Servizio di TLC: insieme di procedure che rendono possibile trasportare ed utilizzare a distanza informazioni (suddivise in unità informative dette IU).

Rete di TLC: insieme degli apparati e dispositivi che intervengono nel trasporto di informazioni.

Le caratteristiche di una TLC sono:

* Tipologia di informazioni: voce, video, dati
* Configurazione: punto-punto, multipunto e broadcast
* Direzione:
  + Servizio unidirezionale: unico flusso informativo dalla sorgente all’utilizzatore
  + Servizio bidirezionale: due flussi informativi per ogni utente, si divide in:
    - Simmetrico: i due flussi hanno le stesse proprietà
    - Asimmetrico: non è simmetrico
* Inizializzazione:
  + Su base di chiamata: richiesta di servizio → utilizzo → rilascio
  + Su base contrattuale: la disponibilità del servizio è (semi) permanente, ad esempio un contratto con Vodafone, ….

I servizi di TLC si dividono in:

* Interattivi: consentono un’interazione tra sorgente e destinazione, ad esempio:
  + Conversazione: l’interazione avviene in tempo reale
  + Messaggistica: l’interazione avviene in tempo differito
  + Consultazione: consentono il reperimento di informazioni presso un centro di servizio tramite opportune procedure di consultazione
* Distributivi: la sorgente di informazione agisce indipendentemente dal comportamento della destinazione, si classificano in:
  + Senza controllo di presentazione
  + Con controllo di presentazione

I requisiti dei servizi di TLC (QoS) sono:

* Probabilità di blocco: probabilità che il servizio richiesto sia rifiutato
* Ritardo: tempo che la rete impiega a trasportare le unità informative
  + Jitter: per segnali audiovisivi, il ritardo tra due segnali monomediali che compongono un segnale multimediale
* Velocità media: frequenza di cifra media con cui la rete trasporta le informazioni
* Probabilità di perdita/errore: parte dei bit che la rete non è stata in grado di trasportare o che ha consegnato al destinatario con errore

Una rete di TLC può essere rappresentata mediante un grafo costituito da nodi e rami

* Nodo: punto in cui vengono smistate le unità informative (IU) verso la destinazione
* Ramo: sistema trasmissivo che consente il trasporto delle IU da nodo a nodo, può essere:
  + Simplex (unidirezionale): posso trasmettere dal nodo A al nodo B ma non viceversa
  + Half-duplex (bidirezionale alternato): posso trasmettere dal nodo A al nodo B e viceversa ma quando trasmette un nodo l’altro non può trasmettere le IU
  + Full-duplex (bidirezionale contemporaneo): posso trasmettere dal nodo A al nodo B e viceversa ed entrambi i nodi possono trasmettere contemporaneamente le IU

Tipologie di uso comune nelle reti di TLC sono a Bus, ad Anello, a Stella e a Maglia.

La tassonomia delle reti si divide in base all’ampiezza:

* Reti in area locale (LAN, Local Area Network)
* Reti in area metropolitana (MAN, Metropolitan Area Network)
* Reti in area geografica (WAN, Wide Area Network)

Per trasferire delle informazioni esistono vai metodi:

* Tecnica di multiplazione: descrive come la banda disponibile su uno specifico canale di comunicazione possa essere condivisa tra le diverse IU che lo devono attraversare, alcune tecniche di multiplazione sono:
  + Frequency Division Multiplexing (FDM)
  + Time Division Multiplexing (TDM)
  + Wavelength Division Multiplexing (WDM)
  + Code Division Multiplexing (CDM)
* Modalità di commutazione: specifica come le IU ricevute da un generico nodo sui suoi canali entranti siano trasferite attraverso il nodo sui canali uscenti
* Architettura di protocolli: descrive le regole (o protocolli) secondo cui due nodi di rete possono scambiare informazioni.

Differenza tra commutazione di circuito e commutazione di pacchetto:

* Commutazione di circuito:
  + il servizio (chiamata) si articola in 3 fasi:
    - Instaurazione
    - Dati
    - Svincolo

Riservo in modo esclusivo le risorse → trasmetto le informazioni → rilascio le risorse. Tutte le informazioni seguono lo stesso percorso (gli stessi link) e arrivano nello stesso ordine con il quale sono stati mandati.

* + La banda richiesta per il trasporto delle IU viene riservata in modo esclusivo durante la fase di instaurazione
  + Svantaggi: Utilizzo inefficiente delle risorse in presenza di sorgenti a rate fortemente variabile (bursty)
  + Svantaggi: non sono necessari meccanismi di bufferizzazione presso i nodi di comunicazione (ritardi di accodamento nulli)
* Commutazione di pacchetto:
  + La banda richiesta per il trasporto delle IU non viene riservata in modo esclusivo

Non alloco e non rilascio risorse, prendo le IU, le inserisco in vari pacchetti, indico il mittente e il destinatario (header del pacchetto), questi pacchetti viaggeranno separatamente su più canali e arriveranno in ordine casuale

* + La banda globalmente prenotata su un canale può essere superiore alla capacità del canale
  + Elevata utilizzazione delle risorse
  + Paradigma Store & Forward (ritardi di accodamento non nulli)
  + Due servizi previsti:
    - A circuito virtuale: le IU vengono divise e inserite in vari pacchetti con mittente e destinatario e seguiranno uno stesso percorso ma in ordine sparso
    - A Datagramma

I servizi possono essere di due tipi:

* Con connessione (connection-oriented) dove:
  + Il servizio è offerto attraverso 3 fasi:
    - Apertura della connessione tra due punti della rete
    - Utilizzo della connessione per inviare i dati
    - Chiusura della connessione
  + I dati inviati seguono la politica FIFO (First Input First Output)
* Senza connessione (connection-less) dove:
  + Non c’è alcuna connessione
  + I dati sono impacchettati in messaggi, ognuno dei quali contiene l’indirizzo completo del destinatario
  + Non segue la politica FIFO

L’ordine di consegna dei dati è garantito solo dai servizi con connessione. Per garantire la ricezione di un messaggio: il ricevitore manda un ack (ricevuta) per ogni messaggio, questi ack sono utilizzati sia dai servizi connection-oriented sia connection-less. Il problema delle ack è che introducono un ritardo non sempre accettabile.

MODELLO ISO/OSI

I protocolli di comunicazione regolano lo scambio di protocolli tra sistemi e tra i protocolli è possibile stabilire una gerarchia (Architettura di Protocolli). Le conversazioni e le regole usate nelle comunicazioni di uno stesso livello tra due macchine sono dette protocollo.

Un insieme di protocolli, uno per livello, è detto pila di protocolli.

Un insieme di livelli, protocolli e interfacce è chiamato architettura di rete.

Un protocollo definisce le regole semantiche e sintattiche per la trasmissione di un’informazione tra unità paritetiche

Nel modello ISO-OSI si raggruppano tra loro funzioni simili per logica e/o tecnologia in modo da definire gruppi omogenei. I livelli comunicano tramite interfacce

Il modello ISO-OSI è diviso in 7 livelli: Application, Presentation, Session, Transport, Network, Data Link, Phisical

Nel modello ISO-OSI si raggruppano tra loro funzioni simili per logica e/o tecnologia in modo da definire gruppi omogenei (raggruppamento), questi gruppi si organizzano gerarchicamente in gruppi (strati o livelli) in modo da identificare regole di interazione inter-stato (interfacce) semplici e univoche. Ogni strato si interfaccia con lo strato immediatamente superiore e con quello immediatamente inferiore. L’interazione tra due sistemi avviene mediante interlavoro di entità omogenee sui due sistemi (entità pari).

Ogni strato usufruisce dei servizi dello stato inferiore, presso opportuni Service Access Point (SAP). Salendo al livello superiore si decapsula l’informazione mentre scendendo al livello inferiore si incapsula l’informazione. Le Protocol Control Information (PCI) conterranno le informazioni necessarie al corretto riassemblaggio delle Protocol Data Unit (PDU) ricevute presso l’entità di livello N-1.

Ci sono 5 sistemi di relaying:

* Repeater: opera al livello 1
* Switch: opera al livello 2
* Bridge: opera al livello 2
* Router: opera al livello 3
* Gateway: opera al livello 4

Application Level: fornisce l’interfaccia utente per l’accesso a servizi informatici distribuiti (Es. Posta elettronica, terminale virtuale, WWW, …). I servizi di questo livello sono legati alle applicazioni:

* Quali dati trasmettere
* Quando trasmettere
* Dove trasmettere e a chi
* Significato di bits/bytes

Presentation Level: consente l’interlavoro tra applicazioni che rappresentano i dati utilizzando formati diversi, le sue funzioni consistono nelle operazioni di trasformazione, formattazione e modifica della sintassi dei dati utilizzati. La sintassi con cui può avvenire lo scambio dei dati può essere quella di uno dei due sistemi interagenti, oppure una sintassi intermedia di trasferimento (Es. Compressione dei dati, traduzione dei codici utilizzati per rappresentare i dati, transcodifica a scopi di sicurezza (encryption)). Le funzionalità di questo livello si limitano alla traduzione dei dati che viaggiano sulla rete in formati astratti

Session Level: gestisce il dialogo e lo scambio dati tra entità di presentazione, questo tipo di funzioni sono necessarie quando le applicazioni usano diversi metodi di trasferimento delle informazioni, oppure quando occorre partizionare in sequenze più brevi un lungo scambio di informazioni. Alcuni servizi offerti da questo livello sono:

* Gestione Modalità Dialogo: ad esempio un terminale half-duplex interlavora con un’applicazione che opera in full-duplex
* Recupero del dialogo seguente ad un’interruzione del servizio di trasporto

Questo livello controlla il dialogo tra le due macchine, gestisce il controllo dei token e gestisce la sincronizzazione nel trasferimento dei dati (Es. Checkpoint).

Transport Level: svolge diversi compiti:

* Multiplazione: trasporto di diverse connessioni di trasporto utilizzando il medesimo servizio offerto dal livello di rete
* Demultiplazione
* Indirizzamento delle unità dati (indirizzo di porta)
* Segmentazione e Riassemblaggio delle unità dati
* Controllo del flusso e2e
* Controllo degli errori e2e
* Gestione QoS ed e2e

Il livello di trasporto è il primo livello “end-to-end”, deve eventualmente sopperire alla mancanza di affidabilità del livello di rete (pacchetti persi, duplicati, invertiti, …). Questo livello accetta i dati dal livello superiore, li spezza in parti più piccole e le trasmette, assicurando un servizio privo di errori e l’ordine corretto di ricomposizione (connection-oriented), effettua il controllo di flusso e2e, fornisce il servizio di recapito dei messaggi senza garanzia (connection-less) e gestisce la diffusione di messaggi a più destinazioni (multicast)

Network Level: sovraintende al trasferimento di informazioni lungo una sequenza di nodi attraverso la rete e maschera al livello di trasporto la tecnica di commutazione utilizzata. Le principali funzioni sono:

* Instradamento
* Interlavoro tra porzioni eterogenee di rete
* Controllo di flusso per prevenire la congestione
* Multiplazione di più connessioni di rete su un unico collegamento dati

Questo livello controlla il cammino ed il flusso di pacchetti (algoritmi di routing), gestisce la congestione della rete, gestisce l’account dei pacchetti sulle reti a pagamento ed implementa l’interfaccia necessaria alla comunicazione tra reti di tipo diverso (internetworking)

Data-Link Level: svolge la funzione di trasferimento dati privo di errori tra due nodi adiacenti lungo un collegamento trasmissivo. Le sue funzionalità sono:

* Rivelazione di errori
* Recupero delle frame perse
* Controllo di flusso
* Controllo di accesso al collegamento

Questo livello trasforma la linea fisica in una linea in cui gli errori di trasmissione vengono sempre segnalati, divide le informazioni in pacchetti e li trasmette attraverso il mezzo fisico, attendendo un segnale di avvenuta ricezione (ack), gestisce l’eventuale duplicazione delle frame ricevute causata dalla perdita dell’ack, sincronizza un mittente veloce con un ricevitore lento (controllo di flusso), gestisce l’accesso al canale di trasmissione condiviso

Physical Level: svolge tutte le funzioni necessarie a interfacciare il sistema con il mezzo fisico:

* Gestione topologia
* Gestione delle procedure di trasmissione
* Codifica dei bit mediante segnali elettrici/ottici

Questo livello riguarda la trasmissione dei bit sul canale fisico di trasmissione, coinvolge aspetti di tipo:

* Elettrico (linee di comunicazione, …)
* Comunicazione (simplex, half-duplex, full-duplex, …)
* Meccanico (standard dei connettori, …)

Nella pila TCP-IP è formata da solo 4 livelli: Application Level, Transport Level, Network Level e Network Access. È un modello a strati di riferimento per internet, prende il nome da due dei suoi protocolli più importanti:

* Transmission Control Protocol (TCP)
* Internet Protocol (IP)

Nel livello di rete contiene l’IP Internet Protocol, avviene uno scambio di datagrammi senza garanzia di consegna

Nel livello di trasporto contiene il TCP Transmission Control Protocol, in questo livello avviene un flusso di byte bidirezionale lungo un canale virtuale, vengono ordinati i dati, non vengono duplicati i dati, avviene il controllo di flusso ed il controllo degli errori. Un altro protocollo utilizzato nel livello di trasporto è l’UDP User Datagram Protocol, lo scambio di messaggi è inaffidabile, è senza connessione e senza ordine.

I vantaggi del TCP/IP sull’OSI sono 2:

* Quando nacque OSI il TCP/IP era già presente nel mondo accademico
* Lo stack TCP/IP è più semplice dello stack OSI

Il TCP/IP parte dai protocolli mentre l’OSI parte dai livelli. Il modello TCP/IP originale non aveva una chiara distinzione tra Servizi, Interfacce e Protocolli. I limiti del TCP sono:

* Non è generale
* Non distingue tra livelli, interfacce e protocolli
* Il livello Host-to-Network non è un livello
* Non sono definiti i livelli Fisico e Data Link

Nel dettaglio i livelli del TCP/IP:

* Application Level: incorpora tutte le funzioni del livello dell’ISO/OSI e dove necessario provvederà a fornire servizi tipici dei livelli di Sessione e Presentazione
* Transport Level: è formato da:
  + User Datagram Protocol (UDP): fornisce un servizio inaffidabile e connection-less, la sua unica funzione è quella del multiplexing
  + Transmission Control Protocol (TCP): fornisce un servizio affidabile e orientato alla connessione, le sue funzioni sono:
    - Controllo del flusso e2e
    - Controllo di congestione e2e
    - Ritrasmissione di SDU perse o corrotte
    - Consegna nella corretta sequenza delle unità dati
* Network Level: è formato da:
  + Internet Protocol (IP): offre un servizio non affidabile e connection-less, le sue funzioni sono:
    - Instradamento
    - Internet-working
  + Internet Control Message Protocol (ICMP): consente lo scambio di informazioni di servizio tra nodi della rete
* Network Access Layer: il livello TCP/IP non pone alcun vincolo e racchiude tutte le funzionalità specifiche della tecnologia usata per il trasporto delle PDU dell’IP

Nell’OSI il Data-Link gestiva la comunicazione tra due nodi direttamente connessi tramite i mezzi forniti dal livello fisico, nel TCP/IP all’interno del Network Access Layer sono presenti diversi protocolli, uno è l’IEEE 802 (gestione reti LAN), questo protocollo è formato da un Logical Link Control (LLC) e da un Medium Access Control (MAC), il MAC definisce le regole di accesso al mezzo fisico e cambia a seconda del mezzo fisico impiegato, LLC fornisce un’interfaccia verso il livello di rete e non cambia a seconda del mezzo fisico impiegato.

A seconda delle implementazioni LLC può fornire al livello superiore 3 diverse modalità di servizio:

* Tipo 1 (Logical Data Link): è un servizio inaffidabile e connection-less, costituito da diversi datagrammi che vengono trasmessi in modo indipendente l’uno dall’altro senza richiesta di alcuna comunicazione. Può essere unicast, multicast o broadcast però non è garantita la consegna dei singoli elementi e neanche l’ordine di consegna, non è prevista nessuna forma di correzione degli errori né di controllo di flusso (se necessari verranno forniti dai protocolli di livello superiore)
* Tipo 2 (Data Link Connection): è un servizio affidabile e connection-oriented, richiede l’apertura di un canale di comunicazione tra una sorgente e una destinazione (unicast o punto-punto) per lo scambio di dati. Sono presenti meccanismi di correzione degli errori e di sequenziamento che garantiscono la consegna dei dati inviati nella sequenza di trasmissione, è simmetrica (entrambi gli interlocutori sono responsabili di ciò che trasmettono)
* Tipo 3: è una modalità di servizio Logical Data Link alternativa, pur essendo connection-less prevede una conferma di ricezione (acknowledge) per i datagrammi inviati e garantisce la consegna ordinaria dei dati trasmessi.

La PDU del livello LLC è formata nel seguente modo:

|  |  |  |  |
| --- | --- | --- | --- |
| Destination Address | Source Address | Control | Information |
| 1 Byte | 1 Byte | 1/2 Byte | Variabile (max 1497) |

Gli indirizzi di LLC (LLC-SAP) specificano i livelli di rete mittente e destinatario mentre il Control specifica il tipo di frame che gestisce i meccanismi di numerazione e riscontro. Es. Layer 3 = IP → AA:AA:03:00:00:00:08:00

L’accesso multiplo al mezzo condiviso può essere:

* Accesso ordinato
* Accesso casuale: a sua volta si divide in:
  + Senza rivelazione del canale
  + Con rivelazione del canale: a sua volta può essere:
    - Senza rilevazione di collisioni
    - Con rilevazione di collisioni

Lo standard IEEE 802.3 è l’evoluzione dello standard Ethernet II e definisce una rete LAN con topologia logica a BUS cablata con cavo coassiale. Il Bus è un mezzo condiviso da più stazioni, l’informazione trasmessa da una stazione è ascoltata da tutte le rimanenti stazioni. Se più stazioni trasmettono contemporaneamente si genera una collisione → l’informazione trasmessa viene persa. Lo standard IEEE 802.3 adotta il protocollo CSMA/CD (Carrier Sense Multiple Access/Collision Detection) per la dell’accesso multiplo. Lavora in questo modo:

1. Canale inattivo? → inizio la trasmissione delle frame
2. Canale occupato? → attendo fino alla rivelazione di canale inattivo → inizio la trasmissione
3. Listen while talking → nessuno trasmette
4. Non c’è collisione? (nessun segnale generato da altre STA rilevato durante la trasmissione) → Frame correttamente spedita, trasmissione arrestata
5. Collisione? → trasmissione del frame arrestata → trasmissione della sequenza di jam (48 bit) → Exponential Backoff
6. Exponential Backoff → attesa di un tempo casuale estratto dall’intervallo TSlot\*[0, 2m-1], m = min(n, 10), n = numero di collisioni consecutive, TSlot = tempo necessario alla trasmissione di una frame a minima lunghezza (512 bit)

La frame 802.3 è formata da:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| MAC | Preambolo | SFD | MAC DA | MAC SA | Lunghezza | Dati | Padding | FCS |
| Byte | 7 | 1 | 6 | 6 | 2 | 0-1500 | 0-46 | 4 |

* Il preambolo è una sequenza di bit utile a sincronizzare trasmettitore e ricevitore
* La SDF (Starting Frame Delimeter) indica l’inizio della frame
* Il MAC DA è il MAC del destinatario (12 cifre esadecimali) le prime 6 sono l’identificativo dell’azienda (Organization Unit Identifier (OUI)) e le ultime 6 sono il numero di scheda di rete
* Il MAC SA è il MAC del mittente
* La lunghezza è la lunghezza del campo in byte
* I dati sono la SDU
* Il padding garantisce la lunghezza minima (Lmin) della frame sia 64 byte
* FCS è la frame Check Sequence e consente la rivelazione dell’errore

I mezzi trasmissivi possono essere i cavi coassiali, i doppini o le fibre ottiche.

La IEEE 802.5 è detta Token Ring, ha una topologia logica ad anello e il diritto ad accedere al mezzo è acquisito mediante un gettone (token) che garantisce l’accesso multiplo ordinato. Funziona nel seguente modo:

1. Cattura del token
2. Man mano che la frame percorre l’anello le stazioni leggono il MAC del destinatario, riportato nell’header per capire se passarlo al livello di rete
3. Le frame trasmesse sono ritrasmesse da ogni stazione e rimosse dall’anello della sorgente
4. Il token non può essere trattenuto oltre il tempo massimo dalla medesima stazione per evitare di monopolizzare il canale

La frame IEEE 802.5 è formato in questo modo:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SD | AC | FC | DA | SA | Dati | FCS | ED | FS |
| 1 | 1 | 1 | 6 | 6 |  | 4 | 1 | 1 |

* SD: Starting Delimeter
* AC: Access Control (indica se segue una frame o un token)
* FC: Frame Control (distingue frame dati da frame di gestione)
* ED: Ending Delimeter
* FS: Frame Status (contiene segnali della stazione destinataria)

Le reti wireless sono reti in cui i terminali accedono alla rete mediante canali “senza fili”.

Le reti radiomobili sono reti wireless dove i terminali utenti possono spostarsi sul territorio senza perdere la connettività.

Le reti cellulari sono reti radiomobili la cui copertura geografica è ottenuta con una tassellatura di aree adiacenti e/o sovrapposte dette celle.

Le wireless LAN (WLAN) sono reti wireless che forniscono coperture e servizi tipici di una LAN.

Rete wireless e rete mobile non sono sinonimi, una rete wireless non può essere una rete mobile. Le reti wireless si dividono in PAN, LAN, MAN e WAN. La trasmissione e la ricezione sono realizzate mediante un’antenna (conduttore elettrico), in una trasmissione bidirezionale una stessa antenna funge da trasmettitore e da ricevitore.

Le antenne isotropiche o omnidirezionali sono quelle ideali perché irradiano la stessa potenza in tutte le direzioni. Il guadagno di un’antenna è la potenza di uscita in una particolare direzione comparata a quella prodotta in qualunque altra direzione da un’antenna isotropica. Le antenne direttive emettono potenza in una particolare direzione e ricevono un segnale più forte.

Il decibel (dB) è l’unità di misura logaritmica di intensità usata per indicare la perdita o il guadagno di potenza tra due segnali:

I dBm sono un valore assoluto riferito alla potenza di 1mW, le sue proprietà sono:

* P1\*P2 (dBm) = P1(dBm) + P2(dBm)
* P1/P2 (dBm) = P1(dBm) – P2(dBm)

Il range di copertura di un’antenna si calcola mediante la formula:

Dove:

* Prx è la potenza in ricezione (valore minimo -70 dBm)
* Ptx è la potenza in trasmissione per classe (20 dBm)
* λ è la lunghezza d’onda sulla banda ISM, la formula è dove C è la velocità della luce (3 \* 108) ed F è la frequenza espressa in s-1
* Grx e Gtx sono i guadagni di un’antenna
* R è l’area di copertura dell’antenna

A0 = è l’attenuazione isotropica nello spazio libero dipende dalla distanza del collegamento e dalla lunghezza d’onda.

I problemi del LAN Wireless sono l’inaffidabilità del mezzo trasmissivo in quanto range e velocità di trasmissione sono influenzate da interferenze elettromagnetiche, multipath fading di ricezione (sovrapposizione del segnale trasmesso e delle sue riflessioni dovute a pareti ed oggetti metallici), sicurezza (libero accesso al mezzo condiviso)

Il WLAN/802.11 è progettato per trasmettere utilizzando 3 tecniche:

* Frequency hopping
* Direct sequence
* Diffused infrared

Le prime due tecniche sfruttano il range di frequenza intorno ai 2,4 GHz e sono tecniche del tipo spread spectrum.

Direct Sequence: ci sono 11 canali da 22 MHz, 3 canali non sovrapposti → codifica del bit in una stringa di bit (chipping sequence) → trasmissione delle chipping sequence su un range di frequenze → cambio di frequenza in caso di interferenza

Ogni bit della frame è rappresentato da molteplici bit nel segnale trasmesso, il mittente invia il risultato dell’OR esclusivo di tale bit e di n bit scelti in maniera pseudo-casuale nota sia al mittente sia al destinatario.

Frequency Hopping: 79 canali ampi 1 MHz → cambio di frequenza (hop) ogni 0.4 secondi, richiede sincronizzazione, ha una ridotta sensibilità alle interferenze e se un pacchetto viene perso viene ritrasmesso al hop successivo

Il segnale è trasmesso su una sequenza “random” di frequenze (tramite algoritmo), il ricevitore utilizza il medesimo algoritmo inizializzando lo stesso seme, così è in grado di saltare le frequenze in maniera sincronizzata con il mittente, per ricevere correttamente le frame.

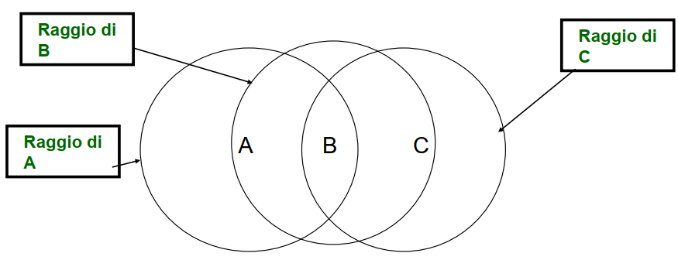
Per fornire il supporto alla mobilità e la connessione ad altre reti si utilizzano dei nodi speciali detti Access Point (AP), sono dei nodi connessi ad un’infrastruttura di rete fissa chiamata Distribution System, ogni nodo si associa ad un particolare AP (Es. se A vuole comunicare con F: A invia una frame al suo AP → AP1 inoltra ad AP3 la frame attraverso il Distribution System → AP3 trasmette la frame ad F).

La tecnica per selezionare un AP è detta scanning e prevede 4 fasi:

1. Il nodo invia una frame di probe
2. Tutti gli APs alla risposta del nodo rispondono con una frame di risposta al probe
3. Il nodo seleziona uno degli APs (solitamente quello con la miglior qualità del segnale), e gli invia una frame di richiesta di associazione
4. L’AP selezionato risponde con una frame di conferma di associazione

Il protocollo è utilizzato quando il nodo si unisce alla rete e quando il nodo diventa “scontento” dell’attuale AP utilizzato (questo può avvenire perché il segnale ricevuto da quel AP risulta indebolito.

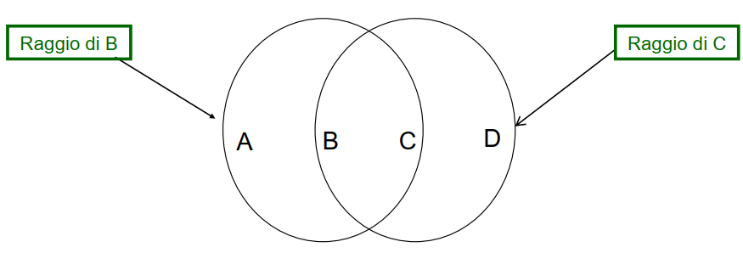
Il metodo di accesso è simile ad Ethernet: prima di trasmettere si attende finché il canale diventa libero, in caso di collisione → Binary Exponential Backoff, bisogna però tenere in considerazione che non tutti i nodi sono sempre alla portata l’uno dall’altro. Questo comporta a 2 problemi: problema del nodo nascosto (Hidden Node Problem) e problema del nodo sovraesposto (Exposed Node Problem)

Hidden Node Problem:

Le trasmissioni di A non sono ascoltate da C

A e C possono inviare simultaneamente verso B causando una collisione in ricezione

Né A né C sono in grado di rilevare la collisione

Exposed Node Problem:

B invia dati ad A

C è al corrente di tale comunicazione perché ascolta le trasmissioni di B:

* È un errore per C concludere di non poter trasmettere a nessuno
* C potrebbe inviare una frame a D senza interferire con B

Lo standard IEEE 802.11 risolve i due problemi introducendo l’algoritmo chiamato CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), prima di inviare i dati il mittente trasmette una frame di richiesta di trasmissione Request to Send (RTS), in questa frame è presente anche un campo che indica la lunghezza della frame dati da trasmettere, il ricevitore risponde con una frame di permesso di trasmissione Clear to Send (CTS), in questa frame viene replicato il valore relativo alla lunghezza dei dati.

Un nodo che riceve la frame CTS sa di essere vicino al ricevitore, esso non può trasmettere per tutto il tempo necessario ad inviare la frame dei dati. Un nodo che vede la frame RTS ma non il CTS non è abbastanza vicino al ricevitore per interferire con esso e quindi può trasmettere senza attendere, il ricevitore invia un ACK dopo aver ricevuto la frame. I nodi non rilevano le collisioni:

* Se due nodi inviano una frame RTS in contemporanea, queste frame collideranno
* I nodi assumono che vi sia stata una collisione se non ricevono una frame CTS di risposta

Il Bluetooth realizza un collegamento wireless a onde radio ed a corto raggio d’azione tra dispositivi fissi e portatili, i fili vengono sostituiti con una minuscola ricetrasmittente radio.

Il Bluetooth al livello RF utilizza la banda ISM (Industrial Scientific Medical), impiega la tecnica FHSS/TDD → avviene una frequenza di hopping pseudocasuale su 79 canali, ogni canale è suddiviso in time slots, dove ogni time slot corrisponde una frequenza RF di salto, lo schema TDD è usato durante la fase di trasmissione alternata master/slave.

Ogni dispositivo è diviso in 3 classi di potenza:

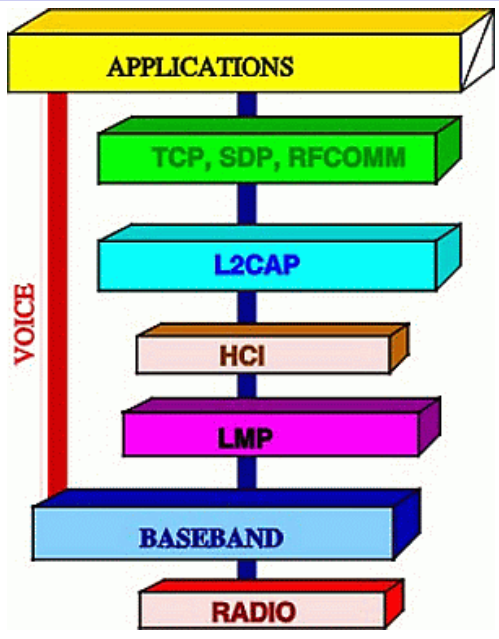
1. Classe di potenza 1: copertura 100 m e potenza d’uscita massima 20 dBm
2. Classe di potenza 2: copertura 10 m e potenza d’uscita massima 4 dBm
3. Classe di potenza 3: copertura 10 cm e potenza d’uscita massima 0 dBm

La piconet è una tecnologia che consente la creazione di piccole reti ad hoc costituite da massimo 8 dispositivi attivi simultaneamente, una piconet consiste in un master e di sette slave al massimo dove il master è l’entità centrale che gestisce l’allocazione delle risorse. Un device può funzionare sia come master sia come slave, ogni piconet ha un solo master ed ogni master in una piconet può essere uno slave in un’altra piconet.

Due o più piconet possono essere collegate creando una scatternet. In questo caso un device in ciascuna piconet (master o slave) svolgono il ruolo di bridge fra le piconet, un dispositivo può funzionare sia da master che da slave.

Il link SCO è un Point-to-Point link tra master e un singolo slave della piconet. Il master mantiene i link SCO usando slot riservati, il link SCO riserva gli slot e quindi può essere considerato una connessione circuit-switched tra master e slave.

Il link ACL è un collegamento point-to-multipoint fra il master e tutti gli slave che costituiscono una piconet, gli slot non sono riservati, il master stabilisce un link ACL anche con uno slave già impiegato in un link SCO, il link ACL realizza una connessione packet-switched fra master e tutti gli slave attivi nella piconet, i pacchetti ACL non sono indirizzati verso uno specifico slave, ma vanno considerati come pacchetti broadcast (leggibili da tutti)

La pila protocollare del Bluetooth è formata da:

* Bluetooth Radio: definisce i requisiti del device transceiver operante nella banda a 2.4 GHz
* Baseband: è un protocollo del livello Link Controller, gestisce i link ACL e SCO, crea la piconet, seleziona i salti di frequenza, corregge gli errori e gestisce il paging e inquiry
* LMP: gestisce il setup, autenticazione e configurazione dei link e altri protocolli
* HCI: fornisce un interfaccia di comando baseband controller e al link manager
* L2CAP: (Logical Link Control and Adaption Protocol): fornisce connection-oriented e connection-less data services ai livelli protocollari superiori
* RFCOMM: emula le porte seriali sul livello L2CAP
* SDP (Service Discover Protocol): fornisce uno strumento per specificare quali servizi siano attivi e determinare le caratteristiche degli stessi

Per definizione il master è l’unità Bluetooth che inizia la connessione verso più slave. Una volta che la rete piconet è stata creata i ruoli master/slave possono essere scambiati.

La connessione prevede due stati: standby e connessione, ci sono 7 sottostati: page, page scan, inquiry, inquiry scan, master response, slave response e inquiry response.

Un device che vuole scoprire altri device entra nello stato di inquiry, un device che vuole essere scoperto entra nello stato inquiry scan. Durante il sottostato di inquiry, l’unità che si trova nello stato di inquiry colleziona tutti gli indirizzi e i clock di ogni device che rispondono all’inquiry message. Il messaggio di inquiry per la sua natura broadcast non contiene alcuna informazione sulla sorgente stessa. La inquiry response è opzionale. Durante la procedura di inquiry ciascun device usa una sequenza di salto (32 frequenze dedicate) ben nota.

Nelle reti cellulari per servire un numero elevato di utenti, siccome la velocità di trasmissione è limitata dalla porzione di spettro disponibile, una soluzione è suddividere il territorio in aree (celle) ed assegnare ad ognuna di esse uno spazio dello spettro (canale di frequenza), questa suddivisione permette un riuso delle frequenze utile per minimizzare l’interferenza tra celle vicine. La struttura delle reti cellulari prevede un punto di accesso fisso (Base Station) per ogni cella ed ogni cellulare utilizza la BS della cella in cui al momento risiede.

Le reti mobili sono reti che supportano la mobilità dell’utente. Le reti mobili possono essere classificate in base al tipo di mobilità che viene supportata:

* Access Mobility: la mobilità è limitata ad un’area intorno alla stazione di accesso alla rete
* Terminal Mobility: il terminale è caratterizzato da un identificativo unico, può essere localizzato in ogni momento e può accedere alla rete mentre è in movimento
* Service Profile Portability: ogni utente è caratterizzato da un profilo che ne specifica le caratteristiche, tale profilo è indipendente dal terminale utilizzato e si sposta con l’utente anche da un Service Provider all’altro
* Personal Mobility: è l’integrazione della Terminal Mobility e Service Profile Portability

L’efficienza nelle reti cellulari viene misurata in base al riuso dei canali disponibili. Le celle vengono organizzate in cluster di N celle, più sono grossi i cluster meno efficiente è il sistema.

Una problematica dei sistemi cellulari è che la frequenza di utilizzo nei sistemi radiomobili è scarsa e gli utenti situati in celle differenti, posti ad una distanza D opportuna, possono usare la stessa frequenza di canale. Il riuso della frequenza incrementa la capacità del sistema ma può introdurre interferenza co-canale.

Se indichiamo con D la distanza di riuso fra i centri di 2 celle co-canali (distanza di riuso), e con R il raggio di ciascuna cella, il rapporto di riuso co-canale è:

Se N è il numero di celle che formano il cluster, si dimostra che:

È necessario calcolare la minima distanza che permette alla stessa frequenza di essere riutilizzata in celle differenti, la distanza può essere calcolata come:

Dove R è il raggio di copertura di ciascuna cella e N il numero di celle che costituiscono il cluster. Mantenendo R costante e aumentando il numero di celle per cluster permette di avere una distanza di riuso D elevata. Ciò diminuisce la probabilità di interferenza co-canale.

Si dimostra che il rapporto Segnale (S) / Rumore interferenze (I) è pari a:

Dove:

* α = coefficiente di propagazione (2 < α < 5)
* i0 = numero di celle interferenti (i0 = 4 per celle quadrate/tonde e i0 = 6 per celle esagonali)

Avere un numero di celle troppo elevato per cluster diminuisce però la banda assegnata a ciascuna cella e quindi il numero di utenti che possono connettersi.

Il numero minimo di celle per cluster che assicura un rapporto tra il segnale d’utente e il livello di interferenza co-canale pari a 18 dB è N = 7

La capacità totale del sistema (numero massimo di chiamate che possono essere effettuate contemporaneamente) è:

Dove:

* M = numero di cluster presenti nel sistema
* K = numero di canali per cella
* N = numero di celle per cluster

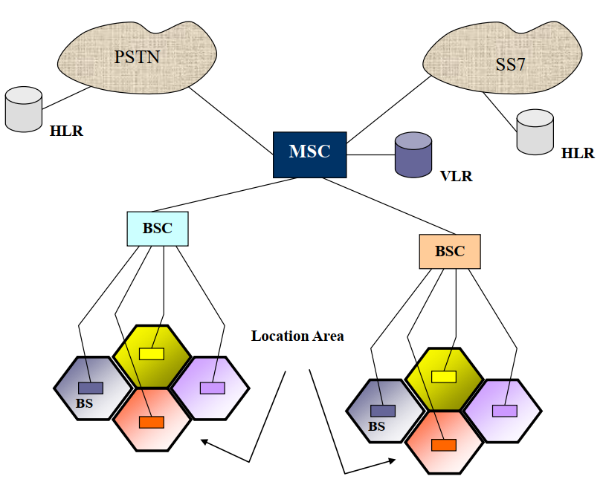
La scelta di N va fatta garantendo che le antenne che usano le stesse frequenze siano abbastanza lontane da non interferire tra loro.

I requisiti di un sistema cellulare sono:

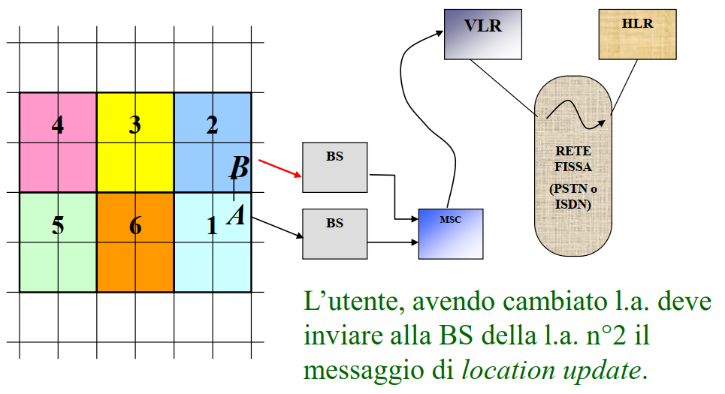
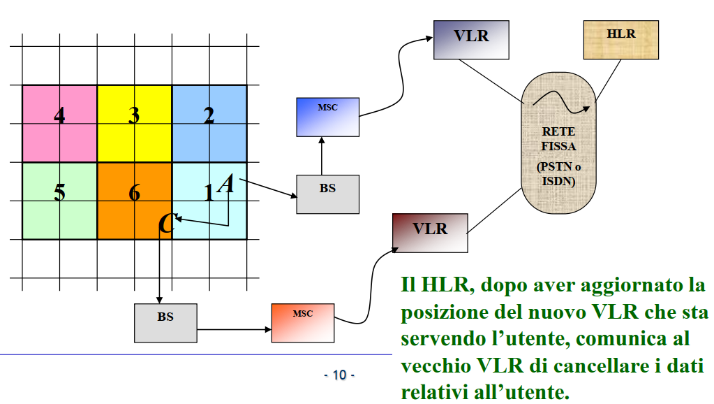
* Servire le chiamate emesse dall’utente mobile
* Inoltrare le chiamate verso l’utente mobile
* Supportare una chiamata mentre l’utente mobile si sposta da una cella all’altra (handover e handoff)
* Localizzare l’utente mobile in ogni istante, indipendentemente se sia in corso una comunicazione (Roaming)
* Terminazione della chiamata quando la qualità è sotto una certa soglia

La Location Area è un insieme di celle entro cui il terminale non deve fare alcun Location Update. Il sistema conosce la Location Area di ciascun utente ma non conosce la cella in cui ci troviamo se non abbiamo chiamate in corso.

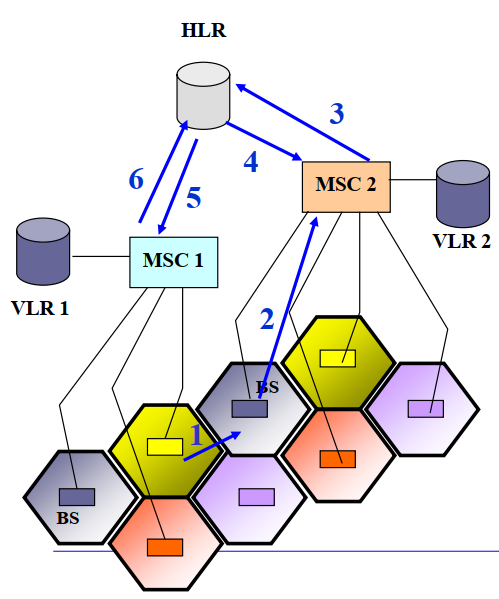
Per Roaming si intende l’insieme di funzioni con cui la rete gestisce la mobilità degli utenti. Gli elementi da cui è composto il roaming sono:

* HLR (Home Location Register): database unico per ogni rete che contiene tutti i dati relativi a ciascun utente, è unico per ogni provider (TIM, Vodafone, …)
* MSC (Mobile Switching Center): unico per ogni LA e si occupa di monitorare la mobilità, gestire le chiamate e handover (può gestire più di una LA)
* VLR (Visitor Location Register): database associato a ciascun MSC e contiene i dati relativi agli utenti attualmente all’interno delle LA del MSC

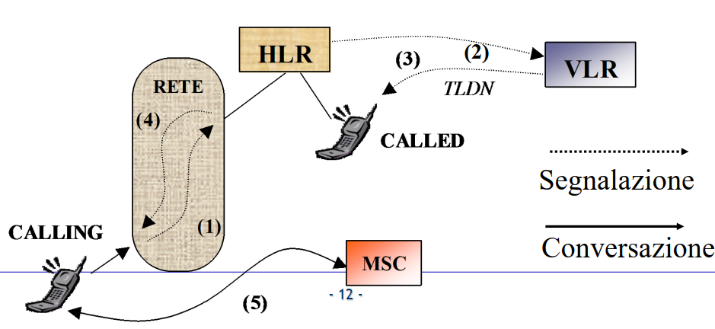
Il roaming viene gestito:

* tra celle appartenenti alla stessa LA: A → Base Station → MSC → VLR → Rete fissa → HLR
* tra celle appartenenti a diversa LA gestite dallo stesso MSC (Location Update): A → cambia LA (B) → BS → MSC → VLS → Rete fissa → HLR
* Tra celle appartenenti a LA diversi gestite da MSC diversi:

La procedura di Location Register è una procedura che si effettua quando un utente si sposta tra due celle diverse che appartengono a LA distinte, che a loro volta sono servite da due MSC differenti:

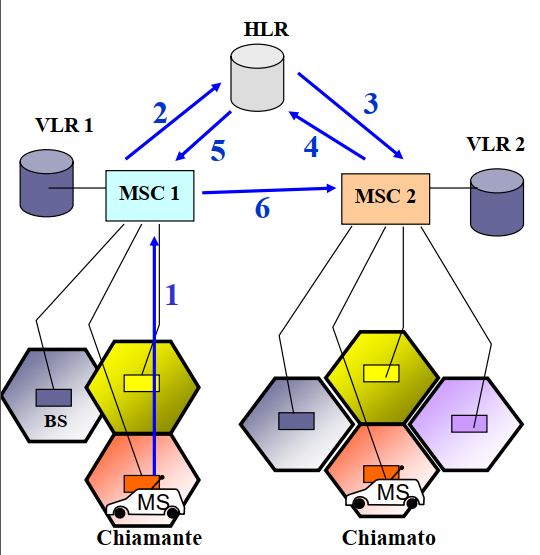
1. L’utente si sposta
2. L’utente capisce che si trova in una LA differenze e invia un messaggio di Location Update al proprio MSC. Il MSC interroga il proprio VLR che lo avverte che l’utente non è nella propria memoria
3. MSC richiede i dati di utente al HLR
4. HLR invia i dati al MSC
5. Contemporaneamente il HLR comunica al vecchio MSC di cancellare i dati dell’utente in questione
6. Il vecchio MSC invia al HLR una conferma della cancellazione

La funzione di Call Delivery funziona in questo modo:

1. Il chiamante, digitando il numero del chiamato, invia una richiesta al proprio MSC. Dal numero l’MSC risale al HLR del chiamato
2. L’HLR comunica al VLR del chiamato che c’è una chiamata in arrivo. In questo modo viene identificata la LA del chiamato
3. Se l’utente è libero, il VLR assegna al chiamato un numero temporaneo (Temporany Location Direction Number, TLDN) e lo comunica all’HLR
4. L’HLR inoltra la disponibilità del chiamato all’MSC del chiamante
5. Dopo il Paging il MSC del chiamate realizza attraverso la rete terrestre un circuito con il MSC del chiamato

La procedura di Paging è una procedura utilizzata per determinare l’esatta posizione (cella) in cui si trova un utente, al fine di realizzare il dialogo tra chiamante e chiamato. Il MSC conosce la LA in cui si trova un utente ma non la BS che lo sta servendo. Per conoscerne la cella esatta, invia in broadcast attraverso dei canali di controllo un messaggio di ricerca dell’utente a tutte le BS appartenenti alla LA in questione. Solo una BS restituirà al MSC un messaggio di reply comunicando che l’utente è all’interno della sua cella

La procedura di consegna della chiamata funziona in questo modo:

1. Il chiamante invia la chiamata al proprio MSC
2. Dall’identificativo dell’utente chiamato, il MSC risale al HLR dell’utente chiamato
3. Il HLR comunica al MSC dell’utente chiamato, che c’è una chiamata in arrivo
4. Tale MSC determina se l’utente è occupato/libero. Se occupato (idle) assegna all’utente chiamato il TLDN e lo comunica al HLR
5. Il HRL inoltra la disponibilità dell’utente chiamato al MSC dell’utente chiamante
6. Dopo la procedura di Paging, il MSC dell’utente chiamate realizza, attraverso la rete PSTN o ISDN, un circuito per collegarsi con il MSC dell’utente chiamato

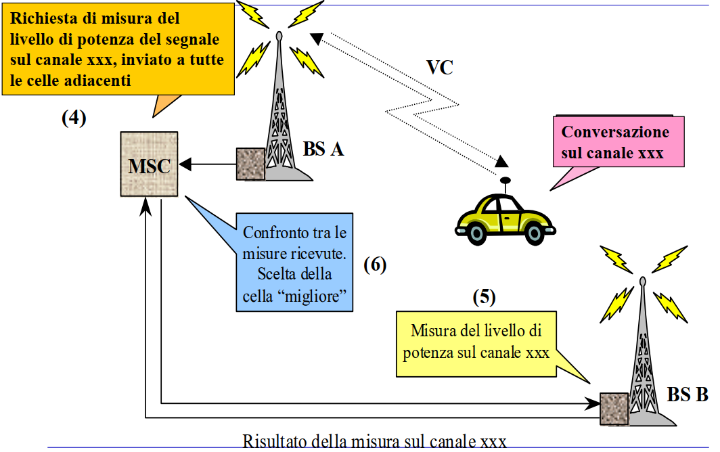
Ci sono alcuni mezzi per migliorare le tecniche di gestione del roaming:

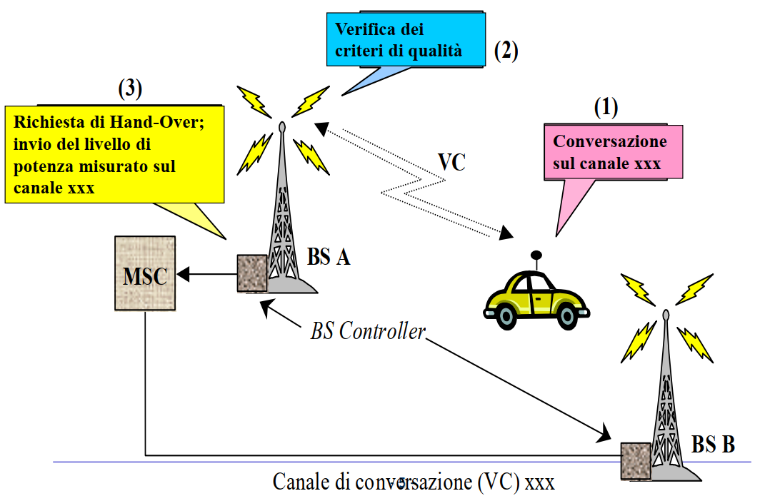
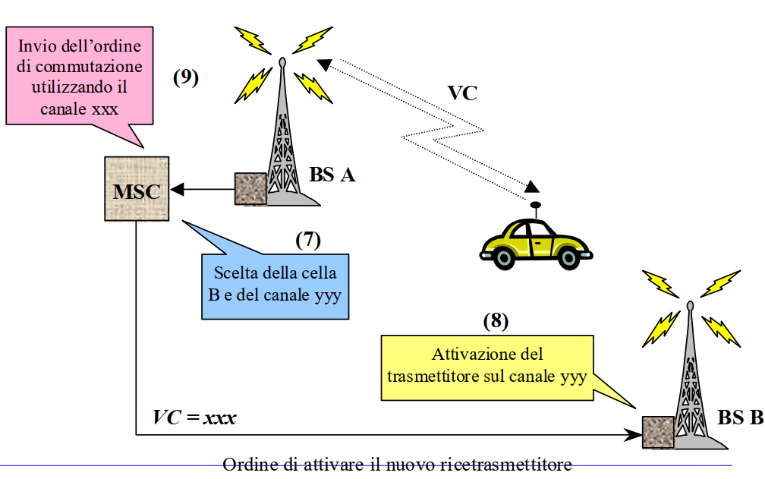
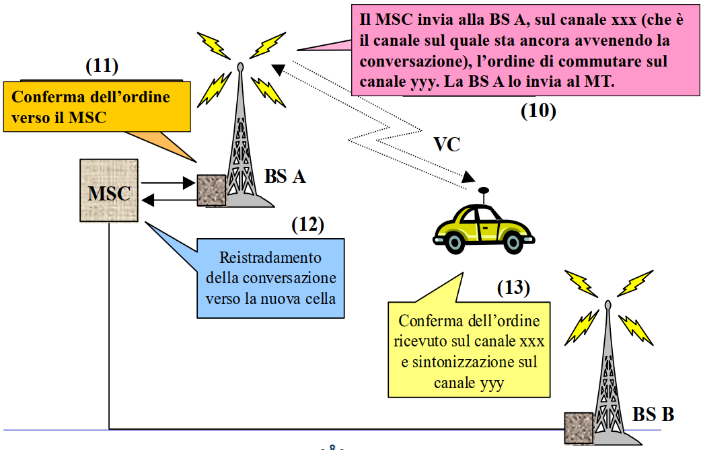
L’area di copertura viene suddivisa in tante LA, le cui dimensioni sono fissate dal gestore. Problema:

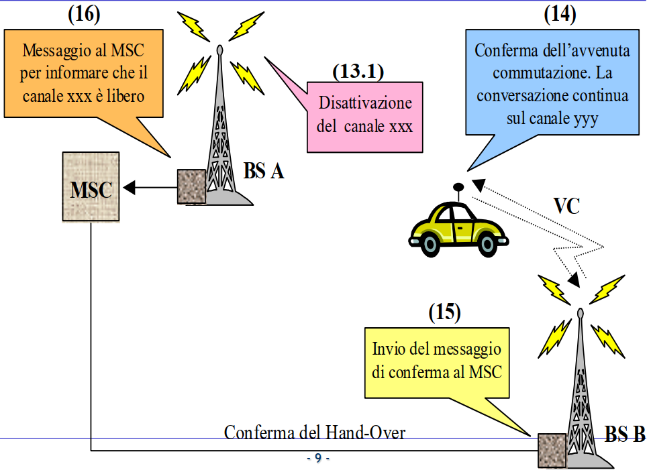
* Piccoli spostamenti dell’utente che si trova in una zona di forte confine tra due LA differenti avviano la procedura di location update che può coinvolgere percorsi molto lunghi. Soluzione:
  + Le LA non sono fisse ma variabili, e si adattano alle caratteristiche di mobilità dell’utente, le possibili strategie sono:
    - A tempo: l’utente comunica la sua posizione ogni DT, indipendentemente dal numero di celle attraversate
    - A movimenti: l’utente comunica la sua posizione ogni d passaggi di cella
    - A distanza: l’utente comunica la sua posizione quando la cella in cui si trova dista D celle da quella in cui si trovava l’ultima volta che ha comunicato la posizione

Altre tecniche sono:

* Per-User Location Caching: il suo obiettivo è minimizzare il numero di messaggi che devono transitare in rete durante la procedura di consegna della chiamata. Si utilizza per evitare che il MSC del chiamante contatti il HLR per determinare la posizione dell’utente chiamato. L’idea è quella di utilizzare un database (STP, Signal Transfer Point) dove registrare gli ID e i VLR degli ultimi terminali contattati dagli utenti che si trovano nella stessa LA
* Pointer Forwarding: il suo obiettivo è minimizzare il numero di messaggi che devono transitare in rete durante la procedura di Location Registration. Quando un utente passa da un MSC ad un altro, questa informazione non viene trasmessa all’HLR che potrebbe essere lontano, invece, nel vecchio VLR viene settato un puntatore al nuovo VLR e se arriva una chiamata per l’utente questa verrà cercata dal HLR nel vecchio VLR che punterà a quello nuovo.

La procedura di Handover (passamano) avviene quando un utente mobile con una chiamata in corso passi da una cella ad un’altra, in questo caso l’utente mobile dovrà passare dalla vecchia BS alla nuova BS.





Esistono 3 tipi di handover:

* Hard Handover: se l’utente si sposta durante la conversazione si ricerca la BS migliore su cui commutare, cade la linea per qualche millisecondo
* Seamless Handover: si viene a formare un canale tra il terminale e la nuova BS durante la conversazione, prima della commutazione. Il terminale non si accorge del cambiamento di BS
* Soft Handover: durante la commutazione la conversazione avviene per mezzo di entrambe le BS

Quando un utente vuole iniziare una chiamata, ma nella cella non ci sono canali radio, si ha un blocco della chiamata (Call Block). Quando un utente con chiamata in corso si sposta in una cella in cui non ci sono canali disponibili, si ha una caduta della chiamata (Call Drop)

Al fine di diminuire la probabilità di Call Drop sono state ideate delle tecniche basate su soglie, un certo numero di canali per ogni cella vengono riservati alle chiamate per handover. Se il numero di canali occupati nella cella è maggiore di una determinata soglia, le nuove chiamate non vengono accettate. Questa tecnica è chiamata Guard Channel.

Un’altra tecnica è il Channel Borrowing, il MSC effettua una gestione dinamica dei canali delle BS di sua responsabilità, prende dei canali dalle celle con basso carico di traffico per offrirli a quelle contigue che sono prossime alla saturazione.

Reti GPRS

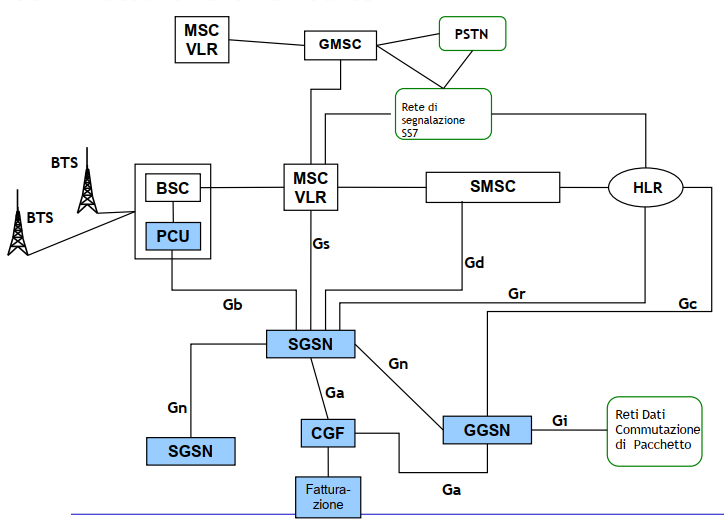
Il GPRS è una trasmissione a commutazione di pacchetto per reti GSM, si interfaccia a IP. Utilizza le stesse tecniche di accesso al mezzo del sistema GSM e la medesima interfaccia aerea, ottenuto dalla banda assegnata tramite tecniche di FDMA (Frequency Division Multiple Access) e suddiviso in 8 time-slot di durata temporale fissata, utilizza l’architettura di rete a commutazione di circuito del sistema GSM per la trasmissione della voce. A differenza del GSM, nel sistema GPRS è possibile allocare più di un time slot per la trasmissione di uno stesso utente. Il sistema GPRS fornisce un servizio dati a commutazione di pacchetto sovrapposto alla rete GSM a commutazione di circuito progettata per la voce.

Ci sono 3 tipi di terminali:

* Classe A: supporta l’utilizzo simultaneo di servizi voce e dati. Un utente di tale classe potrà effettuare chiamate vocali (GSM) e contemporaneamente effettuare trasferimenti dati (GPRS)
* Classe B: supporta connessioni simultanee alla rete GPRS e GSM ma non consente l’uso contemporaneo dei servizi. Se un utente di classe B ha in corso una trasmissioni dati e vuole effettuare una chiamata vocale, la trasmissione GPRS dei dati viene posta in attesa fino alla fine della chiamata
* Classe C: supporta connessioni sia alla rete GPRS che alla rete GSM, ma non simultaneamente. Un utente di classe C impegnato in una conversazione vocale risulta disconensso dalla rete GPRS e dunque irraggiungibile dai servizi dati e viceversa

Il sistema GPRS rappresenta una rete a commutazione di pacchetto sovrapposta alla rete GSM a commutazione di circuito

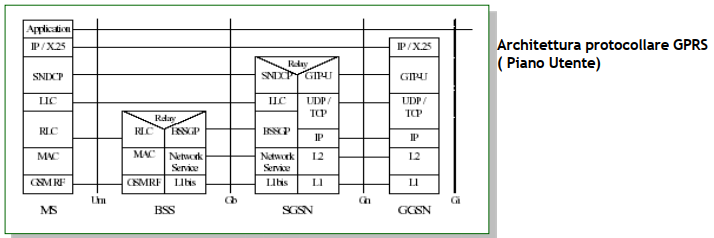
La BSS prevede due interfacce:

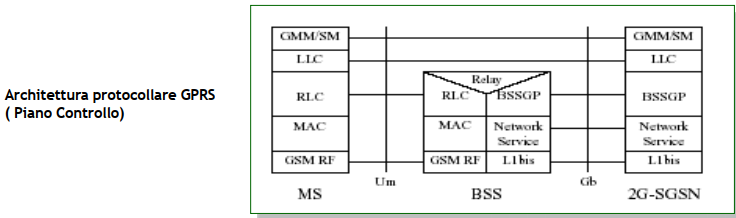
* Interfaccia A: già presente nel sistema GSM, collega la BSC (Base Station Controller) con il centro MSC. Connette la BSC con il dominio a commutazione di circuito
* Interfaccia Gb: connette l’unità PCU con il nodo SGSN (Service GPRS Support Node), permette la connessione degli elementi funzionali dell’interfaccia aerea con il nuovo dominio a commutazione di pacchetto, quest’interfaccia è di tipo “Frame Ralay” e utilizza il protocollo BSSGP (BSS GPRS Protocol) e supporta sia i segnali e le informazioni di controllo che il traffico relativo agli utenti, da e verso il nodo SGSN

Nuovi elementi di rete:

* Unità PCU: gestisce più BTS e si occupa dell’assegnazione delle risorse sull’interfaccia radio agli utenti GPRS
* Nodo SGSN: controlla uno o più PCU, presenta funzioni equivalenti al centro MSC ma nel dominio a commutazione di pacchetto. Gestisce la mobilità GPRS interfacciandosi con HLR per fornire gli aggiornamenti della posizione degli utenti e con altri nodi SGSN per aggiornare i percorsi di routing dei pacchetti durante l’handover e si occupa di raccogliere i dati relativi alla tariffazione. Questo nodo è anche collegato:
  + Tramite l’interfaccia Gr col database HLR per ottenere informazioni dettagliate sugli utenti che il nodo SGSN sta gestendo all’interno della sua area di copertura
  + All’interfaccia Gs, per il coordinamento dei centri MSC/VLR ed i nodi SGSN, relativamente a quegli utenti che supportano contemporaneamente sia i servizi a commutazione di circuito sia quelli a commutazione di pacchetto
  + All’interfaccia Gd, che permette di collegare il nodo con il centro SMSC (Short Message Service Center), consentendo agli utenti GPRS di inviare e ricevere SMS sfruttando la rete e l’interfaccia aerea GPRS
* Nodo GGSN: rappresenta l’interfaccia fra la rete GPRS e le altri reti a commutazione di pacchetto (Reti dati, reti PLMN), nel caso di sessione dati attivata dalla rete esterna, si interfaccia con il database HLR per conoscere ed inviare il flusso informativo al nodo SGSN che sta servendo l’utente mobile, ciò non avviene nel caso di sessione dati attivata dalla stazione mobile poiché i dati trasmessi dall’utente fino al nodo GGSN passano dal nodo SGSN che lo sta servendo. L’interfaccia tra i nodi SGSN ed il nodo GGSN a cui sono collegati è detta interfaccia Gn, essa si basa sul protocollo GTP (GPRS Tunneling) e supporta sia le informazioni di controllo che i dati d’utente. La medesima interfaccia viene utilizzata per connettere direttamente i nodi SGSN, la funzione principale dell’interfaccia è quella di consentire il passaggio dei pacchetti da un nodo SGSN all’altro. Opzionalmente il nodo GGSN può utilizzare l’interfaccia Gc per connettersi direttamente al database HLR.

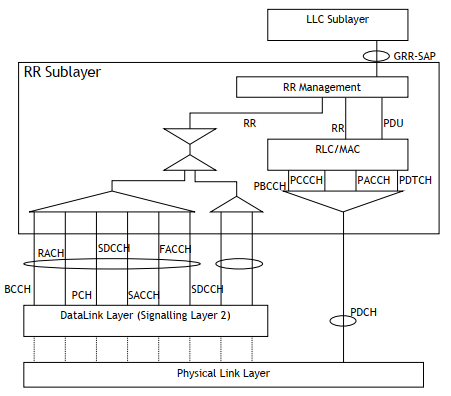
L’architettura protocollare di una rete GPRS è caratterizzata da una suddivisione dei diversi livelli in due piani, il piano di Controllo e il piano d’Utente.





Nel piano di controllo l’architettura protocollare dei livelli inferiori è identica a quella presenta nel piano d’utente. Nei livelli superiori, il protocollo SNDCP viene ad essere sostituito dal protocollo GMM/SM (GPRS Mobility Management and Session Management). Tale protocollo viene utilizzato per funzioni di sicurezza, per gli aggiornamenti delle aree di copertura e per la gestione delle sessioni dati PDP.

I protocolli di interfaccia radio Um si dividono in: Livello fisico, livello Mac, Livello RLC, livello LLC, Livello SNDCP.

Il livello RLC/MAC viene definito come RR-Sublayer, questo blocco comprende le funzionalità di gestione tipiche del sistema GSM che di quello GPRS, è nel blocco RR-Management che le due differenti funzionalità sono riunite:

* Il blocco RR-Management è l’entità responsabile della gestione dei canali di segnalazione GSM e tale funzionalità è stata estesa per permettere la gestione dei corrispettivi canali in ambito GPRS, tale blocco implementa le funzionalità di gestione della segnalazione, nel caso in cui si decida di utilizzare i canali di segnalazione GSM per trasportare anche la segnalazione GPRS.

Il blocco RLC/MAC è connesso al GRR/SAP in modo tale da convogliare l’informazione, proveniente dal livello LLC, verso i canali del livello fisico.

Il livello MAC risolve le problematiche relative all’allocazione delle risorse trasmissive, rendendo trasparenti ai livelli superiori le varie procedure necessarie all’instaurazione dei canali di trasporto a livello “Data Link”, si occupa anche della gestione delle procedure di Packet Idle Mode e Packet Transfer Mode:

* Packet Idle Mode: il mobile non ha un collegamento RLC attivo con la pari entità presenta all’interno della BTS, la MS non è raggiungibile e, non essendo effettuato nessun aggiornamento della posizione, può capitare che la rete sconosca la posizione corrente del mobile. I livelli superiori possono effettuare una richiesta di trasferimento dati che porta il mobile ad iniziare la procedura di connessione. Questa richiesta provoca una transizione nello stato di Packet Transfer Mode, un mobile in stato di idle deve essere continuamente in ascolto dei canali di paging, per poter riconoscere l’arrivo di un’eventuale chiamata da parte della rete
* Packet transfer mode: questo stato è caratterizzato dalla presenza di una connessione di livello RLC/MAC fra il mobile e la BTS. La MS, in stato transfer ha delle risorse allocate a livello radio e può effettuare il trasferimento di una o più LLC-PDU

Le funzioni del MAC sono:

* Multiplexing di dati e controllo: è implementata nella BTS sia per l’uplink sia per il down link. Per il down link il multiplexing è controllato da un meccanismo di scheduling mentre per l’uplink si ha un’allocazione distribuita del mezzo trasmissivo fra i vari utenti, gestita in modo centralizzato dalla BTS
* Risoluzione delle contese: l’accesso alla rete, in uplink avviene sfruttando un canale di segnalazione basato sulla tecnica Slotted-Aloha. La rete è responsabile dell’individuazione e della risoluzione di eventuali contese durante l’accesso
* Gestione delle priorità: il MAC all’interno della rete è responsabile della gestione delle priorità e di un’allocazione dei canali efficiente, secondo le direttive dei livelli superiori, in modo tale da soddisfare le richieste di QoS.

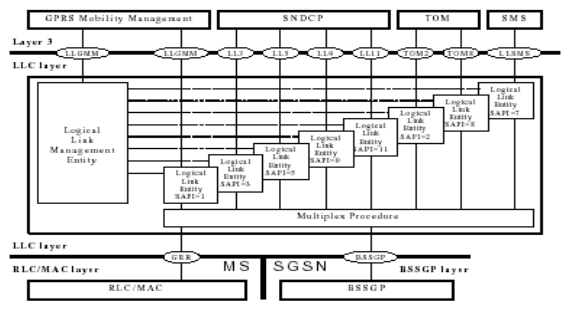
Il sistema GPRS condivide le stesse risorse radio del sistema GSM, l’assegnazione delle risorse può essere:

* Statica: un determinato numero di time slot per cella viene riservato in maniera esclusiva ai servizi GPRS
* Dinamica: i time slot vengono assegnati alla connessione GPRS se non utilizzati per chiamate vocali (precedenza servizi voce rispetto ai servizi dati a pacchetto)

Le risorse assegnate al sistema GPRS vengono condivise da più utenti, la trasmissione GPRS è asimmetrica (un utente ha a disposizione un numero differente di timeslot nella direzione di down link e uplink).

Il livello RLC (Radio Link Control) è responsabile di instaurare della connessione tra il mobile e la BOT, la connessione definita mediante la creazione di un flusso di informazione (Temporary Block Flow, TBF) per permettere la connessione fra due entità LLC, il TBF rappresenta un flusso dati a cui sono allocate risorse su uno o più PDCH e viene mantenuto attivo soltanto per l’effettiva durata del trasferimento dati. Le funzioni del livello RLC sono:

* Interfacciare il livello LLC: in modo tale da gestire il trasferimento delle relative LLC PDU
* Segmentazione e riassemblaggio: le LLC-PDU vengono segmentate in RLC-blocks per avere una dimensione tale da essere compatibili con la trasmissione a livello fisico
* Protezione dagli errori: è prevista la trasmissione degli RLC block in modalità unacknowledged o acknowledged sfruttando un meccanismo di ritrasmissione di tipo ARQ (Automatic Repeat Request)
* Countdown Procedure: procedura utilizzata dalla rete per predisporre il rilascio delle risorse assegnate al mobile

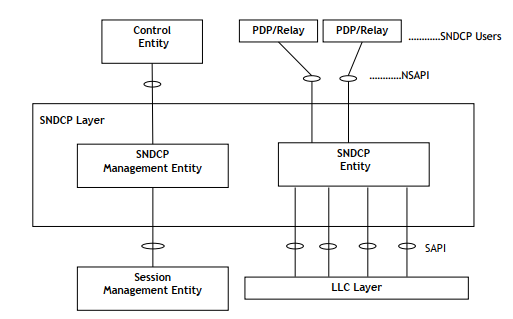
Il livello LLC (Logical Link Control) instaura una connessione logica per il trasferimento dei dati fra MS e SGSN. Ogni mobile è specificato, a livello LLC, da un identificativo, chiamato TLLI (Temporany Logical Link Identity) che unitamente al SAP Identifier viene utilizzato per determinare il flusso dati di un particolare mobile. Il SAPI indica infatti il Service Access Point (SAP) sull’interfaccia LLC, sia all’interno del SGSN che all’interno del mobile, mentre TLLI è utilizzato per risalire ad una particolare Mobile Station. I livelli superiori utilizzano i servizi del livello LLC tramite diversi SAP.

I principali livelli superiori che sfruttano le funzionalità del livello LLC sono:

* GPRS Mobility Management: si occupa di gestire funzioni quali l’instaurazione di un nuovo servizio ed il suo successivo abbattimento nell’aera servita dal SGSN, così come della mobilità fra le varie routing area
* SMS è l’entità responsabile della gestione dell’omonimo servizio di messaggistica
* TOM è utilizzato per il tunneling dei messaggi

Le funzioni del livello LLC sono:

* Gestione dell’instaurazione e del mantenimento di un link logico fra MS e SGSN
* Supporto per il trasferimento dei dati in frame di lunghezza variabile sia in modalità acknowledge che unacknowledge
* Multiplazione dell’informazione proveniente dall’SGSN e diretta alle diverse MS sfruttando la stessa interfaccia radio in modo condiviso
* Trasferimento dei dati secondo criteri di servizio differenziati in modo tale da diversificare i vari flussi a priorità differente

Lo scopo principale del livello SNDCP (Subnetwork Dependent Convergence Protocol) è quello di mappare le caratteristiche dei diversi livelli di rete, che possono essere presenti nell’architettura protocollare del GPRS. Le sue funzioni sono:

* Trasferimento dei dati in modalità unacknowledged verso il livello LLC
* Multiplexing dei dati provenienti dal livello di rete sul SAPI appropriato, prevedendo eventualmente la possibilità di condividere lo stesso SAPI per più flussi pervenuti dal livello superiore
* Gestione dell’instaurazione della connessione a livello LLC e suo rilascio
* Segmentazione (e riassemblaggio) dei dati provenienti dal livello rete su unità pari alla massima dimensione del blocco dati di livello LLC, scelta in fase di instaurazione della connessione

Il sistema GPRS offre nuovi servizi dati a commutazione di pacchetto (Web Browsing, E-mail, …), l’espletamento di tali servizi viene garantito mediante un set di parametri prestazionali che vengono raggruppati in classi.

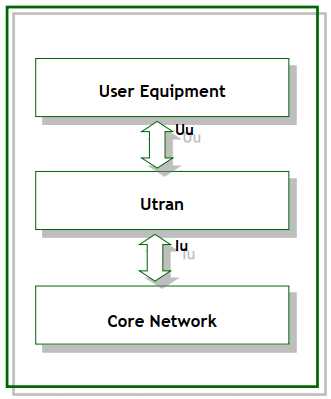
* Precedence Class: Differenti livelli di priorità (High, Medium, Slow) nell’espletamento dei servizi nel caso di congestione della rete o in presenza di scarse risorse
* Reliability Class: sono previsti tre differenti affidabilità della rete (Probabilità di perdita di pacchetti, probabilità di errori nelle informazioni trasmesse, probabilità di avere pacchetti fuori sequenza)
* Delay Class: 4 livelli di ritardo che la rete deve garantire, nessuno adatto a servizi interattivi real-time
* Throughput Class: Valore della banda richiesta per il trasferimento dei dati. È possibile negoziare sia il bit rate di picco che il valore medio.

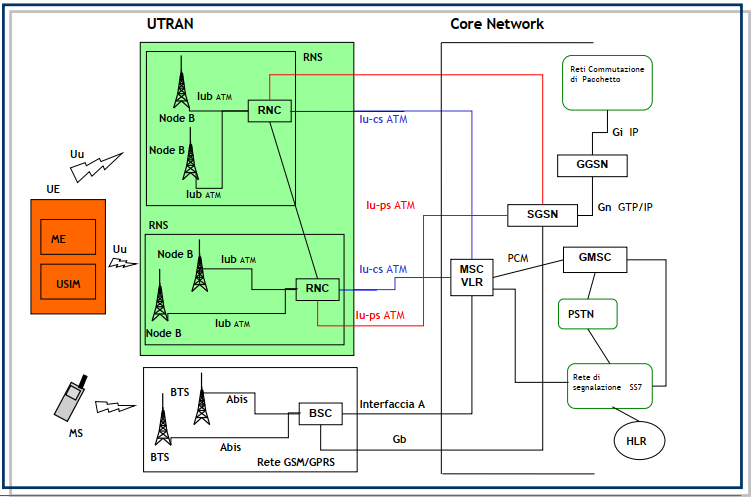
Reti UMTS

Le caratteristiche principali dell’UMTS sono:

* È una rete integrata per servizi voce e dati con trasmissione a commutazione di pacchetto
* È ad Accesso Multiplo a Divisione di Codice al mezzo comune (interfaccia aerea) (WCDMA)
* Maggiore capacità del sistema, limitata dall’interferenza dovuta dai diversi segnali d’utente
* Supporto di nuovi servizi real-time a bit-rate elevate
* Maggiori velocità di trasporto in funzione del servizio da espletare e dalle caratteristiche di mobilità

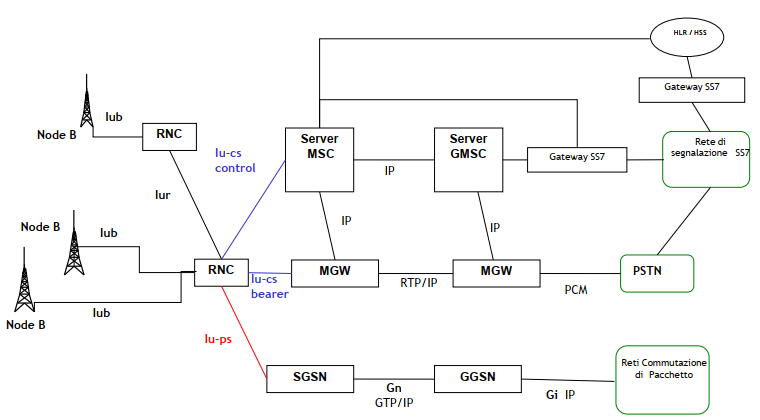
L’architettura dell’UMTS è formata da:

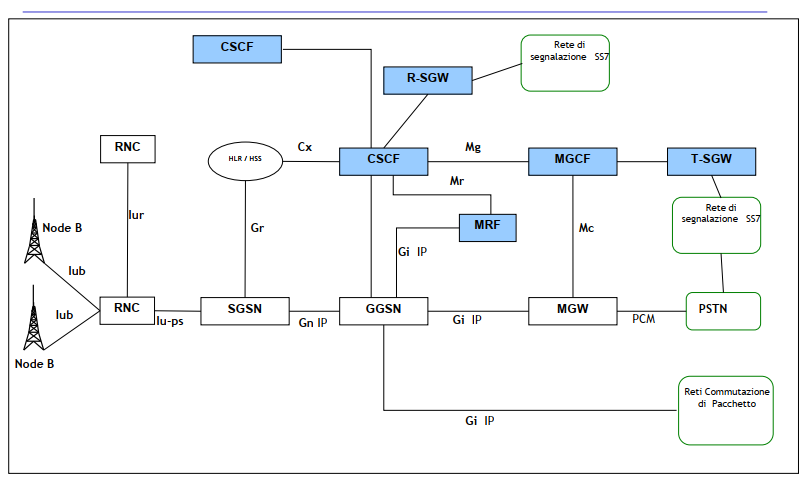
* User Equipment: terminale mobile utilizzato dall’utente per usufruire di tutti i servizi offerti dal sistema. Comunica con l’Ultran tramite l’interfaccia radio UU che rappresenta l’interfaccia di accesso WCDMA
* Utran: rete di accesso, ossia l’entità dedicata al controllo dell’accesso alla rete tramite la gestione delle risorse radio. Rappresenta l’unica che maggiormente differenzia il sistema UMTS dai sistemi GSM/GPRS, principalmente perché introduce la tecnica di multiplazione a divisione di codice per l’accesso radio. Per la parte di rete fissa, gli studi eseguiti hanno portato a adottare come sistema di trasporto una soluzione ATM/IP. La rete d’accesso è connessa alla Core Network tramite l’interfaccia IU
* Core Network: entità che si occupa della commutazione e dell’instradamento. Comprende due domini di rete: uno a commutazione di circuito (CS domani, Circuit Switched domain) ed uno a commutazione di pacchetto (PS domani, Packet Switched domain)

L’architettura di rete (release 1999) è formata da:

* User Equipment: costituito dal dispositivo ME (Mobile Equipment), gestisce la trasmissione radio e contiene le varie applicazioni ed i vari servizi offerti, e dal modulo USIM è il chip contenente alcune informazioni relative al profilo dell’utente ed i codici di sicurezza
* La rete di accesso è costituita da due tipi di nodi: il Nodo B, che presentano caratteristiche analoghe alle stazioni BTS presenti nel sistema GSM/GPRS, ed i controller RNC (Radio Network Controller) che sono invece equivalenti ai controller BSC del GSM/GPRS
* Il controllore RNC è connesso tramite l’interfaccia IUb ad uno o più nodi B, formando il sottosistema RNS (Radio Network Subsystem). A differenza dell’equivalente interfaccia Abis presente nel GSM, l’interfaccia IUb è aperta e standardizzata, ciò permette di connettere RNC e nodi B sviluppati da produttori differenti

A differenza del sistema GSM/GPRS dove i controller BSC non sono connessi tra loro ma per effettuare l’handover si è obbligati a raggiungere gli MSC, nel sistema UMTS sono presenti interfacce IUr che collegano direttamente gli RNC tra loro, rendendo più semplice sia il processo di handover (soft handover) che la mobilità all’interno dell’Utran. Il controller RNC che gestisce le risorse radio relative al proprio nodo B è detto CRNC (Controlling RNC), mentre quello che gestisce fisicamente la connessione tra l’User Equipment e la Core Network, controllando le risorse utilizzate dall’utente ed inoltrando la connessione verso le interfacce lu-CS o lu-PS a seconda del tipo di servizio richiesto. Normalmente il controller SRNC è anche il controller CRNC.

L’architettura di rete (release 4) è formata da:

* Un server MSC si occupa della gestione della mobilità e del controllo della connessione
* Un MGW (Media Gateway) contiene la matrice di commutazione, che gestisce fisicamente i vari flussi vocali attraverso il percorso di trasmissione. È necessario quindi che MSC e MGW siano interfacciati
* HLR: già presenta nell’architettura di rete GSM/GPRS e nella precedente release
* HSS (Home Subscriver Server) svolge la medesima funzione del HLR, entrambi rappresentano dei database che raccolgono tutte le informazioni relative ai diversi utenti. HLR utilizza interfacce SS7, un HSS utilizza interfacce basate su un trasporto a pacchetto (IP)

L’architettura di rete finale è formata da:

* Un nuovo dominio, in aggiunta a quelli CS e PS completamente basato su IP detto appunto dominio IM (IP Multimedia).

Tale dominio si basa sul protocollo SIP (Session Initiation Protocol)

* Terminale d’utente diventa in realtà un agente SIP
* CSCF (Call State Control Function): si comporta come un proxy SIP gestendo fondamentalmente i diversi step relativi alle sessioni multimediali (attivazione, mantenimento e rilascio) ed occupandosi delle funzioni di routing
* MFR (Multimedia Resource Function): supporta nuovi servizi come le chiamate fra più utenti ed i servizi di videoconferenza

L’interfaccia radio può essere divisa in 3 livelli principali:

* Livello Fisico (livello 1)
* Livello Data-Link (livello 2)
* Livello Network (livello 3)

Ci sono due piani:

* Piano di Controllo (C-Plane)
* Piano d’Utente (U-Plane)

Il livello 2 è a sua volta suddiviso in 4 sottolivelli:

* MAC (Medium Access Control)
* RLC (Radio Link Control)
* PDCP (Packet Data Convergence Protocol)
* BMC (Broadcast/Multicast Control)

Il livello 3 è a sua volta suddiviso in 2 sottolivelli:

* RRC (Radio Resource Control)
* Un sottolivello superiore che fa parte dell’Access Stratum con funzionalità di Duplication avoidance che termina nella Core Network

Funzioni del livello fisico:

* Esecuzione dei soft-handover
* Rilevamento degli errori sui canali di trasporto ed indicazione degli stessi ai livelli superiori
* Codifica e decodifica FEC (Forward Error Correction)
* Multiplexing dei canali di trasporto
* Adattamento della velocità di trasmissione
* Modulazione e demodulazione, spreading e despreading dei canali fisici
* Sincronizzazione nel dominio del tempo e della frequenza
* Misurazioni ed indicazione ai livelli superiori

Funzioni del livello MAC:

* Trasferimento dati: in modalità unacknowledged, di MAC-SDU fra entità di parli livello senza però supportare funzioni di segmentazione e riassemblaggio, per garantire il trasferimento dei dati il MAC definisce, nell’interfaccia con il sottolivello RLC, una serie di canali logici. Una classificazione dei canali logici è in Canali di controllo (trasferimento delle informazioni) e Canali di traffico (trasferimento delle risorse relative al piano d’utente)
* Riallocazione delle risorse radio su richiesta del RRC
* Rapporto delle misurazioni (misure locali sul volume di traffico e sulla qualità della trasmissione)
* Mappatura tra canali di trasporto e canali logici
* Selezione del formato di trasporto: assegnato dal RRC per il controllo
* Gestione delle priorità tra diversi flussi dati di uno stesso UE
* Gestione delle priorità tra UE
* Identificazione degli UE sui canali di trasporto comuni
* Multiplexing e demultiplexing delle PDU dei livelli superiori
* Monitoraggio del volume di traffico
* Cambiamento del tipo di canale di trasporto: esegue la commutazione tra canali di trasporto comuni e dedicati in base alle decisione del RRC
* Cifratura: protegge i dati trasmessi in modalità RLC trasparente, prevenendone l’acquisizione non autorizzata

RLC: rappresenta il sottolivello 2 del data-link layer, da un lato riceve i servizi offerti dal MAC e dall’altro garantisce un determinato numero di servizi specifici ai livelli superiori. Questo livello prevede 3 modalità differenti di trasmissione dei dati:

* Transparent
* Unacknowledged
* Acknowledged

Le sue funzioni sono:

* Segmentazione e riassemblaggio: segmenta e riassembla le PDU, di dimensioni variabili
* Concatenazione: se il contenuto di una RLC PDU non rientra in un numero intero di RLC PU, il primo segmento della successiva RLC PDU può essere concatenato con l’ultimo segmento della precedente
* Padding: nel caso in cui la concatenazione non sia attiva e i dati rimanenti da trasmettere non occupano un’intera RCL PU, il restante della RCL PU viene riempito con bit di padding
* Correzione d’errore: funzione presente solo nella modalità Acknowledged che fornisce la correzione degli errori mediante ritrasmissione
* Consegna in sequenza delle PDU di livello superiore
* Rilevamento dei duplicati
* Controllo di flusso: permette al RLC ricevente di controllare la velocità alla quale l’altra entità invia le informazioni
* Controllo del numero di sequenza: utilizzato in modalità unacknowledged per garantire l’integrità delle PDU riassemblate e fornire un meccanismo per il rilevamento delle SDU errate
* Cifratura: funzione utilizzata solo nella modalità trasparente per prevenire l’acquisizione non autorizzata dei dati
* Funzioni di Suspend and Resume: permettono di sospendere o riattivare il trasferimento dei dati

Livello PDCP (Packet Data Convergence Protocol): è il primo livello del piano utente e il suo obiettivo primario è di consentire l’utilizzo dei livelli comuni inferiori 8Fisico, MAC, RLC) in maniera indipendente dal tipo di struttura dati d’utente. Le sue funzioni sono:

* Segmentazione e riassemblaggio: segmenta e riassembla le PDU di livello superiore
* Trasferimento dati: garantisce la trasmissione e la ricezione di PDU di livello rete nelle diverse modalità supportare dall’RLC
* Consegna in sequenza: il livello PDCP permette di mantenere l’ordine con cui le PDU di livello superiore sono state trasmesse
* Compressione e decompressione delle intestazioni di rete
* Multiplexing: indirizza verso la stessa entità RLC diversi Canali Radio Bearer

Questo protocollo è formalmente simile al SNDCP (Subnetwork Dependent Convergence Protocol) del GPRS.

Livello BMC (Broadcast Multicast Control): trasparente a tutti i servizi esclusi quelli di broadcast e multicast. È responsabile delle trasmissioni in broadcast dei messaggi verso tutti gli utenti presenti in una cella, utilizza la modalità unacknowledged.

RRC (Radio Resource Control): è responsabile della gestione delle risorse radio e della quantità di risorse da allocare ad ogni singolo utente, è il gestore dell’interfaccia aerea. Le sue funzioni sono:

* Instaurazione, mantenimento e rilascio della connessione RRC: alloca e gestisce le risorse radio che verranno utilizzate
* Instaurazione, riconfigurazione e rilascio dei radio bearer: il livello RRC su richiesta dei livelli superiori può instaurare, riconfigurare e rilasciare i canali radio bearer nel piano utente, ossia quei canali atti alla realizzazione del servizio di trasporto (Bearer Service) necessario a garantire la QoS
* Assegnamento, riconfigurazione e rilascio delle risorse radio: il livello RRC gestisce l’assegnazione delle risorse radio per soddisfare le richieste sia nel piano utente sia in quello di controllo, gestisce sia l’allocazione delle risorse radio a più radio bearer sia il controllo delle risorse radio per realizzare comunicazioni asimmetriche tra Utran e gli UE
* Funzioni di gestione della mobilità: comprende le procedure di handover e di preparazione agli handover verso reti GSM o di altro tipo
* Paging: può trasmettere in broadcast informazioni di paging ad un determinato numero di utenti interessati
* Controllo della QoS richiesta
* Controllo della cifratura

Le funzioni dell’UTRAN sono:

* Trasferimento dei dati d’utente: permette di trasferire i dati d’utente attraverso l’UTRAN
* Funzioni relative al controllo dell’accesso al sistema che permettono all’utente di riconnettersi alla rete UMTS e di usufruire dei servizi offerti. Deve sia rilevare i vari tentativi di accesso alla rete da parte degli utenti, sia risolvere eventuali contese nei canali radio. Tra queste funzioni ci sono:
  + Controllo d’accesso: accetta o rifiuta nuovi utenti, cercando di evitare sovraccarico
  + Controllo della congestione
* Cifratura e decifratura dei canali radio: serve per proteggere i dati trasmessi da eventuali intercettazioni non autorizzate
* Funzioni relative alla mobilità: procedura di handover
* Funzioni relative alla gestione e al controllo delle risorse radio: queste funzioni comprendono:
  + Configurazione delle risorse radio: gestisce e configura le celle e i canali
  + Monitoraggio dei canali radio
  + Controllo della divisione e della ricombinazione dei flussi dati
  + Instaurazione e rilascio dei Radio Bearer
* Codifica e decodifica di canale
* Controllo della codifica di canale: genera informazioni di controllo, richieste dalle funzioni di codifica e decodifica

I nuovi servizi offerti dal UMTS richiedono velocità elevate di trasferimento dei dati e requisiti prestazionali alla rete, vengono definite 4 classi:

* Conversazionale:
  + Servizi real-time con velocità di trasferimento simmetriche. Bassa tolleranza ai ritardi e al Jitter, bit-Rate dipendente dal tipo di servizio
* Streaming:
  + Servizi monodirezionali con bassa tolleranza agli errori e in generale un elevata tolleranza ai ritardi.
* Interattiva:
  + Servizi di real-time di tipo dati, con requisiti temporali più lassi della classe conversazionale ma molto più sensibili agli errori (Web-Browsing)
* Background:
  + Traffico best-effort, caratterizzato da nessun vincolo temporale. Le applicazioni di tale classe richiedono che la trasmissione sia esente da errori (SMS, E-Mail)

Sicurezza nelle reti wireless

Le principali minacce alla sicurezza wireless sono:

* Frode commesse da parte di utenti del sistema autorizzati e non
* Spionaggio industriale
* Malicious code
* Spionaggio governativo
* Violazione della privacy

Ci sono 5 requisiti di sicurezza:

1. Autenticazione: siamo sicuri che A sia proprio A?
2. Confidenzialità: siamo sicuri che nessuno eccetto A e B possono accedere al messaggio m?
3. Integrità: siamo sicuri che m è il messaggio originale inviato da A?
4. Non-Repudiation: siamo sicuri che non c’è alcun modo per A di negare la “paternità” di m?
5. Autorizzazione: siamo sicuri che A possa accedere a questa risorsa?

Le problematiche relative alla sicurezza devono essere considerate in fase di progettazione. Un tradeoff tra utilizzabilità, performance e rischi.

WEP (Wired Equivalent Privacy):

è il primo protocollo utilizzato per garantire al sicurezza nelle reti wireless. Utilizza un algoritmo di cifratura (RC4 e CRC-32) che utilizza due chiavi, a 40 e a 104 bit. Non c’è protezione a livello data-link e non c’è protezione end-to-end.

L’autenticazione può essere:

* Cryptographic: usa RC4, ad una stazione è concesso di unirsi alla rete se dimostra di condividere la chiave
* Non-Cryptographic: si divide in:
  + Open System Authentication: una stringa vuota come SSID è accettata (NULL Authentication), una stazione può collegarsi alla rete trasmettendo una stringa vuota come SSID
  + Closed System Authentication: deve avere un valido SSID, una stazione può unirsi alla rete se fornisce un valido SSID per l’AP

L’autenticazione mediante Shared Key si basa sullo schema Challenge/Response basato sulla conoscenza da parte del client e dell’AP della chiave segreta, è una tecnica di encryption a chiave segreta, la procedura è:

* L’AP invia un random challenge al client
* Il client usando la shared secret key cripta il challenge e lo invia al AP
* L’AP decripta il messaggio e verifica che il risultato sia uguale al challenge trasmesso inizialmente

Per evitare di criptare due payloads con la stessa chiave, il WEP adotta un vettore di inizializzazione (Initialization Vector, IV). Mediante il vettore di inizializzazione è possibile ottenere chiavi RC4 per ogni pacchetto, IV è incluso nel pacchetto ed è un campo di 24 bit trasmesso nella parte in chiaro del messaggio. Un IV di 24 bit è così corto che determina il riuso della stessa chiave (Es. AP che invia 1500 byte di pacchetti a 11Mbps esaurisce lo spazio del IV in 5 ore →

L’intervallo di tempo è molto breve e quindi un hacker può trovare due chipertexts che siano criptati con la stessa chiave → Initialization Vector Collision

Per migliorare l’integrità viene utilizzata una tecnica basata sul CRC-32:

* Viene calcolata la frame check sequence per ogni payload trasmesso e ricevuto
* Il campo per il controllo dell’integrità è criptato nel payload del pacchetto
* CRC-32 è lineare → un hacker può cambiare n bits nel messaggio criptato e sistemare la checksum in modo che il messaggio finale sia apparentemente corretto

Il WEP ha problemi di autenticazione: chiunque può conoscere il SSID per accedere alla rate e ogni AP trasmette delle beacon frames in broadcast che contengono SSID in chiaro, non esiste l’autenticazione a due fattori, la shared-key authentication usa la stessa chiave per l’autenticazione e per le operazioni di encryption ed è facilmente esposta ad attacchi di man-in-the-midde

Ha un basso livello di confidenzialità a causa della natura broadcast del traffico wireless e dell’utilizzo di hubs (il traffico è soggetto ad attacchi da parte di utenti non autorizzati) e l’inserimento di AP non autorizzati

Ha un basso livello di Availability. Le principali cause di DoS sono:

* Jamming: un malicious user trasmette un segnale da un wireless device per danneggiare i segnali legittimi. Il risultato è un breakdown della connessione
* Un non-malicious user può causare DoS monopolizzando mediante un segnale wireless la rete, effettuando il download di file di grandi dimensioni

Per mitigare il rischio si sono pensate a due contromisure:

* Management Countermeasures: indentificare chi può utilizzare la WLAN in una organizzazione, identificare ogni accesso ad internet richiesto, descrivere chi può installare un AP e altri wireless devices, fornire delle limitazioni sulla localizzazione degli AP, …
* Operational Countermeasures: controllo di accesso mediante identificazione facciale, lettori di bedge, …

Altre contromisure possono essere:

* Configurazione AP: aggiornamento della password di default, controllo della funzione di reset, utilizzo delle funzionalità MAC ACL, cambio del SSID e della chiave di default, …
* Autenticazione: username e password, smart card, biometria, …
* Firewall
* VPN: usata per comunicazioni sicure tra locazioni remote, inizialmente forniva una Point-to-Point encryption tra remote user e corporate network, veniva usata per crittografare e proteggere il pacchetto IP

Per incrementare la sicurezza si è pensato ad una seconda versione del WEP, WEP 2. Utilizza una chiave a 128 bit, richiede un nuovo hardware e cambiamenti protocollari. L’obiettivo del WEP 2 è superare i problemi del WEP includendo la prevenzione dagli attacchi esterni e dai replay attacks, i problemi però sono che i Known plaintext sono ancora possibili e i client possono associarsi ad AP non autorizzarsi in quanto i beacon messages non sono autenticati.

Nasce lo standard IEEE 802.1x, è uno standard per la definizione di una generica framework per sistemi a controllo di accesso port based e per Key distribution, utilizza Extensible Authentication Protocol (EAP), gli AP autenticano la NIC consultano un server di autenticazione.

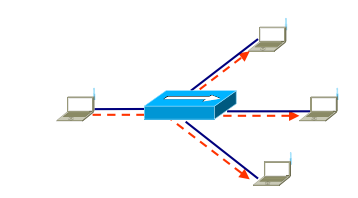
802.1x-EAP realizza una mutua autenticazione tra client e server, evitando in tal modo la presenza di rogue AP, consente una generalizzazione e distribuzione dinamica delle chiavi

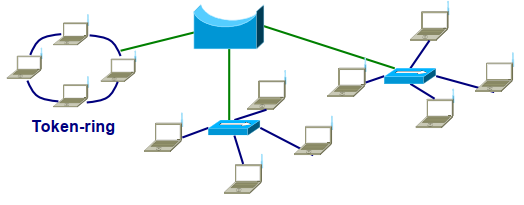
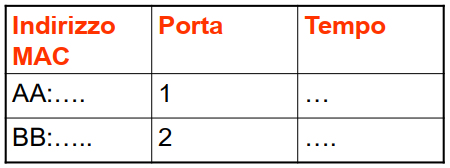
Lo standard IEEE 802.11i è progettato per includere lo schema di autenticazione di un 802.1x, EAP. Introduce un nuovo schema di criptaggio e un nuovo schema di distribuzione delle chiavi. Utilizza il TKIP per generare una chiave a 128 bit e include anche un Advanced Encryption Standard (AES, algoritmo che consente l’utilizzo di chiavi di varia lunghezza). Il TKIP è una soluzione a breve termine per risolvere alcuni problemi del WEP, non richiedi cambiamenti hardware o cambiamenti nel firmware o software

Dopo la WEP 2 viene presentata la Wi-Fi Protected Access (WPA), derivato dallo standard IEEE 802.11i, include lo 802.1x e TKIP, è flessibile sia per tipo di credenziali da fornire che per la versione di EAP da utilizzare, ha diverse applicazioni: Small Office and Home (SOHO), Enterprise e Public Access:

* SOHO: non c’è un server di autenticazione centrale né un EAP framework, lavora utilizzando Pre-Shared Key e funziona in questo modo:
  + Home user introducono la loro master key per entrare nel loro AP o home wireless gateway
  + WPA automaticamente procede: TKIP utilizza la master key solo nella fase iniziale di autenticazione, dalla master key deriva matematicamente la chiave da utilizzare per le operazioni di encryption
  + TKIP cambia le chiavi in modo che una stessa chiave non venga utilizzata due volte. Tutto ciò avviene in background
* Enterprise: effettua autenticazione, richiede un network server e richiede una master key per l’encryption
* Public Access: utile a WISPs (Wireless Internet Service Provider) per garantire Wi-Fi access in hotspot evitando l’uso della VPN

|  |  |  |
| --- | --- | --- |
|  | WEP | WPA |
| Encryption | Chiave a 40 bit | Chiave a 128 bit |
|  | Chiave statica | Chiave dinamica |
|  | Distribuzione manual | Distribuzione automatica |
| Autenticazione | Utilizza la stessa chiave | Strong-using 802.1x ed EAP |

Un HUB è un dispositivo di relaying operante a livello 1, è utilizzato per realizzare una topologia logica a bus mediante topologia fisica a stella (più affidabile), le stazioni sono tutte connesse con cavi UDP e il segnale generato su una porta è replicato sulle rimanenti porte.

Un BRIDGE è un dispositivo di relaying di livello 2, consente di interconnettere porzioni di reti LAN differenti e distinte che possono utilizzare tecnologie differenti e i frame in modo intelligente sulla base del destination MAC address e della MAC Table isolando i domini di collisione. La MAC Table è inizialmente vuota e viene riempita dal bridge in funzione dei frame in transito

Uno Switch è un dispositivo operante al livello 2, interconnette LAN omogenee e abilita la comunicazione full duplex (nessuna collisione), ha 3 modalità di funzionamento:

* Store and Forward:
  + Lo switch legge l’intera frame e verifica il CRC (scarto della frame se errato)
  + La frame viene memorizzata temporaneamente nel buffer associato alla porta d’uscita
  + La frame è trasmessa quando la linea della porta d’uscita è libera
* Cut and Through:
  + Lo switch legge solo l’header della frame
  + La frame è inoltrata senza memorizzazione intermedia
* Fragment Free:
  + Lo switch legge solo i primi 64 byte del frame all’interno dei quali possono avvenire collisioni
  + Scarta frame di dimensioni minori di 64 byte
  + Le frame errate più lunghe passano anche se il CRC non è corretto

Solitamente in una rete gli switch sono organizzati gerarchicamente:

1. Switch di piano (sezione di accesso alla rete)
2. Switch centrale (sezione di transito della rete)

Il protocollo Spanning-Tree (802.1d) evita che si formino anelli di bridge, i bridge si scambiano informazioni di controllo sulla base delle quali decidono quali porte lasciare attive. L’obiettivo è creare un albero di attraversamento dove ogni bridge è identificato da un ID unico (bridge identifier = Bridge Priority + MAC Address) e viene definito root-bridge quello con ID più basso. Le porte di ogni bridge possono assumere le seguenti funzioni:

* Root (R): individua il percorso più breve dal bridge al root-bridge (Stato = forwarding)
* Designated (D): determina il percorso più breve dalla LAN interfacciata al root-bridge (stato = forwarding)
* Blocked (B): (stato = blocking)

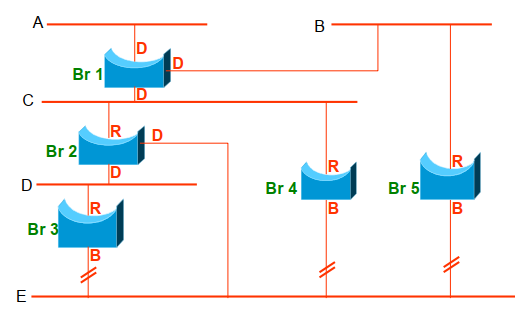
Lo Spanning tree è costituito mediante scambio di Bridge Protocol Data Unit (BPDU) che hanno un formato del tipo (C1, C2, C3) dove:

* C1 è l’ID del bridge che emette la BPDU
* C2 è l’ID del root-bridge secondo il bridge che ha messo la BPDU
* C3 indica il costo della via da C1 a C2 (espresso in numero di LAN da attraversare)

Come viene eletto il Root bridge e scelte le porte di Root:

* All’inizio ogni bridge (ID = x) ipotizza di essere il root-bridge ed emette BPDU del tipo (x, x, 0)
* Un bridge che riceve su una porta una BPDU tale che C2<ID cessa l’emissione di BPDU etichettando quella porta come R
* Un bridge che non sia root-bridge ritrasmette le BPDU ricevute sulla porta R verso tutte le altre porte aggiornando C1 con il proprio ID e incrementando C3
* Alla fine della procedura:
  + Il root-bridge (ID = r) è l’unico ad emettere BPDU e tutte le sue porte sono etichettate come D
  + Il generico bridge etichetta come R la porta da cui riceve BPDU con C2 = r e più piccolo valore di C3

Per selezionare le porte designate:

* Per eliminare il loop è sufficiente eleggere come D un’unica porta per segmento LAN connesso a più bridge, etichettando le altre come B
* Ogni bidge ritrasmette le BPDU di configurazione ricevute sulla root port verso tutte le altre porte
* Nel caso vi siano più bridge affacciati sulla stessa LAN, questi ricevono le BPDU da porte non root
* Se il costo C4 della BPDU ricevuta è più basso delle BPDU emesse dal bridge stesso, la porta è messa in blocking state; se C3 è più alto, la port aè osta in Designated cioè posta in forwarding state
* Le porte che non ricevono BPDU sono Designated perché non esistono altri bridge che inoltrano pacchetti nella LAN

Nelle operazioni normali lo stato delle porte di uno Spanning-Tree è blocking o forwarding, se per cambiamenti topologici una porta passa da blocking a forwarding state, vi sono due stati transitori: listening e learning:

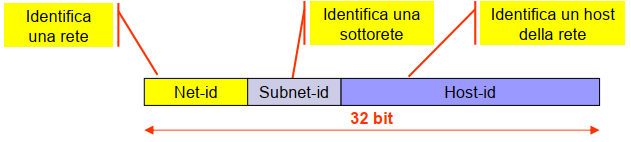
* Blocking: la porta è bloccata per le trasmissioni, ma può ricevere le BPDU di configurazione
* Listening: la porta è bloccata, riceve le BPDU di configurazione, ma attende prima di attivarsi per evitare loop
* Learning: la porta non inoltra le frame ma popola la sua MAC table
* Forwarding: la porta riceve e inoltra le frame

Indirizzi IP

Un indirizzo IP è composto da 32 bit ed è suddiviso in una porzione dedicata alla rete ed una agli host. Esistono 5 classi di indirizzi IP: A, B, C, D, E

Gli indirizzi IP possono essere:

* Pubblici: l’indirizzo può essere utilizzato esclusivamente da una specifica organizzazione e sono usati per instradare pacchetti in internet
* Privati: possono essere usati solo in una rete privata, ma non si possono instradare pacchetti con tali indirizzi in internet
* Statici: l’IP dell’host non varia nel tempo
* Dinamici: l’IP dell’host varia nel tempo

Tramite il subnetting una parte dei bit adibiti all’identificazione dell’host sono dedicati alla definizione di una sottorete, la rete è suddivisa in molteplici sottoreti che è invisibile all’esterno della rete. I bit dedicati alla definizione di rete e sottorete sono identificati nella Subnet Mask (Es. 193.204.59.56/24)

Il multicasting consiste nel trasmettere verso destinazioni multiple da un’unica sorgente dati. Il gruppo di host coinvolti nella comunicazione si definisce host group ed è identificato da un indirizzo IP di classe D

L’Address Resolution Protocol (ARP) è un protocollo di risoluzione degli indirizzi MAC, è utilizzato per conoscere il MAC address corrispondente ad un determinato IP. Siano A l’host mittente e B l’host di cui non si conosce il MAC address, A invia una richiesta in Broadcast indicando l’IP di B → B risponderà ad A con un reply Unicast

Il datagramma dell’IP è formato da:

* Version (4 bit): definisce la versione del protocollo (IPv4/IPv6)
* Header Length (4 bit): dimensione dell’header in parole da 32 bit
* Type Of Service (8 bit): definisce i requisiti in termini di QoS, viene utilizzato per definire il forwarding behaviour associato al datagramma
* Total Length (16 bit): lunghezza del datagramma espressa in byte
* Identification (16 bit): indentifica in modo univoco un datagramma generato dall’host mittente
* Flag (3 bit): informazioni utili alla frammentazioni (MF indica se il datagramma è l’unico dei frammenti, DF indica se il datagramma può essere frammentato)
* Fragment Offset (13 bit): identifica il frammento di un datagramma espresso in multipli di 8 byte. La Maximum Transfer Unit (MTU) è la massima dimensione di una SDU del livello data-link e limite la dimensione del datagramma IP
* Time To Live (8 bit): è impostato dal mittente (128), ad ogni hop è decrementato di una unità e quando raggiunge il valore 0 viene scartato
* Header Checksum (16 bit): si ottiene sommando 16 bit a 16 bit i 18 byte dell’header e facendo il complemento a 1 del risultato
* Source address (32 bit): indirizzo IP dell’host mittente
* Destination address (32 bit): indirizzo IP dell’host destinatario
* Options: operazioni per il routing del datagramma

Il Dynamic Host Configuration Protocol (DHCP) consente ad un host di ottenere da un DHCP server l’indirizzo IP, l’indirizzo IP del router di default e l’indirizzo IP del server DNS, la richiesta è inviata dall’host in broadcast sulla rete locale. Se non è disponibile alcun DHCP server nella rete locale, la richiesta può essere inoltrata verso un’altra rete. Se sono presenti più DHCP server nella medesima rete locale, dopo una contesa, l’indirizzo IP è fornito dal server che per primo ha ricevuto la richiesta

La Zero Configuration Networking è una configurazione della rete in assenza di server e amministratori, è ideale solo per le piccole reti (dove non ci sono DHCP e DNS). Link-Local Address: 169.254.0.0/16, gli indirizzi Link-local sono di tipo privato e non possono essere usati per il forwarding di dati fuori dalla rete locale.

Il NAT (Network Address Translation) consente a tutti gli host della rete locale di usare l’indirizzo IP del router di frontiera per connettersi ad internet. Nel NAT ogni host della LAN ha un indirizzo IP non visibile all’esterno della LAN, tutti i datagrammi IP che viaggiano da/verso la LAN hanno il medesimo indirizzo IP mittente/destinatario. Il NAT utilizza una Tabella di traduzione per selezionare a quale host della LAN è diretto un datagramma che proviene dall’esterno.

Il NAT Statico è utilizzato quando all’interno LAN è presenta un Server e in tal caso si crea un’associazione statica tra indirizzo privato del server e indirizzo pubblico del router di frontiera.

Il Private Network è un IP network non connesso direttamente ad internet, gli indirizzi IP in una Private network possono essere assegnati arbitrariamente.

I principali utilizzi del NAT sono:

* Messa in comune degli indirizzi IP: solitamente una rete aziendale ha molti host ma pochi indirizzi IP, la soluzione che offre il NAT è:
  + La rete aziendale viene gestita con un indirizzo privato
  + Il NAT, localizzato tra la rete aziendale e internet gestisce la messa in comune degli IP
  + Quando un’host dalla rete aziendale manda un datagramma IP ad un’host nella rete internet, il NAT prende l’IP pubblico dall’Address Pool, e nasconde il suo indirizzo all’indirizzo privato dell’host
* Supporto della migrazione tra network service providers: gli IP in una rete aziendale sono ottenuti dal service provider. Cambiare il service provider richiede un cambiamento di tutti gli IP nella rete, la soluzione che offre il NAT è:
  + Assegna indirizzi privati agli host dell’azienda
  + Il NAT ha un indirizzo di transazione statico che nasconde l’indirizzo privato di un host ad un indirizzo pubblico
  + Migra alla nuovo service provider che può richiedere un aggiornamento del NAT. La migrazione non viene notata dagli host della rete

La differenza nell’usare il NAT con la messa in comune degli IP è che il mapping degli IP pubblici e privati è statico

* Mascheramento dell’IP: chiamato anche Network Address and Port Translation (NAPT) o Port Address Transaltion (PAT), un singolo IP pubblico viene mappato in più host in una rete privata, la soluzione che offre il NAT è:
  + Assegna indirizzi private agli host dell’azienda
  + Modifica il numero di porte per il traffico in uscita
* Bilanciare il carico dei server: bilanciare il carico su dei server identici che sono accessibili da un singolo IP, la soluzione che offre il NAT è:
  + I server hanno un IP privato
  + Il NAT fa da proxy per fare richieste da una rete pubblica
  + Il NAT cambia l’IP di destinazione dei pacchetti in arrivo ad uno degli indirizzi privati del server
  + Una strategia sensibile per il bilancio del carico di lavoro è quello di assegnare agli indirizzi del server una round-robin

Alcuni problemi del NAT possono riguardare:

* Performance:
  + Modificare l’header dell’IP cambiando l’indirizzo IP richiede che il NAT ricalcoli l’header checksum dell’IP
  + Modificare il numero di porte richiede al NAT di ricalcolare la TCP checksum
* Fragmentation:
  + Si occupa che il datagramma che è frammentato prima che raggiunga il NAT, non sia assegnato ad un differente indirizzo IP o ad un diverso numero di porte per ogni frammenti
* Connessione end-to-end:
  + Il NAT distrugge l’universale raggiungibilità end-to-end degli host ad internet
  + Un host in internet non può iniziare la comunicazione con un host in una rete privata
  + Il problema è peggiore quando due host in una rete privata cercano di comunicare tra loro
* Indirizzi IP nelle applicazioni dati:
  + Applicazioni che portano l’IP nel payload dell’application data generalmente non funzionano attraverso una private-public network boudndary
  + Qualche NAT ispeziona il payload utilizzando i protocolli dell’application layer e, se l’IP viene identificato nell’header dell’application layer o nel payload dell’applicazione, transa l’indirizzo in base all’indirizzo della tabella di transizione

Algoritmi di routing: tassonomia

Ogni router consulta una propria tabella di routing per scegliere verso quale porta d’uscita (next hop) instradare i datagrammi in ingresso. Vengono utilizzate delle metriche per il costo dei path:

* Bandwidth: la capacità di un link
* Delay: il tempo necessario ad ogni pacchetto lungo il percorso per andare dalal sorgente alla destinazione
* Load: il carico di lavoro degli elementi della rete come i router o i link
* Reliability: l’affidabilità è generalmente riferita al tasso di errore di ogni singolo link
* Hop count: il numero di router che un pacchetto deve attraversare per raggiungere la sua destinazione
* Ticks: il ritardo con un collegamento dati usando gli IBM PC clock ticks
* Cost: un valore arbitrario, generalmente basato sulla banda, sul costo economico di un link, o sua altre misure stabilite dall’amministratore di rete

Le operazioni svolte da un router sono:

* Ricerca nella routing table una entry con lo stesso indirizzo di rete del destinatario del datagramma ricevuto
* Se la entry corrisponde ad una rete direttamente connessa al router allora viene individuata la sottorete e poi il datagramma è inoltrato
* Se la entry corrisponde ad una rete remota il datagramma è inoltrato (forwarding)
* Se nessuna entry è trovata allora viene utilizzato il default route

Il Classes Inter Domanin Routing (CIDR) è la parte di indirizzo IP relativa alal rete e può avere lunghezza qualsiasi. Il formato dell’indirizzo è a.b.c.d/x dove x indica il numero di bit significativi che individua la rete, in questo modo è possibile ridurre le dimensioni delle tabelle di routing (Es. 193.204.59.0 e 193.204.60.0 → 193.204.56.0/21, viene detto supernetting)

L’instradamento gerarchico in internet è l’insieme di router amministratore dallo stesso gestore che viene definito Autonomous System (AS), si distinguono algoritmi di routing intra ed inter come:

* RIP (intra): Routing Information Protocol
* OSPF (intra): Open Short Path First
* BGP (inter): Border Gateway Protocol

Distance Vector: ogni router invia, periodicamente o quando c’è un cambiamento topologico, la propria tabella di routing ai vicini, i router scelgono la strada migliore confrontando i distance vector ricevuti. Ogni router non conosce l’intera topologia. Un problema del distance vector è che la definizione di un massimo blocca il “counting to infitiny”. Per evitare i loop si può usare:

* Split horizon: non si inviano informazioni su una route all’indietro verso la porta da cui quell’informazione è giunta
* Split horizon with poisoned reverse: le route vengono annunciate con metrica infinity sulla rete su cui si trova il loro next hop se apprese da esso stesso
* Trigger Update: gli aggiornamenti delle tabelle di routing sono inviate ogni qualvolta vi è un cambiamento topologico e non solo allo scadere del route timer

Una rete dichiarata irraggiungibile è considerata tale (la sua entry è eliminata) solo allo scadere di un hold-down timer.

Il RIP è adatto a reti di piccole dimensioni, è un protocollo di routing di tipo Distance Vector e usa come metrica gli hop count, il valore massimo è 15 e il 16 indica rete irraggiungibile. Ogni router comunica lo stato della propria tabella di distanze ai router direttamente raggiungibili. Il formato dei messaggi RIP:

* Utilizza UDP a livello di trasporto per lo scambio di messaggi RIP
* Ogni messaggio contiene fino a 25 descrittori di route
* Nel RIPv2 si trasmette anche la subnet mask associata all’indirizzo
* RIPv2 utilizza i Route Tag per le route interne o esterne e il NextHop per indicare un router diverso da chi ha mandato il messaggio
* RIPv2 permette di autenticare i messaggi di routing

OSPF: ogni nodo conosce la topologia della rete, possono essere utilizzate molteplici metriche per ognuno dei servizi previsti dal campo ToS del protocollo IP, il miglior percorso è determinato con l’algoritmo di Dijkstra. Ogni AS è diviso in aree ognuna definita da 4 ottetti. Limita la dimensione delle aree e i messaggi tra aree. Ogni router ha un suo router ID incluso negli Hello packet inviati periodicamente su tutte le interfacce

Link State Advertisement: periodicamente ogni nodo invia lo stato dei suoi collegamenti (Link State Packet, LSP). In OSPF si parla di Link State Advertisement (LSA). Ogni pacchetto scambiato tra router può contenere più LSA. I router con interfacce solo nella stessa area sono Internal Router e generano LSA che descrivono la rete interna. I router tra due aree sono detti Area Border Router e devono avere almeno un’interfaccia verso la Backbone Area. I router di bordo dell’intero AS sono detti Boundary Router e inseriscono nei loro LSA informazioni sull’esterno dell’AS. Gli LSA sono inviati dali Internal Router vicini mediante Selecrive Flooding