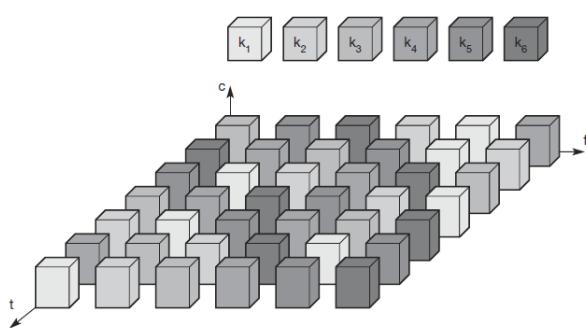
Nelle comunicazioni wireless, il multiplexing spaziale implica un trasmittente separato per ogni canale di comunicazione con una distanza abbastanza ampia tra i trasmittenti. Questa tipologia di multiplexing è utilizzata per esempio dalle stazioni FM radio dove il range di trasmissione è limitato a una certa regione. Utilizzando questa tipologia di multiplexing, i problemi insorgono quando se due o più canali di comunicazione vengono aperti nello stesso spazio; ad esempio se molte stazioni radio vogliono trasmettere nella stessa città. Ma in questo caso si utilizzano altre tipologie di multiplexing. A ogni canale di comunicazione viene fornito la stessa frequenza, ma per evitare interferenze, ci deve essere uno spazio di **guardia**, una zona cuscinetto per evitare interferenze.

MULTIPLEXING FREQUENZA FDM



Il **frequency division multiplexing (FDM)**, descrive schemi per dividere lo spettro delle frequenze in molte bande di frequenza che non si sovrappongono. A ogni canale viene fornita la sua frequenza. Una trasmittente che utilizza questa frequenza, la può utilizzare continuamente. Questo schema viene utilizzato dalle stazioni radio che vogliono trasmettere in una stessa regione di spazio, dove ogni stazione radio ha la propria frequenza.

MULTIPLEXING TEMPORALE TDM

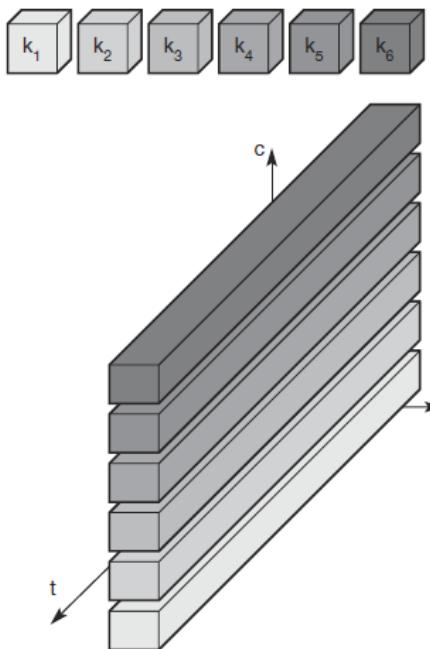


Una forma di multiplexing più flessibile è il **time division multiplexing (TDM)**. A un canale viene data una frequenza per un certo periodo di tempo. I trasmittenti utilizzano tutta la stessa frequenza ma con finestre temporali diverse. È necessaria una rigorosa sincronizzazione per evitare interferenze tra i trasmittenti. Frequenza e time division multiplexing possono essere combinati tra loro; in questo modo un canale può utilizzare una certa frequenza per un determinato periodo di tempo.

Il gsm utilizzava la separazione in tempo e frequenza per una trasmissione tra un telefono e una base station.

MULTIPLEXING CODICE

Il **code division multiplexing (CDM)** è un nuovo schema commerciale nel settore delle telecomunicazioni. Prima veniva utilizzato per applicazioni militari per la sicurezza che esso offre. Ora viene utilizzato in ambito civile. I canali di comunicazione possono utilizzare la stessa frequenza, allo stesso momento per le trasmissioni. La separazione ora è ottenuta assegnando a ciascun canale un codice. Il tipico esempio del CDM è il seguente: immaginiamo un party in cui ci sono molti partecipanti provenienti da paesi differenti che decidono di comunicare tra loro utilizzando un range di frequenze (300-6000 Hz, che dipende dalla voce della



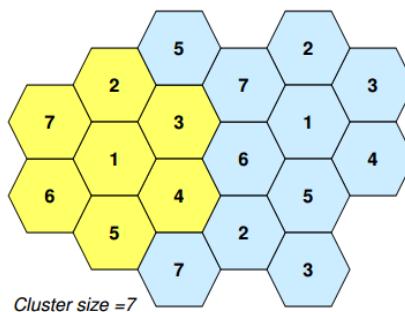
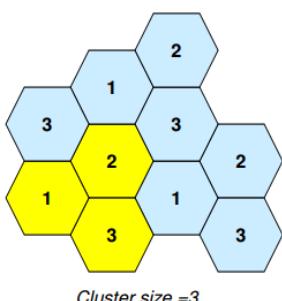
persona) allo stesso istante. Se tutti parlano la stessa lingua, SDM è necessario per poter stabilire una comunicazione (parlando a distanza ravvicinata con chi ho di fronte). Se iniziamo a utilizzare un'altra lingua, io posso separare la mia comunicazione da altre che utilizzano la stessa lingua, ma diversa dalla mia (le altre conversazioni appaiono come rumore di fondo). Questo spiega perché il CDM è sicuro. Se la lingua è sconosciuta, i segnali possono essere ancora ricevuti, ma sarebbero inutili. Utilizzando un codice segreto, una comunicazione sicura può essere stabilita in un ambiente ostile.

Il CDM fornisce vantaggi per le trasmissioni wireless e da una buona protezione contro le interferenze. Vanno assegnati differenti codici, ma sicuramente lo spazio dei codici è più ampio di quello delle frequenze.

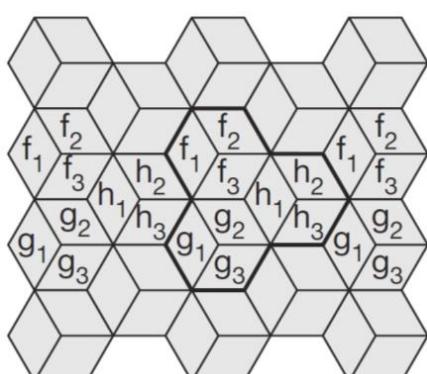
Assegnare un codice individuale a ciascun trasmittente non è un problema. Il problema è l'alta complessità del ricevente. Il ricevente deve sapere il codice e deve riuscire a separare la comunicazione con il trasmittente dal rumore di fondo e degli altri segnali. Quando trasmetto prenderò il segnale e lo moltiplico per il codice.

comunicazione con il trasmittente dal rumore di fondo e degli altri segnali. Quando trasmetto prenderò il segnale e lo moltiplico per il codice.

COPERTURA DI SEGNALE



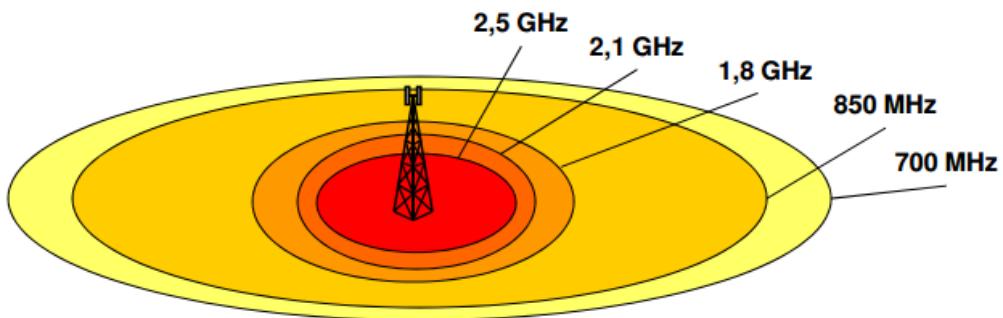
I sistemi per la telefonia mobile implementano l'SDM. Ciascun trasmittente, tipicamente chiamato **base station**, copre una determinata area chiamata **cella**. La dimensione delle celle può variare da alcune decine di



metri negli edifici, a centinaia di metri nelle città, fino a decine di chilometri nelle pianure. La forma delle celle non è mai perfettamente circolare o esagonale, ma dipende dall'ambiente (palazzi, montagne...) o dalle condizioni atmosferiche. Per evitare interferenze, differenti trasmittenti utilizzano l'FDM. Le celle formano **clusters**. I cluster si ripetono regolarmente, e ogni frequenza può essere utilizzata una sola volta per cluster. Più grande è il cluster, minore è l'interferenza, ma maggiore è l'utilizzo di risorse. Le celle dentro i cluster utilizzano un insieme disgiunto di frequenze. Una cella utilizza una frequenza d1,

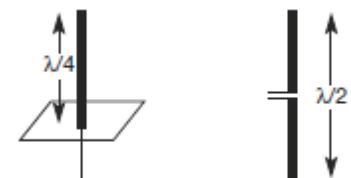
un'altra una frequenza f2 e la terza una frequenza f3. Celle vicine tra loro, hanno frequenze diverse assegnate per evitare interferenze. Nelle reti in cui non si utilizzano i principi di copertura delle reti cellulari (WLAN) non c'è il clustering e una pianificazione delle frequenze. L'immagine mostra il riutilizzo delle frequenze. La potenza di un trasmittente deve essere limitato per evitare interferenze con le celle accanto che utilizzano la stessa frequenza. Per evitare ulteriori interferenze, vengono utilizzate le **sectorized antennas**. La figura accanto mostra l'utilizzo di 3 settori per cella in un gruppo di tre celle. Ha senso utilizzare le sectorized antennas invece di antenne omnidirezionali per celle di

raggio più grande. Il fisso assegnamento di frequenze a gruppi di celle e alle celle, non è molto efficiente se il carico di traffico varia (Schema **fixed channel allocation**). Nel caso di traffico pesante in una cella e di carico leggero nella cella accanto, avrebbe senso **prestare** le frequenze. Alle celle con più traffico vengono assegnate più frequenze. Questo schema è conosciuto come **borrowing channel allocation (Bca)**. L'**FCA** è utilizzato nel GSM system. A seconda delle frequenze che si utilizzano, il cerchio attorno alla cella è più o meno grande. Il segnale degrada di più. Più è alta la frequenza, più è basso il cerchio, in quanto l'alta frequenza sottoposta ad assorbimenti e fenomeni prima visti. La bassa frequenza invece offre un raggio di portabilità più ampio. Più alta è la frequenza, più sono necessarie celle per coprire una stessa area. Le celle ad alta frequenza tornano utili quando il traffico è intenso e utilizzo più celle per coprire una stessa aerea.



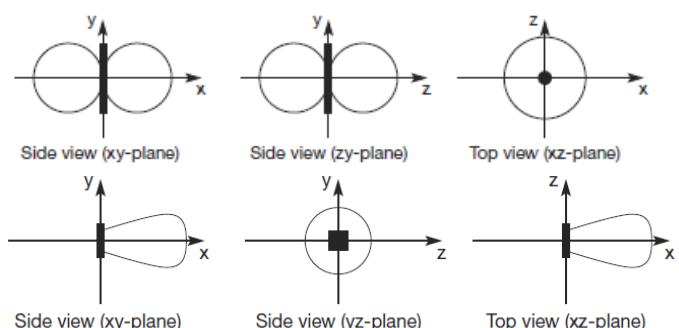
LE ANTENNE

Le antenne catturano l'energia delle onde elettromagnetiche e la mandano da un cavo coassiale allo spazio attorno a essa. Un'antenna di riferimento teorica è l'**isotropic radiator**, un'antenna nello spazio che irradia la stessa potenza in tutte le direzioni; tutti i punti sono alla stessa potenza e sono collocati su una sfera attorno all'antenna. La radiazione attorno all'antenna, è simmetrica in tutte le direzioni. Questa antenna non esiste nella realtà. Nella realtà le antenne hanno intensità della radiazione che non è uguale in tutte le direzioni. L'antenna più semplice è l'antenna **Hertian dipole**. Essa consiste in due conduttori di uguale lunghezza disposti linearmente, separati da un piccolo spazio, la lunghezza di un'antenna non è casuale, ma dipende dalla lunghezza d'onda che deve ricevere o inviare. Le antenne della macchina montate sopra il tetto sono di lunghezza $\lambda/4$.



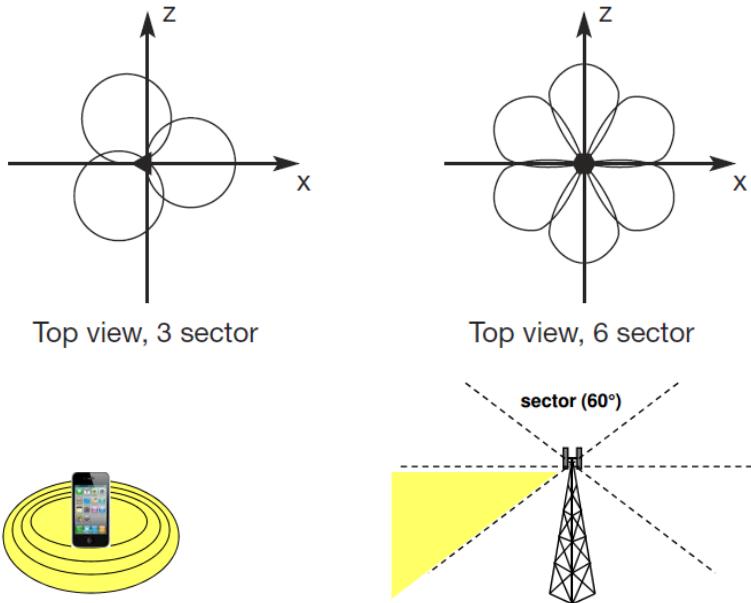
Le antenne possono essere di due tipi:

- **Omnidirectional**: questa antenna è progettata per trasmettere\ricevere in tutte le direzioni con la stessa efficienza. Ad esempio i telefoni cellulari predispongono di antenne omnidirezionali.
- **Directional**: se un'antenna è posizionata in una valle, oppure tra due palazzi, un'antenna omnidirezionale non torna utile. In questo caso le antenne direzionali propagano il segnale in una determinata direzione. Un esempio sono le antenne satellitari, utilizzate per trasmettere e ricevere in una sola direzione.



Le antenne direzionali vengono utilizzate nelle celle della telefonia mobile. Molte antenne direzionali possono essere combinate tra loro per costruire un'**antenna settorizzata**. Un'antenna può essere settorizzata in 3,4,6 settori per abilitare il riutilizzo delle frequenze. Le antenne direzionali coprono settori con un angolo di 45°-60°- 90°-120° sul piano orizzontale.

Un'altra tipologia di antenna, è la MIMO; sono una nuova tipologia di antenna che dispongono di elementi indipendenti, ravvicinati per trasmettere e ricevere. Il 2x2 MIMO dispone di due trasmettitori e due ricevitori. Questi elementi possono trasmettere diverse copie dello stesso segnale con tempi appropriati e phase shift, che combinati, al ricevitore arriva un segnale più robusto. In condizioni di buona propagazione, MIMO system può trasmettere segnali indipendenti in parallelo per aumentare la velocità di trasmissione.



ARCHITETTURA GSM

Il GSM è il sistema di telecomunicazioni che ha avuto più successo al mondo fino a oggi. È utilizzata da oltre 800 milioni di persone in più di 190 paesi. Il GSM (Global System for Mobile communication) nacque nel 1982. La rete GSM che vedremo noi, supporta solo voce ed sms. Il primario obiettivo della rete GSM, era quello di trasmettere la voce con una buona qualità. Un altro servizio offerto dalla rete GSM è il numero di emergenza. Lo stesso numero può essere utilizzato in tutta Europa. Questa connessione al numero di emergenza ha alta priorità rispetto alle altre comunicazioni e sarà stabilità con il centro emergenza più vicino. Un altro servizio offerto è l'SMS (Short Message Service) che permette una trasmissione di messaggi fino a 160 caratteri.

Partendo dal terminale per poter interagire con l'architettura GSM, esso è costituito da:

- **Mobile station (MS)**
- **Sim (Subscriber identity module)**

L'MS può essere identificato attraverso l'**international mobile equipment identity (IMEI)**. Senza la SIM card è possibile effettuare solo chiamate di emergenza. La SIM è caratterizzata da:

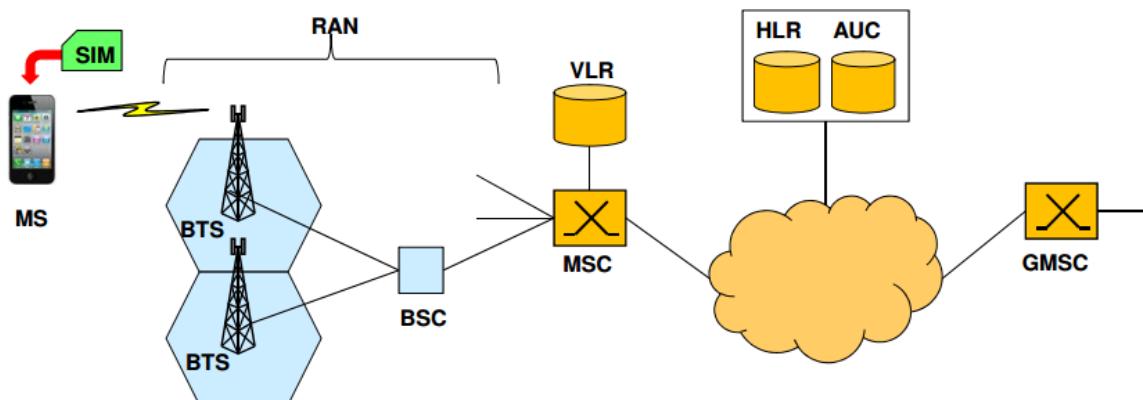
- Numero seriale
- Lista dei servizi a cui è sottoscritta
- Codice PIN (Personal Identity Number)
- Codice PUK (Personal Unblocking key)

Il PIN è utilizzato per sbloccare il telefono e se lo si sbaglia per tre volte, è necessario utilizzare il codice PUK.

Un sistema GSM consiste di un'architettura gerarchica; l'utente vede solo alcune parti della rete GSM come la mobile station e la base transceiver station (BTS).

Vediamo nello specifico la rete GSM:

- **Radio Access Network (RAN)** comprende:
 - **Base Transceiver Station (BTS)**: comprende le antenne radio per la trasmissione delle comunicazioni. La BTS può formare una radio cella utilizzando sectorized antenne. Una cella GSM misura dai 100 m a 3.5 km a seconda dell'ambiente in cui si trova (palazzi, montagne...). La BTS si connette con la MS, la mobile station.
 - **Base Station Controller (BSC)**: il BSC gestisce le BTS. Gestisce le frequenze radio, l'handover della MS; gestiscono tutta la parte dei controlli radio (si accorgono se il segnale cade o no...).
- **Rete core** comprende:
 - **Mobile services switching center (MSC)**: sono switcher da alte performance. Stabiliscono la connessione con altri MSC e BSC.
 - **Home Location register (HLR)**: è il più importante database nella rete GSM in quanto conserva le informazioni relative agli utenti. Comprende informazioni come l'ISDN number (MSISDN), servizi a cui è sottoscritta la sim (inoltro di chiamata, restrizioni roaming...) e il codice international mobile subscriber identity (IMSI). Altre informazioni che vi sono all'interno sono la **location area (LA)** del mobile station, il VLR corrente e il MSC corrente. Come la MS lascia la LA corrente, le informazioni nell'HLR vengono aggiornate. Questo database è utile per localizzare un utente nel mondo all'interno della rete GSM. Ogni gestore possiede un database centrale, denominato Home Location Register (HLR), che memorizza permanentemente sia i dati di abbonamento degli utenti (noti come statici) sia i dati (detti dinamici) che possono variare a seguito di azioni degli utenti stessi (attivazione servizi supplementari, ecc.) che l'identità del VLR presso cui la MS dell'utente è registrata come "visitor".
 - **Visitor Location Register (VLR)**: il VLR è associato a ogni MSC. È un database dinamico che conserva informazioni importanti per le MS correnti che si trovano nella LA, la quale è associata alla MSC. Se una nuova MS entra nella LA, il VLR ha il compito di copiare tutte le informazioni rilevanti del nuovo utente dall'HLR. Questa gerarchia di HLR E VLR evita frequenti aggiornamenti dell'HLR. Nel VLR c'è la lista degli utenti, presenti presso un nodo della rete radiomobile.



	MS = Mobile Station = Mobile Equipment + SIM SIM = Subscriber Identity Module BTS = Base Terminal Station BSC = Base Station Controller (GM)SC = (Gateway) Mobile Switching Center VLR = Visitor Location Register HLR = Home Location Register AUC = Authentication Center RAN = Radio Access Network
--	--

Il location register sa dove si trova l'utente. Scenario: terminale nuovo, quindi aggiorno il location register: guarda che qui mi è comparso questo nuovo dispositivo. Il location manager cambia il VLR e avverte il vecchio VLR dicendogli che non è più lì.

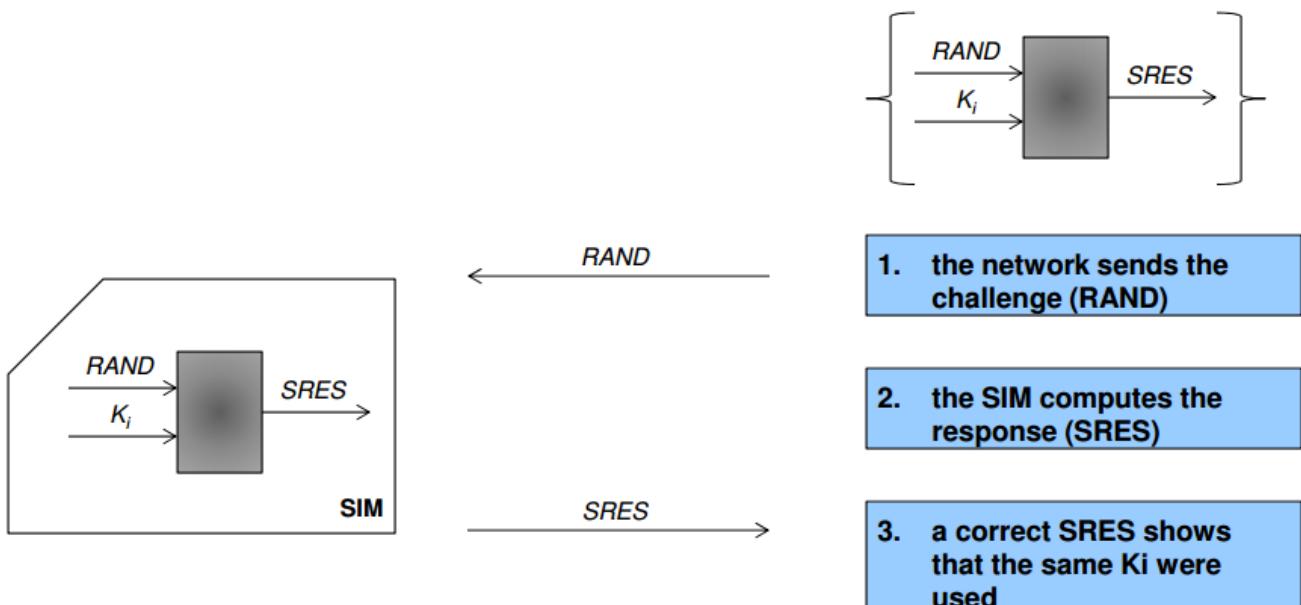
La rete GSM utilizza tecniche FDM e TDM. Upstream e downstream sono separati in frequenza (Frequency Division Multiplexing).

Gli identificatori nella rete GSM sono i seguenti:

- **MSISDN (Mobile Station ISDN Number)**: identifica univocamente un abbonato nel piano di numerazione della rete telefonica commutata pubblica internazionale. È il nostro numero di cellulare. Rappresenta noi.
- **IMSI (International Mobile Station Identifier)**: identifica univocamente l'abbonato all'interno di una qualunque rete GSM e che è contenuto anche all'interno della SIM card;
- **TMSI (Temporary Mobile Station Identifier)**: usato per garantire la sicurezza del IMSI, viene assegnato ogni volta che si cambia Location Area (LA);

SICUREZZA GSM

Prima che un utente possa iniziare a utilizzare i servizi della rete GSM, è necessaria l'autenticazione. L'autenticazione si basa sulla SIM, la quale contiene la chiave di autenticazione individuale K_i , lo user identification IMSI. Le credenziali di un radiomobile, che si chiamano chiavi ki , non sono nella rete. Sono nella sim e nell'Authentication center e da lì non escono. L'authentication center con la stessa chiave ki della sim genera un SRES. Successivamente usa il numero random RAND, utilizzato assieme alla ki per generare il SRES, e lo invia alla SIM, la quale con questo numero RAND, assieme alla ki che essa possiede, genera uno SRES. Così i due SRES, uno della sim e l'altro dell'authentication center, vengono confrontati e verificati. Se sono compatibili allora alla sim viene permesso di accedere alla rete.

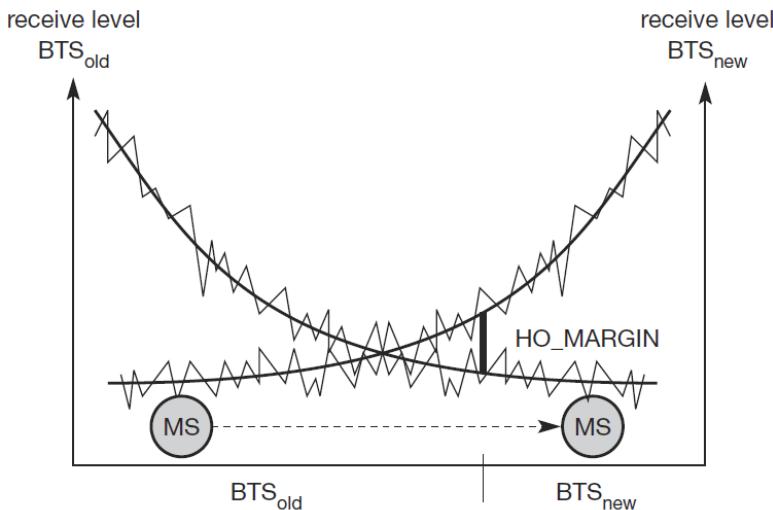


**GSM authentication guarantees the SIM (that is the MS); the user identity is assured by his/her ability to activate the SIM (PIN knowledge)
The network identity is not verified**

HANDOVER

La rete cellulare richiede l'**handover**, una procedura indispensabile, in quanto le celle non coprono uno spazio infinito, ma limitato; fino a 35 km per le antenne in spazi aperti e poche centinaia di metri per le celle in città. Più è piccola la cella più e più è veloce il passaggio di una mobile station attraverso le celle (fino a 250 km/h per le reti GSM), più handover sono richiesti. L'handover non dovrebbe causare la terminazione di una chiamata. Il GSM, mira a far durare l'handover per un massimo di 60 ms. Ci sono 2 ragioni per cui viene effettuato l'handover.

- La mobile station si muove fuori dal range della BTS. La potenza del segnale ricevuto decresce continuamente fino a quando non raggiunge i livelli minimi indispensabili per mantenere la comunicazione. L'error rate cresce a causa delle interferenze e della distanza dall'antenna. Tutti questi fattori diminuiscono fino a ridurre la qualità del collegamento radio.
- La rete cablata (MSC, BSC) potrebbero decidere che il traffico in una cella è troppo alto e sposta alcuni mobile station in altre celle che hanno un carico minore (se possibile). L'handover è dovuto a un fenomeno di **load balancing**



Durante ogni conversazione si esegue continuamente l'analisi del livello e della qualità di questa. Quando il terminale si allontana dalla BS, il livello del segnale utile diminuisce, mentre aumenta quello del rumore dovuto ad interferenze. Quindi il BS Controller (che rappresenta l'interfaccia tra la BS e il MSC) si accorge che il valore del rapporto S/N richiesto è diminuito e invia una richiesta di handover al MSC. Questo MSC verifica se le celle adiacenti sullo stesso canale xxx offrono una qualità migliore del segnale utile. Quindi, il MSC invia alla BS "B" e a tutte le eventuali BS delle celle adiacenti, la richiesta di handover, a cui tutte le BS rispondono inviando il risultato del calcolo del rapporto S/N sul canale xxx. Se dal confronto la BS "B" è quella che offre il più alto S/N, si realizzerà l'handover tra la BS "A" e la BS "B", e dal MSC partirà l'ordine, impartito attraverso un messaggio di segnalazione che viaggia sul canale xxx, di attivare il nuovo ricetrasmettitore sul canale yyy. Di seguito (Fig. 12.1-29) il MSC invierà l'ordine di commutazione alla vecchia BS, utilizzando il canale xxx, la quale provvederà a trasmetterlo al terminale mobile, usando sempre il canale xxx (perché è su questo canale che sta dialogando il terminale). A questo punto la stazione mobile (MS) invia una conferma dell'ordine ricevuto sul canale xxx e si sintonizza sul canale yyy. Per terminare l'handover la BS "A" rilascia il canale xxx, che sarà così disponibile ad altre conversazioni; nel frattempo MS e la BS "B" si attivano sul canale di conversazione yyy. La richiesta di handover può essere avanzata sia

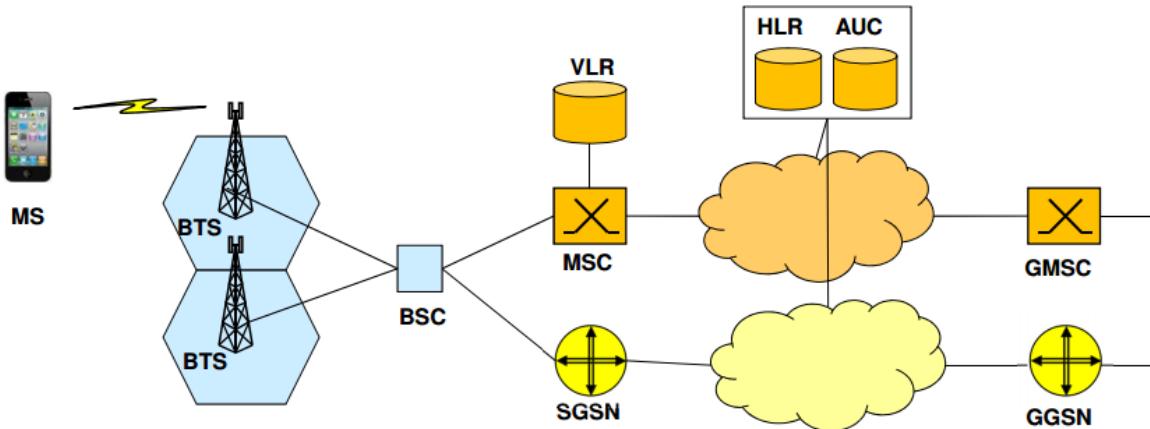
Come già detto, l'operazione che la rete mobile compie per mantenere la comunicazione anche quando il terminale si muove, prende il nome di **HANDOVER** (passamano), in quanto si verifica una sorta di "passamano" tra la vecchia e la nuova BS. Essendo la connessione gestita dal MSC, quando l'utente si sposta in una cella, relativa ad una nuova BS, confinante con la precedente, si crea un circuito che collega il MSC alla nuova BS e attraverso un'interfaccia aerea si raggiunge il terminale.

dalla BS (in questo caso si parla di NETWORK CONTROLLER) oppure dal terminale stesso (MOBILE ASSISTANT).

EVOLOZIONE ARCHITETTURA GSM



Overlaying data on GSM: GPRS and EDGE



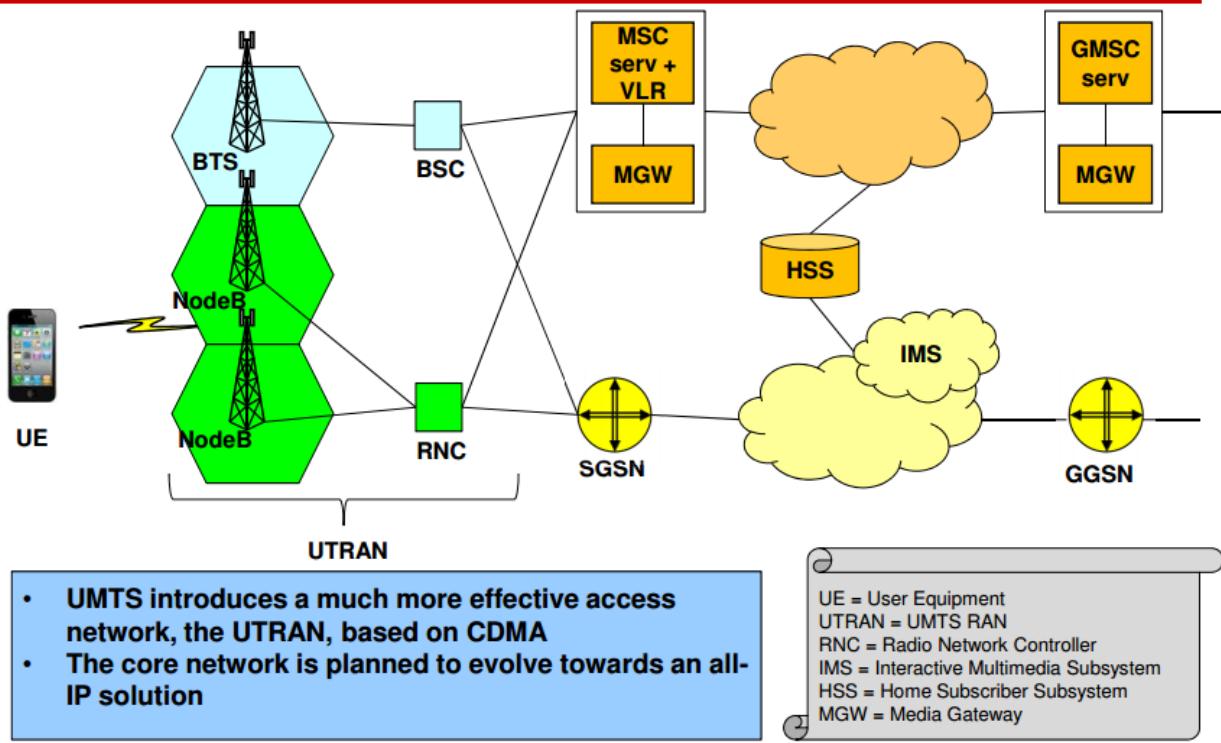
- In 2° generation mobile networks such as GSM, the solution to support data communication was to overlay a packet-switching core network to the existing infrastructure
- In this way basic access to data networks (and the Internet) was provided, but the RAN remained the same, with its limited capacity: GPRS/EDGE networks offered Internet access at tens of kbits/s

GPRS = General Packet Radio Service
 SGSN = Serving GPRS Support Node
 GGSN = Gateway GPRS Support Node
 EDGE = Enhanced Data rate for GSM Evolution

In telecomunicazioni il **General Packet Radio Service (GPRS)** è una delle tecnologie di telefonia mobile cellulare. Viene convenzionalmente definita di generazione 2.5, vale a dire una via di mezzo fra la seconda (GSM) e la terza generazione (UMTS). È stato il primo sistema cellulare progettato specificatamente per realizzare un trasferimento dati a commutazione di pacchetto e a media velocità su rete cellulare per agganciarsi alla rete Internet, usando i canali TDMA della rete GSM. Si tratta quindi di un'evoluzione o servizio aggiuntivo per il sistema GSM, per mezzo di alcune modifiche hardware e software al sistema, tanto che si parla di GSM/GPRS conservando la classica commutazione di circuito propria del GSM per il traffico vocale e tutti gli altri servizi. Il **GPRS** espande le funzionalità dei servizi di scambio dati basati su GSM, fornendo:

- Servizio PTP (*Point-to-Point*): interconnessione fra reti internet (protocollo IP) e reti basate su X.25
- Servizio PTM (*Point-to-Multipoint*): chiamate di gruppo e chiamate multicast
- Messaggistica MMS (*Multimedia Messaging Service*)
- Servizi in modalità anonima: accesso anonimo a determinati servizi.
- Future funzionalità: massima flessibilità e possibilità di aumentare le performance, il numero di utenti, di creare nuovi tipi di protocollo, di utilizzare nuove reti radio.

A better radio network: 3° generation cellular networks



La rete interna oggi è tutta IP. HLR, VLR... si usano fino al 3G. dal 4G in poi diventa tutto IP. Spesso capita che non si è raggiungibili, perché il meccanismo non è così perfetto e a volte la rete non mi trova. L'assenza totale di circuito per ora non è del tutto stupenda. La transizione è lenta. Ci sono operatori furbi che fanno lo switching fold back, ovvero: devi navigare? Usi il 4g. Devi chiamare? Torni 3G. che brutto!

XX.0 LOCALIZZAZIONE

La localizzazione comprende 4 macro categorie di strumenti:

- **Rete radiomobile:** Ci permette con delle soluzioni di conoscere la nostra posizione in modo più o meno preciso
- **Hotspot wifi:** se ho un meccanismo che permette di mappare gli ssid (il **service set identifier**, o **SSID**, è il nome con cui una rete Wi-Fi o in generale una WLAN si identifica ai suoi utenti) degli hotspot wifi su un riferimento geografico affidabile, posso usare i nomi per determinare la posizione della persona.
- **Qr code- rfid-ibeacon (bluetooth low power energy):** sapere dove si trova una persona. Queste soluzioni vanno bene per soluzioni ben definite (dove mi trovo n un negozio, attività di marketing; non vanno bene per sapere dove mi trovo in un deserto).
- **GPS:** Localizzazione satellitare. I sistemi che possiamo utilizzare sono GPS, GLONASS (Sistema russo), Galileo (Europeo); il problema dei sistemi satellitari è l'indoor. Il segnale satellitare che arriva negli edifici è infimo. Per avere un segnale di localizzazione sulla superficie terrestre devo ricevere il segnale da tre satelliti. Se voglio la quota devo avere il 4° satellite.

I satelliti che si utilizzano sono quelli a media orbita. Queste tecnologie sono pervasive, sono sufficientemente precise, e coprono il mondo.

LOCALIZZAZIONE TRAMITE RETE RADIOMOBILE

Con la localizzazione tramite rete radiomobile, utilizzo il **cid** (cell identification).

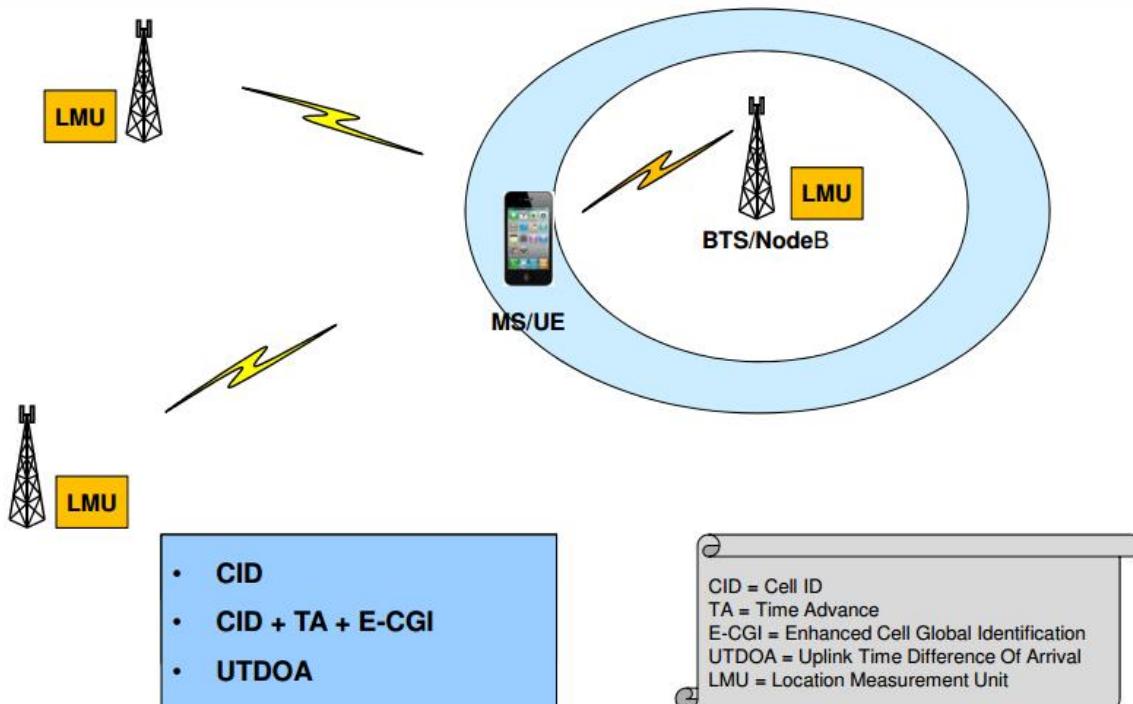
Ho una precisione dell'ordine di qualche centinaio di metri. Posso migliorare utilizzando due altri concetti. Quando sono su una rete radiomobile posso utilizzare:

- Identificativo cella
- Potenza segnale
- tempo o ritardo

Utilizzo **cid + ta (time advance)**, misura della distanza in tempo che impiega il segnale per andare dalla mobile station alla base station); il time advance serve a sincronizzare l'arrivo delle trame sui terminali. La precisione con cui c'è un time advance dipende dal bit rate del segnale. Le misure di potenza fanno pena: la potenza del segnale misurata subisce variazioni se ci sono anche degli ostacoli nel raggio d'azione. I telefoni non ricevono un solo segnale; ricevono il segnale anche da altre celle e quindi si può fare un'operazione di triangolazione. La cella a cui sono agganciato effettivamente è la cella primaria. Sono una serie di stime che faccio basandomi su quello che riceve il terminale.



Mobile_network-based location



NFC

Molti smartphone hanno la tecnologia **NFC (Near Field Communication)**. È una tecnologia che fornisce connettività wireless bidirezionale a corto raggio (fino a un massimo di 10 cm); permette

una comunicazione bidirezionale: quando due apparecchi NFC (lo *initiator* e il *target*) vengono accostati entro un raggio di 4 cm, viene creata una rete *peer-to-peer* tra i due ed entrambi possono inviare e ricevere informazioni. È una tecnologia RFID, più evoluta dell'RFID semplice. Nell'NFC, abbiamo una definizione di protocolli più complessa e una sicurezza maggiore. Il cellulare deve avere:

- **un'antenna**
- **Controller dell'nfc**
- **Secure element**: è fisicamente sicuro. È un'area di memoria dove possono essere memorizzate credenziali di sicurezza non accessibili dell'utente. È accessibile solo tramite primitive ben precise. Esso ha anche delle caratteristiche, che a seconda del tipo di utente, può avere una gerarchia di privilegi. Esso potrebbe essere parte dell'hardware del telefono, nella sim/usim, dentro Secure Digital card.

Cosa ci posso fare? L'NFC mi permette di fare molte cose. Posso avere 3-4 modi di funzionamento:

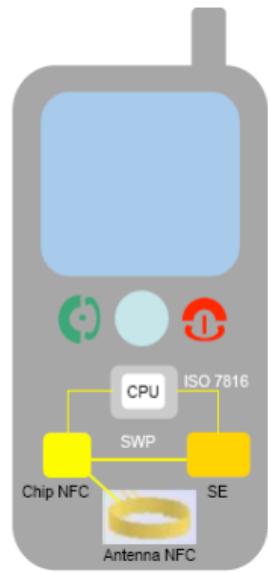
- **posso usare il mio cellulare per leggere dei tag**
- **proximity payments**:
- **trasferimento diretto di dati**
- **pairing: trasferire pass keys del bluetooth**

4G LTE

La **LTE (Long term evolution)**: è di radicale semplificazione. È scomparsa la rete a circuito. Finalmente il mondo che era partito con il gprs e gsm, si evolve sul mondo puramente a pacchetto. L'architettura di rete LTE, si traduce in una architettura molto semplificata. LTE ha un'architettura di rete semplificata rispetto a quella UMTS. La rete di accesso è costituita da un unico elemento, l'**evolved NodeB (eNodeB)**, che gestisce tutte le operazioni relative alla trasmissione dei segnali sul canale radio:

- gestione algoritmi controllo potenza;
- attivazione handover che venivano fatti dal controllore prima.

Gli eNodeB sono connessi tra loro tramite le interfacce dedicate e ogni eNodeB è poi connesso alla core network attraverso un'interfaccia specifica. In LTE tutti i dati, anche quelli voce, viaggiano su protocolli a pacchetto. L'eNodeB svolge tutte quelle operazioni che in UMTS prevedevano la collaborazione tra NodeB e RNC (Radio Network Controller). Si occupa quindi di modulazione/demodulazione, misure di qualità sul canale radio, controllo di potenza, ma anche di gestione della chiamata, controllo del carico di cella, e gestione delle procedure di handover. La struttura semplificata della rete di accesso LTE riduce l'interazione tra gli strati della pila



RFID/NFC tag reading



Tag emulation



Peering



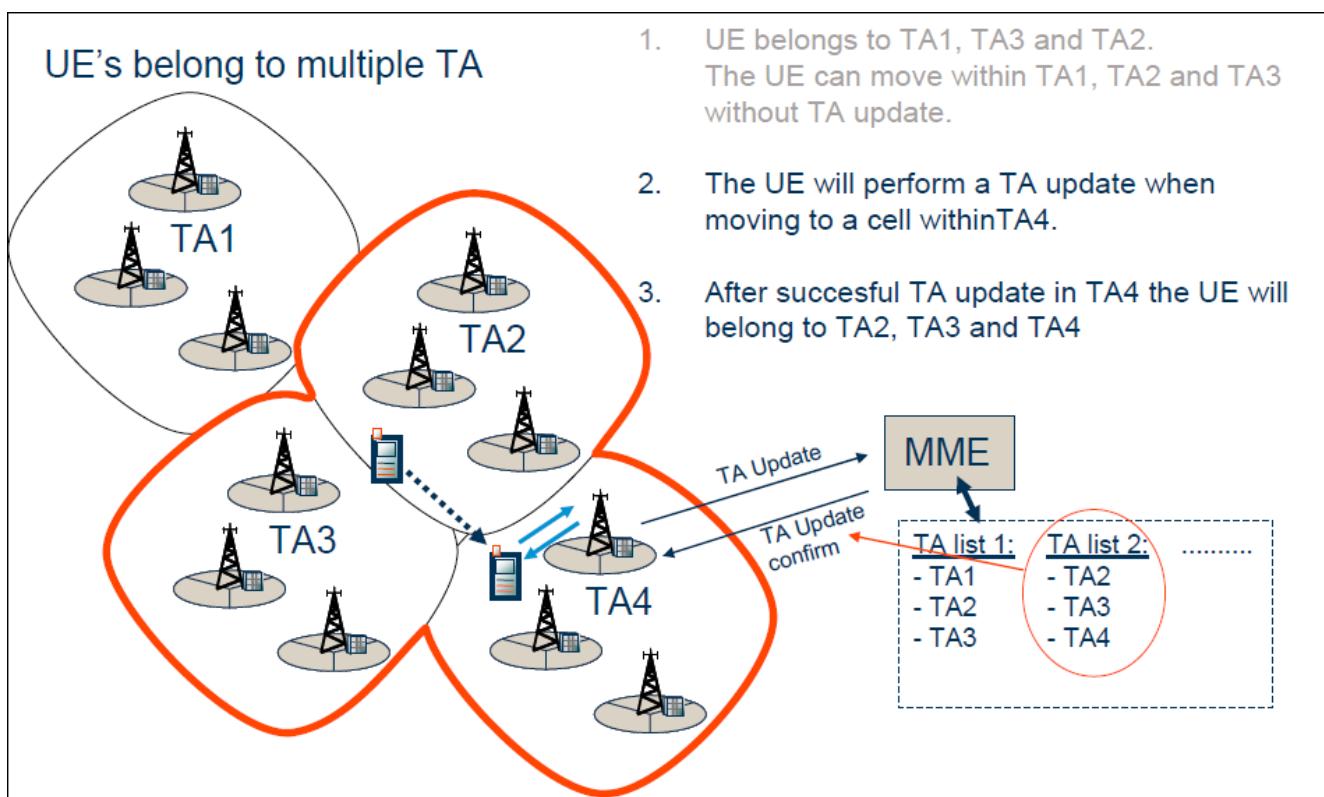
Pairing

protocollare, diminuendo la latenza e la quantità di dati di segnalazione. La rete è pensata con un'architettura più schiacciata.

I principali nodi logici che costituiscono la Core Network sono:

- Home Subscriber Server (HSS). Si tratta di un database di tutte le informazioni utili per gestire un utente mobile. L'HSS include anche l'Authentication Center (AuC) che si occupa di generare le chiavi per la cifratura dei dati e per la mutua autenticazione dell'utente e della rete;
- Serving Gateway (S-GW). Si tratta del nodo d'interfaccia con la rete di accesso E-UTRAN e con le altre reti 3GPP (i.e. UMTS/GPRS). Si occupa della gestione della mobilità di un terminale mobile che si sposta da un eNodeB a un altro;
- Mobility Management Entity (MME). È il principale nodo di controllo della core network. Gestisce la segnalazione tra UE e CN e si occupa delle procedure d'instaurazione della connessione per un terminale che si connette per la prima volta alla rete. L'MME è l'evoluzione del vecchio location register. La **Mobility Management Entity** è quella roba che sa dove si trova il terminale

La tracking area è quel gruppo di celle dove si trova il terminale. Non c'è un livello di aggiornamento continuo. Mi aggiorno quando cambio la tracking area, questo per ridurre il traffico di aggiornamento dei dati della tracking area. Esempio: mi autentico alla rete e assegno un indirizzo ip al terminale e gli rimane fino a quando non viene spento io terminale o esce dall'area di copertura. Quando mi sposto devo comunicare, mi sposto da gruppo di celle a gruppo di celle, viene fatto un aggiornamento simile a quello delle reti di 2° generazione. La tracking area può chiedere la nuova autenticazione, quando il dispositivo entra.



CONCLUSIONI

Il terminale diventa un insieme di funzioni. Gli insiemi di funzioni sono quelli dei vecchi telefoni, ma anche la funzione pagamenti, accedere a una serie di spazi con il telefono come chiave di accesso. Lo smartphone può essere l'hub che raccoglie i dati da altri dispositivi come sensori. Si parla di internet of things e machine to machine: Lo smartphone può raccogliere dati da sensori esterni a lui o interni a lui.