

Domande di RETI DI TELECOMUNICAZIONE

Indice:

Quali sono i parametri che influenzano l'attenuazione isotropica? Quali sono i parametri che influenzano la distanza di riuso? Quali sono i parametri che influenzano il traffico offerto? "" l'efficienza? etc. (formule).

1. Descrivi la differenza tra commutazione di circuito e commutazione di pacchetto;
2. Come può essere l' accesso al canale?
3. Descrivi il protocollo CSMA/CD; e descrivere il protocollo CSMA/CA
Descrivere il protocollo del binary exponential backoff
4. Descrivi il funzionamento del frame 802.5;
5. Come avviene la trasmissione Wi-Fi? Quali sono le tecniche spread spectrum riconosciute?
6. Descrivere come un device o nodo seleziona un access point e come si chiama tale tecnica;
7. Come avviene l' accesso al canale nel Wi-Fi?
8. Che cosa sono i nodi nascosti e i nodi esposti (o sovrapposti)? E come si risolve il problema delle collisioni a causa di questi tipi di nodi?
9. Come avviene la trasmissione nel Bluetooth?
10. Indica quali sono le principali cause di interferenza nel Wi-Fi;
11. Da cosa è costituita una Piconet? E che cos' è una Scatternet?
12. Come sono i collegamenti all' interno di una Piconets?
13. Come fa una rete mobile ad avere copertura globale usando un set di frequenze finito e senza avere interferenza co-canale?
14. Che cos' è e a cosa serve il roaming;
15. Descrivi la procedura di Location Update del roaming;
16. Quali tecniche esistono per migliorare il roaming?
17. Descrivi la procedura di consegna della chiamata; (call delivery)
18. A cosa serve l' Handover?
19. Descrivere la procedura di Handover;
20. Quanti tipi di Handover esistono?
21. Quali tecniche esistono per migliorare l' Handover?
22. Descrivi il protocollo CDMA;
23. Che cos' è il GPRS?
24. Come avviene l' accesso al canale nelle reti GPRS?
25. In quante e in quali classi si dividono i terminali con l' introduzione del GPRS?
26. Descrivi l' architettura di rete delle reti GPRS; Quali sono gli elementi di architettura del GSM? quali sono differenti tra GSM e GPRS?
27. A cosa serve il nodo SGSN? NOVITA gprs e umts: piano d'utente e piano di controllo.
28. Descrivi l' architettura protocollare del GPRS;
29. Descrivi le funzioni del sottolivello RLC/MAC;
30. Descrivi le funzioni del MAC; che cos'è il mac address e quale notazione utilizza?
31. Descrivi l' architettura protocollare dell' UMTS; Che cos'è il dominio IM dell'umts?
32. Quanti e quali sono i requisiti che deve avere una rete wireless per essere considerata sicura?

33. Che cos' è il WEP?
34. Come avviene l' autenticazione nel WEP?
35. Come funziona il challenge-response? Che cos' è l'IV collision?
36. Come viene garantita la confidenzialità nel WEP?
37. Come viene garantita l' integrità?
38. Quali sono le debolezze del WEP?
39. Descrivi l' evoluzione dei protocolli di sicurezza;
40. Descrivi il funzionamento di WPA per SOHO;
41. Illustra le differenze tra WEP e WPA;
42. Descrivere brevemente i dispositivi di realying;
43. Descrivi il protocollo spanning tree;
44. Quali sono gli stati intermedi per passare da B a D?
45. Descrivi il protocollo IP; Che cos' è IP Address? e quale notazione utilizza Qual' è il protocollo per ottenere degli indirizzi dinamici?
46. A cosa serve il DHCP (Dynamic Host Configuration Protocol) e lo ZCN (Zero Configuration Networking)? e cos' è?
47. Che cos' è l' ARP?
48. Come funziona il trasferimento dei pacchetti sulla stessa rete? E come funziona su reti differenti?
49. Che cos' è il NAT? E quali funzioni svolge?
50. A cosa servono gli algoritmi di routing e com' è la loro tassonomia?
51. Spiegare il funzionamento di un router;
52. Spiegare gli algoritmi di routing; Che cos' è il RIP? e il BGP? e OSPF? Inter Autonomus System è solo il BGP Quali sono gli algoritmi di routing intra autonumun system?
53. Come si crea una socket?
54. Descrivi il protocollo TCP e indica a cosa serve il controllo di flusso; Descrivere il protocollo di congestione del TCP
55. Descrivi il processo di creazione e di interruzione di una connessione TCP;
56. Indica come avviene la trasmissione dei segmenti in una connessione TCP e a cosa serve la sliding window;
57. Come varia il valore della CW nei diversi TCP (NB: potrebbe essere collegata alla domanda precedente);
58. Descrivi il WWW (World Wide Web);
59. Descrivi i protocolli applicativi;
60. Descrivi il DNS ed il suo funzionamento;
61. Descrivi il Resource Record;
62. Descrivi l' electronic mail (e-mail); Decrivi quali sono i protocolli utilizzati per la gestione delle email?
63. Descrivi la pila dei protocolli per il trasferimento di contenuti multimediali e indica cos' è l' RTP; E cos' è l' RTP?
64. Indica le soluzione per ridurre la World Wide Wait;
65. Che cos' è e a cosa serve il proxy server;

66. Che cos' è il CDN (Content Distribution Networks);
67. Che cosa sono le sensor networks?
68. Quali sono i fattori che influenzano la progettazione di una sensor network?
69. Perché non è possibile utilizzare l' indirizzo IP nelle sensor networks?
70. Quali sono i protocolli di routing nelle SN (livello di trasporto)?
71. Quali sono le funzioni svolte da un protocollo di trasporto?
72. Descrivi come possono essere le query;

===== MODELLO ISO/OSI E MODELLO TCP/IP =====

1. Descrivi la differenza tra commutazione di circuito e commutazione di pacchetto

Nella commutazione di circuito il canale viene allocato in via esclusiva, viene trasmessa l' informazione e poi viene rilasciata la risorsa.

- **VANTAGGI:**
 - È garantito l' ordine di arrivo dei pacchetti (dato che seguono tutti lo stesso percorso);
 - Non c' è perdita d' informazione (in quanto i pacchetti persi vengono ritrasmessi).
- **SVANTAGGI:**
 - Le risorse sono sprecate perché restano bloccate finché non termina la comunicazione (non sono utilizzate in maniera efficiente).

Nella commutazione di pacchetto invece, non c' è allocazione delle risorse; le informazioni vengono divise in pacchetti che contengono ognuno l' indirizzo del mittente e del destinatario. Ne esistono 2 varianti:

- **A datagramma:** i pacchetti seguono percorsi diversi in base alle migliori condizioni del traffico sul canale;
- **A circuito virtuale:** i pacchetti seguono lo stesso percorso senza che il canale sia allocato in via esclusiva.
- **VANTAGGI:** le risorse sono utilizzate in maniera efficiente e lo scambio d' informazioni è più veloce;
- **SVANTAGGI:** non è garantito l' ordine di arrivo e ci può essere perdita d' informazione (in quanto i pacchetti persi non vengono rispediti).

I servizi con connessione utilizzano una commutazione di circuito:



- Conferma dell' avvenuta ricezione attraverso un ACK

I servizi senza connessione utilizzano una commutazione di pacchetto:

- Conferma di avvenuta ricezione opzionale.

2. Come può essere l' accesso al canale?

L' accesso al canale può essere:

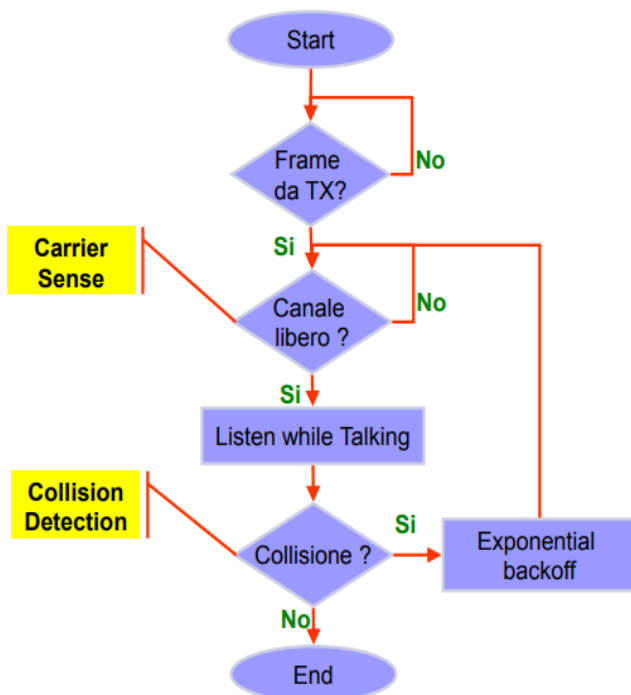
- **Ordinato**: parla solo chi possiede il token (es. frame 802.5 token ring);
- **Casuale**: che può essere:
 -  
 - **Con rilevazione del canale (CSMA)** che **a sua volta può essere**:
 - **Con rilevazione delle collisioni (CSMA/CD)**;
 - **Senza rilevazione delle collisioni (CSMA/CA)**.

3. Descrivi il protocollo CSMA/CD

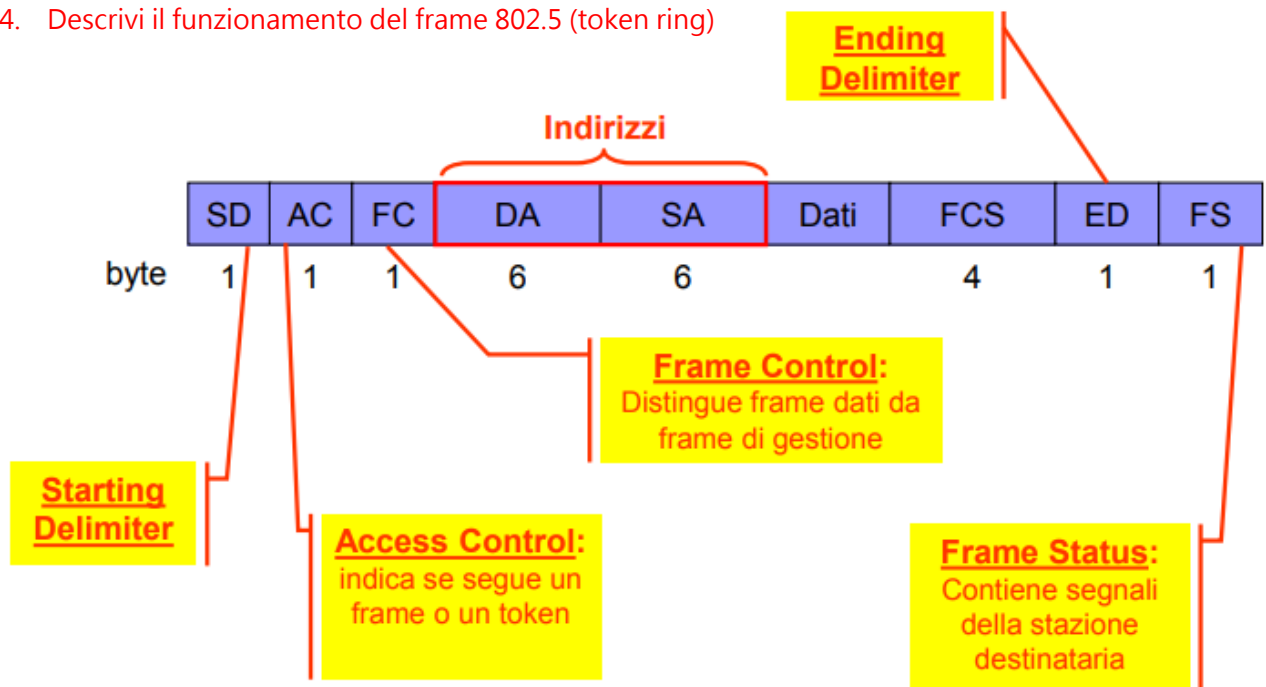
Il protocollo CSMA/CD è un protocollo adottato dallo standard 802.3 ad accesso casuale con rilevazione del canale e con rilevazione delle collisioni.

FUNZIONAMENTO: quando una stazione vuole trasmettere, ascolta se il canale è libero e se lo è trasmette la frame. Se nello stesso momento un' altra stazione trasmette, si ha una collisione e l' informazione viene persa; in caso di collisione la stazione prima di ritrasmettere attende per un tempo casuale (*exponential backoff*) compreso nell' intervallo di tempo $[0, 2^m - 1]$; dove $m = \min(n, 10)$ e n è il numero di collisioni consecutive avvenute.

il time slot equivale al tempo necessario per trasmettere una frame a minima lunghezza (512 bit).



4. Descrivi il funzionamento del frame 802.5 (token ring)



Il frame 802.5 (token ring) è un protocollo per l' accesso al canale ordinato in cui parla solo chi ha il token e sfrutta una topologia logica ad anello. Il token percorre l' anello e, quando una stazione vuole trasmettere:

- La stazione cattura il token;
- Man mano che il frame percorre l' anello, le stazioni leggono l' indirizzo MAC del destinatario, riportato nell' header, per dedurre se passarlo al livello di rete;
- I frame trasmessi sono ritrasmessi da ogni stazione e rimossi dall' anello dalla sorgente;
- Il token non può essere trattenuto oltre un tempo massimo dalla medesima stazione, per evitare di monopolizzare il canale.

Quando la frame ritorna al mittente, esso lo raccoglie e lo distrugge reimmettendo il token nell' anello.

===== PROTOCOLLI DI ACCESSO WIRELESS =====

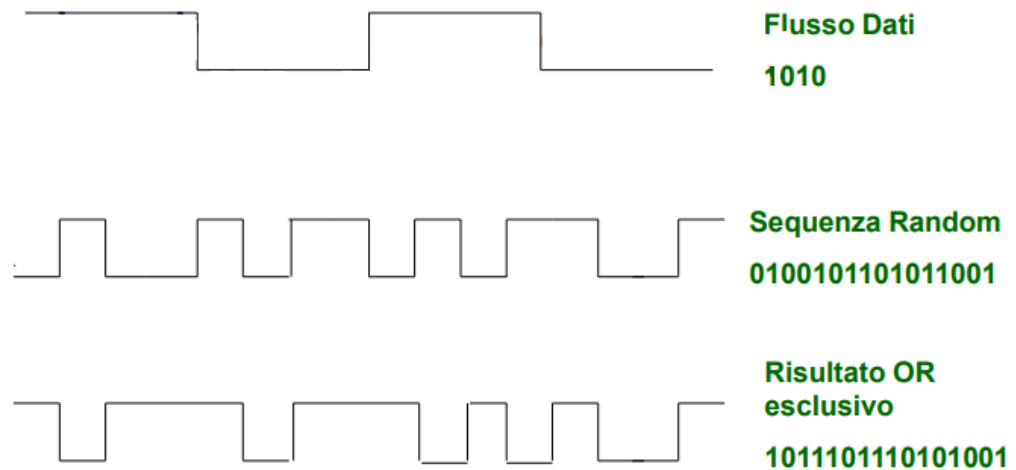
5. Come avviene la trasmissione Wi-Fi?

La trasmissione Wi-Fi può avvenire mediante 3 tecniche differenti:

- Frequency hopping: il messaggio è trasmesso su una sequenza random di frequenze. Utilizza 79 canali ognuno da 1MHz e salta da un canale ad un altro ogni 0,4 secondi. Mittente e destinatario sono sincronizzati e conoscono l' algoritmo di salto per ricevere tutte le frames in modo corretto. Se una frame viene persa, essa verrà ritrasmessa al prossimo *hop*.

- Direct sequence: il messaggio, prima di essere inviato, viene XORato con un numero casuale (generato da un generatore di numeri pseudo-casuali noto sia al mittente che al destinatario). I valori trasmessi, noti come *chipping sequence*, verranno ricevuti dal destinatario che ripeterà lo XOR;

Esempio: chipping sequence a 4 bit.



- Diffused infrared.

Le prime 2 tecniche trattate utilizzano un range di frequenza attorno ai 2,4 GHz e hanno l'obiettivo di multiplexare la frequenza e ridurre l'interferenza tra devices.

6. Descrivere come un device o nodo seleziona un access point e come si chiama tale tecnica la tecnica per selezionare l' access point è detta *scanning* e prevede 4 passaggi:

- Il nodo invia una frame di probe in broadcast (questo perché siamo nel livello 2);
- Tutti gli AP alla portata del nodo rispondono con una frame di risposta al probe;
- Il nodo seleziona l' AP con la migliore qualità del segnale e invia una frame di richiesta di associazione;
- L' AP risponde con una frame di *conferma di associazione*.

Lo scanning è usato anche quando il nodo vuole cambiare AP perché non più soddisfatto della qualità del segnale. In questo caso il nuovo AP invia una notifica del cambiamento al vecchio AP attraverso il *distribution system*.

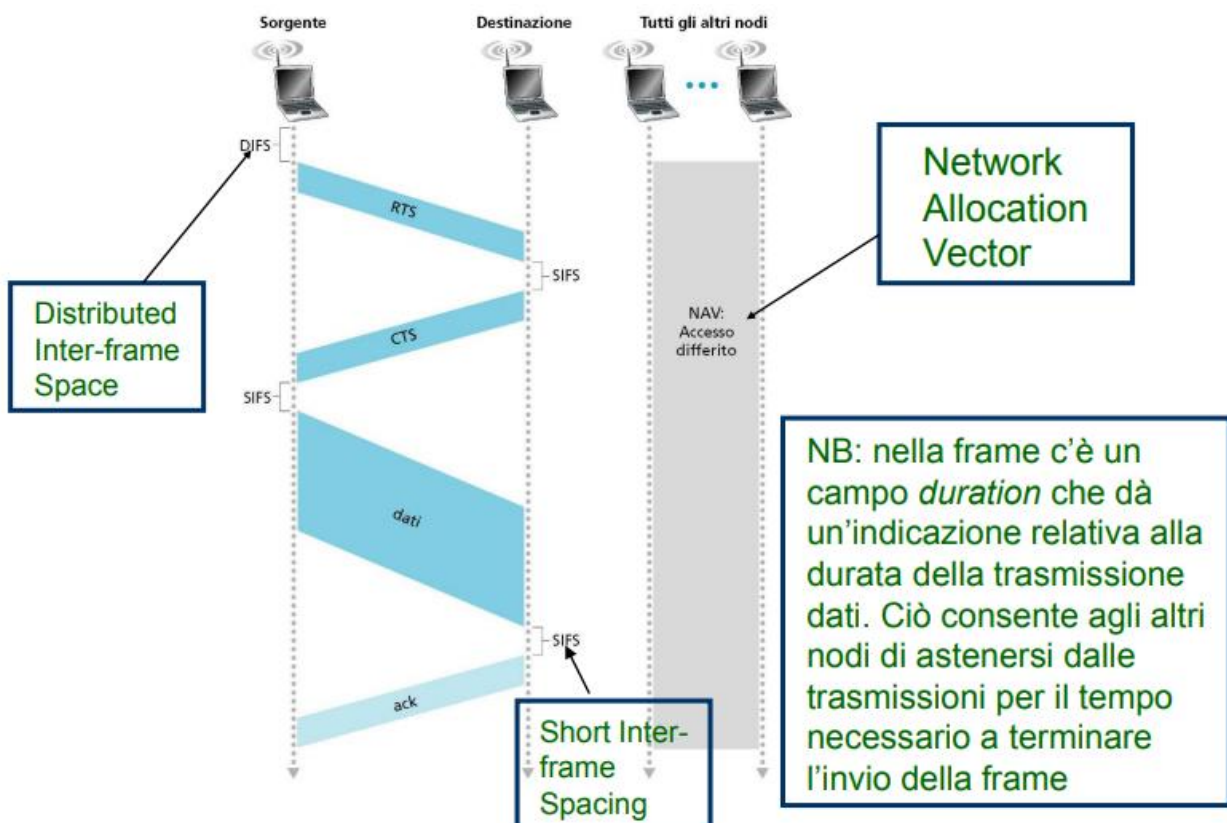
7. Come avviene l' accesso al canale nel Wi-Fi?

L' accesso al canale avviene in maniera simile all' Ethernet in quanto anche il Wi-Fi utilizza CSMA/CA. Prima della trasmissione ascolto se il canale è libero e in caso di collisione attendo per un tempo casuale (algoritmo di *Binary Exponential Backoff*). Collisioni che nel Wi-Fi sono molto più numerose a causa di nodi nascosti e nodi esposti.

8. Che cosa sono i nodi nascosti e i nodi esposti (o sovrapposti)? E come si risolve il problema delle collisioni a causa di questi tipi di nodi?

Un nodo si dice **nascosto** rispetto ad un nodo che sta trasmettendo se sente il CTS ma non l' RTS. Al contrario, un nodo è detto **sovrapposto** rispetto ad uno che sta trasmettendo se sente l' RTS ma non il CTS.

Per risolvere questa problematica sono stati introdotti 2 frame di controllo: RTS e CTS: un nodo, prima di trasmettere invia al destinatario un RTS (*Request To Send*) con all' interno un campo (NAV) nel quale è indicata la durata della conversazione. Il nodo destinatario in risposta, invia il CTS (*Clear To Send*) nel quale ricopia il NAV. Se un nodo sente il CTS ma non l' RTS, sa di essere vicino al ricevitore e per tutta la durata della conversazione non trasmette; un nodo che invece sente l' RTS ma non il CTS, sa di non essere vicino al ricevitore e quindi può trasmettere senza aspettare. Se ad un nodo arrivano 2 RTS contemporaneamente. Inoltre, un nodo capirà che c' è stata collisione se non ottiene CTS entro tempi brevi e quindi attenderà per un tempo casuale prima di inviare un altro RTS.



9. Indica quali sono le principali cause di interferenza nel Wi-Fi

Oltre alle interferenze dovute a fattori esterni (muri o oggetti metallici che fanno rimbalzare il segnale causando duplicazione o perdita del segnale), le principali cause di interferenza nel Wi-Fi sono la presenza di nodi esposti e sovrapposti.

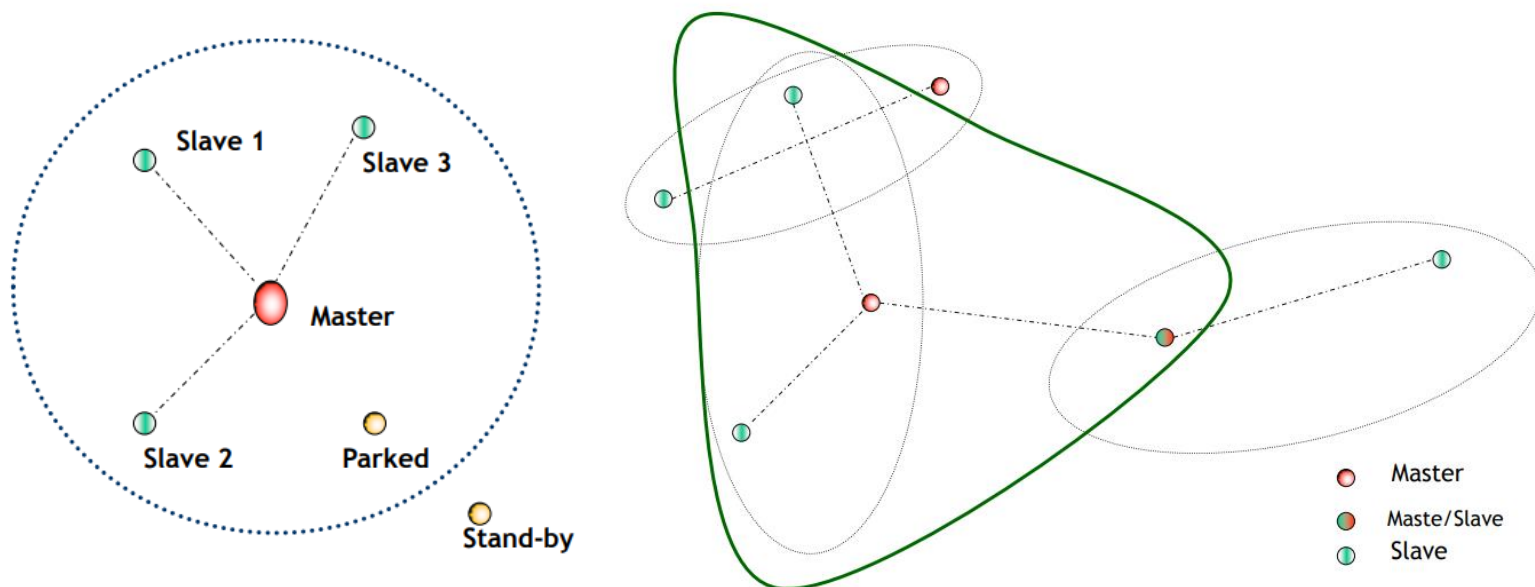
10. Come avviene la trasmissione nel Bluetooth?

La trasmissione nel Bluetooth avviene mediante Frequency Hopping: il messaggio è trasmesso su una sequenza random di frequenze. Utilizza 79 canali ognuno da 1MHz e salta da un canale ad un altro ogni 0,4 secondi. Mittente e destinatario sono sincronizzati e conoscono l'algoritmo di salto per ricevere tutte le frames in modo corretto. Se una frame viene persa, essa verrà ritrasmessa al prossimo *hop*.

11. Da cosa è costituita una Piconet? E che cos'è una Scatternet?

Una Piconet (immagine a sinistra) è una rete ad hoc, costituita al massimo da 8 devices di cui al più 1 master e 7 slaves. Il master è il device che inizia la connessione tra uno o più slaves e gestisce l'allocazione delle risorse. In una Piconet i ruoli di master e slave possono essere scambiati inoltre, un device che è master in una Piconet, può essere slave in un'altra. Vi possono essere infine 2 stati principali in una Piconet --> *Standby* e *connection* e 7 sottostati --> *Inquiry*, *Inquiry Scan*, *Inquiry response*, *Page*, *Page scan*, *Master response* o *Slave response*.

Una Scatternet (immagine a destra) è una rete nella quale 2 o più Piconets vengono collegate. In questo caso un device (master o slave) deve fungere da bridge tra le due piconets.



12. Come sono i collegamenti all' interno di una Piconets?

All' interno di una Piconet esistono due tipi di collegamenti:

- **Link SCO:** collegamento punto-a-punto tra un master e uno slave; venendo allocati degli slot, offre un servizio connection-oriented. SCO può essere considerato una connessione circuit-switched tra master e slave;
- **Link ACL:** collegamento punto-multipunto --> di natura broadcast. Non vengono allocati slot quindi offre un servizio connection-less. I pacchetti ACL non sono indirizzati verso uno specifico slave.

questo tipo di link viene utilizzato durante la procedura di Inquiry.

Entrambi i link sono gestiti dal livello Baseband.

===== RETE CELLULARE =====

13. Come fa una rete mobile ad avere copertura globale usando un set di frequenze finito e senza avere interferenza co-canale?

Si divide l' intero territorio in celle; in ogni cella c' è un' antenna e ad ognuna di esse è assegnato un set di frequenze. La dimensione delle celle dipende dalla potenza dell' antenna e dalla densità del traffico. Per evitare di avere interferenza co-canale tra due celle adiacenti si introduce il concetto di *cluster*. Un *cluster* è un insieme di celle all' interno del quale viene esaurito l' intero set di frequenze radio disponibili senza che si ripetano.

Per evitare che celle adiacenti appartenenti a cluster differenti abbiano la stessa frequenza, si introduce la distanza di riuso che corrisponde alla distanza tra i centri delle 2 celle in corrispondenza della quale è possibile riusare la stessa frequenza.

14. Che cos' è e a cosa serve il roaming

Il *roaming* è l' insieme delle funzioni con cui la rete mobile gestisce la mobilità degli utenti. Gli elementi che effettuano le funzioni di *roaming* sono:

- **HLR:** è un database unico per ogni provider e contiene i dati relativi ai propri clienti;
- **MSC:** è unico per ogni *Location Area* (o *LA* --> *insieme di celle entro cui il terminale non deve effettuare location update; LA non coincide con il cluster*). L' MSC gestisce il *Location Update*, l' *Handover* e la consegna della chiamata. Un MSC può gestire più LA;
- **VLR:** è un database associato a ciascun MSC che contiene i dati relativi che attualmente si trovano in quella LA.

Mobile Switching Center

Il roaming serve a localizzare l' utente, anche quando non ha chiamate in corso, al fine di ridurre i tempi di consegna della chiamata.

15. Descrivi la procedura di Location Update del roaming

La procedura di LU può essere descritta dal seguente elenco puntato

- Se l'utente si sposta da una cella ad un'altra, entrambe appartenenti alla stessa LA, non deve fare LU;
- Se l'utente si sposta da una cella ad un'altra appartenente ad una diversa LA ma gestita dallo stesso MSC, il device manda un messaggio di LU alla BS della nuova cella. La BS lo comunica all'MSC che aggiornerà la LA dell'utente nel VLR;
- Se l'utente si sposta da una cella ad un'altra di una diversa LA e gestita da un diverso MSC, il device invia un messaggio di Location Registration alla BS. La BS lo comunica all'MSC, l'MSC interroga il VLR il quale dirà all'MSC che l'utente non è presente nella propria memoria. A questo punto l'MSC chiederà all'HLR di fornirgli i dati relativi a quell'utente e l'HLR invierà i dati al nuovo MSC, informando il vecchio MSC di cancellare i dati relativi all'utente in questione. Alla fine di questo processo, il vecchio MSC invierà la conferma di cancellazione all'HLR.

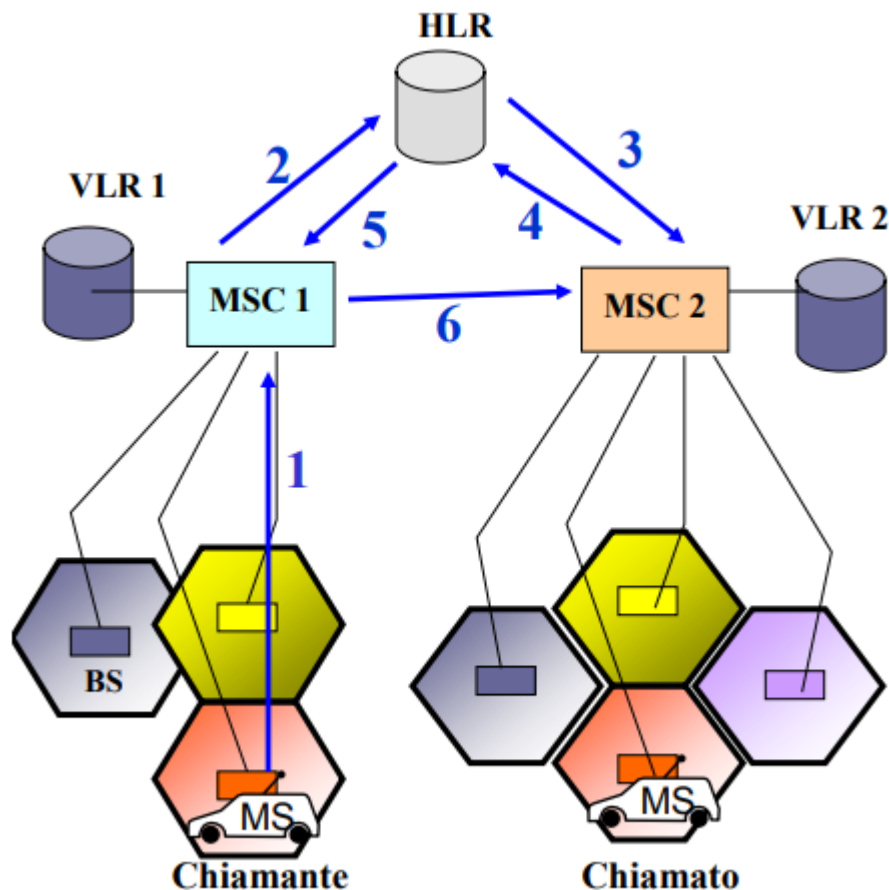
16. Quali tecniche esistono per migliorare il roaming?

Per migliorare il roaming esistono 5 tecniche:

- **A tempo:** il terminale comunica la propria posizione allo scadere di un timer, indipendentemente dal numero di celle attraversate;
- **A movimenti:** il terminale comunica la propria posizione dopo d passaggi di cella;
- **A distanza:** il terminale comunica la propria posizione quando si troverà in una cella distante D dall'ultimo luogo in cui ha comunicato la sua posizione;
- **Per-user location catching:** serve a ridurre il numero di messaggi scambiati in rete durante la procedura di consegna della chiamata. Ad ogni MSC viene associato un database (STP) nel quale sono riportati gli ID e i VLR degli ultimi utenti chiamati dagli utenti della LA. Quando viene effettuata una chiamata, l'STP controlla se l'utente è presente nella propria tabella; in caso affermativo, viene contattato direttamente il suo VLR, altrimenti si avvia la procedura classica (come quando un utente chiamato abbia cambiato MSC);
- **Pointer forwarding:** serve a ridurre il numero di messaggi scambiati in rete durante la fase di *Location Registration*. Quando un utente cambia MSC, non viene comunicato all'HLR ma viene settato un puntatore dal vecchio VLR al nuovo; nel momento di ricezione della chiamata, l'HLR controlla nel vecchio VLR che conterrà il puntatore al nuovo VLR (e così via). Per evitare catene di VLR troppo lunghe, si è fissato a 3 il numero massimo di puntatori.

17. Descrivi la procedura di consegna della chiamata

L'utente compone il numero e invia la richiesta al proprio MSC che, in base al prefisso, risale all'HLR del chiamato. L'HLR in questione contatta il proprio MSC e lo informa che l'utente sta per ricevere una chiamata. A questo punto l'MSC del chiamato verifica se l'utente è disponibile: se sì, gli assegna un numero temporaneo e lo comunica all'HLR. L'HLR quindi comunica la disponibilità all'MSC del chiamante che, dopo il *paging* (serve per identificare la cella del chiamato), realizza un circuito con l'MSC del chiamato attraverso la rete.



18. A cosa serve l' Handover?

L' Handover serve a supportare una chiamata mentre l'utente si sposta da una cella all'altra.

19. Descrivere la procedura di Handover

La procedura di Handover si sviluppa come segue:

- Durante la chiamata, la BS (o la Mobile Station), verifica che il rapporto *potenza segnale/potenza rumore* del canale *xxx* (quello su cui avviene la conversazione), non scenda sotto una certa soglia;
- Se scende sotto la soglia invia una richiesta di Handover al proprio MSC, inviandogli anche il livello del rapporto *segnale/rumore*;

- L' MSC invia in broadcast a tutte le BS delle celle adiacenti la richiesta di calcolare il rapporto *segnale/rumore* per il canale *xxx*;
- Le BS dopo averlo calcolato, inviano i risultati all' MSC, che sceglierà la nuova cella in base al valore migliore e il nuovo canale *yyy*;
- A questo punto la nuova cella attiva il canale *yyy*;
- L' MSC comunica sul canale *xxx* alla vecchia BS di commutare sul canale *yyy*; la vecchia BS lo comunica poi al mobile terminal e invia la conferma all' MSC che re instrada la conversazione verso la nuova cella;
- Il mobile terminal si sintonizza sul nuovo canale *yyy*;
- La vecchia BS disattiva il vecchio canale *xxx* e comunica all' MSC che ora *xxx* è libero;
- La comunicazione continua quindi su *yyy* e la nuova BS invia la conferma all' MSC.

20. Quanti tipi di Handover esistono?

Esistono 3 tipi di Handover:

- **Hard Handover:** se l' utente si sposta durante la conversazione, il terminale si attacca al nuovo canale solo dopo essersi staccato dal vecchio canale. --> Per qualche secondo la chiamata cade;
- **Seamless Handover:** si viene a formare un nuovo canale tra il terminale e la nuova BS durante la conversazione, prima della commutazione. Il terminale non si accorge del cambiamento della BS;
- **Soft Handover:** il terminale attiva il nuovo canale e per un breve lasso di tempo la chiamata avviene su entrambi i canali.

Oggi, grazie al CDMA (Code Division Multiple Access) si utilizza il soft handover.

21. Quali tecniche esistono per migliorare l' Handover?

Per migliorare l' Handover esistono diverse tecniche:

- **Guard Channel:** in ogni cella vengono riservati dei canali per le procedure di Handover. Questa procedura riduce la probabilità di *call drop* (caduta di chiamata) ma aumenta la probabilità di *call block* (blocco della chiamata), per questo non è utilizzata dagli operatori di rete;
- **Channel Borrowing:** prevede che l' MSC gestisca dinamicamente i canali delle proprie BS; preleva dei canali alle celle con minore densità di traffico e li assegna alle celle prossime alla saturazione --> Permette di sfruttare al meglio le risorse;
- **Per-user location caching:** l' obiettivo è quello di minimizzare il numero di messaggi che devono transitare in rete durante la procedura di consegna della chiamata;
- **Pointer forwarding:** l' obiettivo è quello di minimizzare il numero di messaggi che devono transitare in rete durante la fase di Location Registration.

22. Descrivi il protocollo CDMA

Il protocollo CDMA è un protocollo per l'accesso al canale. In questo modo, segnali che utilizzano la stessa frequenza, non fanno interferenza tra di loro in quanto il loro prodotto è 0. Un segnale infatti, è un vettore e questo implica che ha un'intensità, un verso e una direzione.

- **VANTAGGI:**

- i. Sicuro e difficile da decodificare;
- ii. Permette a stazioni base adiacenti di comunicare con lo stesso mobile (*soft-handoff*);
- iii. Non esiste un limite fisso sul numero massimo di stazioni;
- iv. Non v'è la necessità di realizzare una pianificazione di frequenza.

- **SVANTAGGI:**

- i. Di difficile realizzazione;
- ii. Richiede un controllo di potenza accurato in quanto tutti i ricevitori trasmettono sullo stesso canale;
- iii. Richiede la disponibilità di larghi tratti di spettro liberi.

23. Che cos'è il GPRS?

Il GPRS è una generazione di passaggio tra le reti GSM e l'UMTS. Serviva ad introdurre la commutazione di pacchetto; le reti GPRS infatti utilizzano una commutazione di circuito per la voce ed una commutazione di pacchetto per il dati (SMS).

24. Come avviene l'accesso al canale nelle reti GPRS?

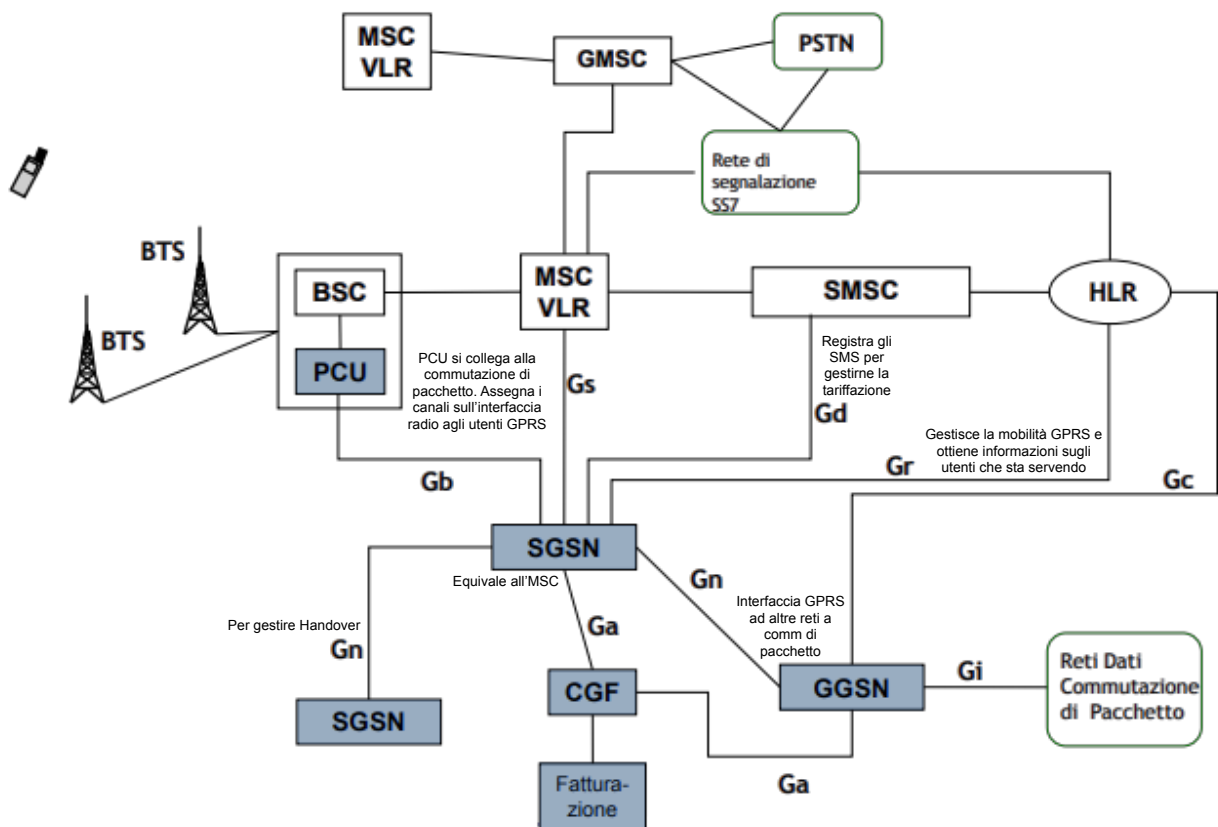
L'accesso al canale avviene in modo molto simile alle reti GSM con la differenza che in quest'ultime, ad ogni conversazione viene assegnata una frequenza per un *time-slot* e, una volta scaduto il *time-slot*, viene cambiata la frequenza. Nelle reti GPRS si utilizza invece il FDMA/TDMA; ciò significa che ad una trasmissione possono essere assegnati più *time-slot* consecutivi della stessa frequenza (fino ad un max. di 8) <--> Meno ritardo per cambiare frequenza.

25. In quante e in quali classi si dividono i terminali con l'introduzione del GPRS?

Con l'introduzione del GPRS i terminali vengono divisi in 3 classi:

- **Classe A:** terminali che supportano l'utilizzo simultaneo dei servizi dati e voce (un utente mentre sta chiamando può inviare e ricevere messaggi);
- **Classe B:** terminale che supportano la connessione simultanea alle reti GPRS e GSM, ma non l'utilizzo simultaneo;
- **Classe C:** terminali che non supportano la connessione simultanea alle reti GPRS e GSM (un utente che sta trasferendo dati risulta disconnesso dalla rete GSM e per tanto non è raggiungibile dalle chiamate e viceversa).

26. Descrivi l' architettura di rete delle reti GPRS



L' architettura di rete delle reti GPRS è molto simile all' architettura delle reti GSM per quanto riguarda la trasmissione della voce con la differenza che nelle reti GPRS sono stati aggiunti elementi per supportare la commutazione di pacchetto.

La BSS prevede 2 interfacce:

BSS insieme di BTS o BS (Base Station) e BSC (Base Station Controller)

- **A:** già presente nelle reti GSM, collega il BSC (Base Station Controller) al dominio a commutazione di circuito (MSC);
- **Gb:** collega la PCU al nodo SGSN. --> collega la PCU alla commutazione di pacchetto.

I nodi aggiunti per la gestione della commutazione di pacchetto sono:

- **Nodo PCU:** assegna i canali sull' interfaccia radio agli utenti GPRS. Questo nodo gestisce più BS;
- **Nodo SGSN:** è l' equivalente del nodo MSC nei domini a commutazione di pacchetto.

Questo nodo è collegato:

- Attraverso l' interfaccia **Gb** al PCU;
- Attraverso l' interfaccia **Gs** all' MSC relativamente a quegli utenti che supportano contemporaneamente i servizi a commutazione di circuito e commutazione di pacchetto;

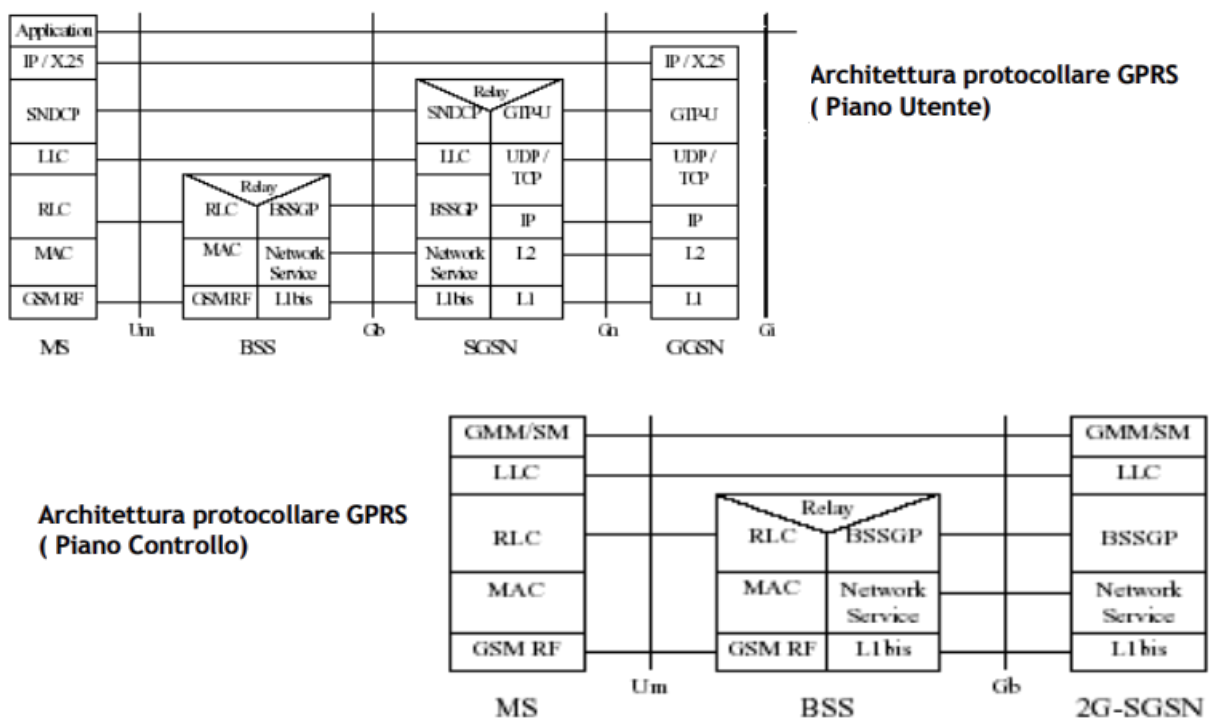
- Attraverso l' interfaccia **Gd** al SMSC che registra gli sms per gestirne la tariffazione;
- Attraverso l' interfaccia **Gr** all' HLR per gestire la mobilità GPRS e ottenere informazioni sugli utenti che sta servendo;
- Attraverso l' interfaccia **Gn** al GGSN che interfaccia la rete GPRS con altre reti a commutazione di pacchetto (es. Internet) ed a altri nodi SGSN per gestire l' handover.

27. A cosa serve il nodo SGSN?

Il nodo SGSN serve per gestire l' handover nel dominio della commutazione di pacchetto; è collegato ad altri nodi SGSN per velocizzare la procedura. Il roaming invece, è ancora gestito dall' MSC perché la voce viaggia ancora con commutazione di circuito.

28. Descrivi l' architettura protocollare del GPRS

L' architettura protocollare specifica l' insieme delle regole semantiche e sintattiche con cui i nodi comunicano tra loro. Nel GPRS l' architettura protocollare, oltre ad essere suddivisa in livelli, è suddivisa anche in 2 piani: **PIANO UTENTE** --> per la trasmissione delle informazioni tra utenti e **PIANO DI CONTROLLO** --> per la trasmissione di informazioni di controllo; l' architettura protocollare dei livelli inferiori è uguale a quella del **piano utente** mentre ai livelli superiori, il protocollo **SNDCP** è sostituito dal protocollo **GMM/SM** (utilizzato essenzialmente per funzioni di sicurezza, per gli aggiornamenti delle aree di copertura e per la gestione delle sessioni dati PDP),.



● 29. Descrivi le funzioni del sottolivello RLC/MAC

il sottolivello RLC/MAC costituisce il livello RR-Sublayer; questo livello svolge le procedure di gestione del sistema GSM e del sistema GPRS, riunite nel blocco RR-Management. Inoltre, è connesso al livello LLC attraverso il GRR.

● 30. Descrivi le funzioni del MAC

MAC ha principalmente 3 funzioni:

1. **Assegna le risorse radio:** l' assegnamento può essere di 2 tipi:
 - **Statico** --> nelle celle, alcuni time slot sono riservati esclusivamente per i servizi GPRS;
 - **Dinamico** --> i time slot vengono assegnati ai servizi GPRS solo se non utilizzati per chiamate vocali.
2. **Gestisce le procedure di:**
 - **Packet idle mode** --> il mobile non sta trasmettendo e non c' è quindi un collegamento logico tra l' RLC del mobile e quello della BSS. Il mobile non è raggiungibile e la rete può non conoscere la sua posizione nonostante sia comunque in ascolto dei canali di paging; i livelli superiori possono fare di passaggio nello stato di packet transfer mode attraverso l' invio di LLC PDU.
 - **Packet transfer mode:** il mobile ha un collegamento RLC con la BSS e può trasferire LLC PDU.
3. **Multiplexing di dati e controllo, gestione delle contese e delle priorità.**

31. Descrivi l' architettura protocollare dell' UMTS

L' architettura protocollare dell' UMTS introduce la commutazione di pacchetto sia per il trasferimento della voce che per quello dei dati. L' architettura generale è formata da *User equipment, Utran, Core Network*

31b. Che cos'è il dominio IM?

Il dominio IM (IP Multimedia) viene aggiunto nell'ultima versione del release dell'UMTS. In questo ultimo modello tutto viene portato su commutazione di pacchetto e vengono introdotti anche flussi di tipo multimediali. Il dominio IM si basa sul protocollo SIP (Session Initiation Protocol).

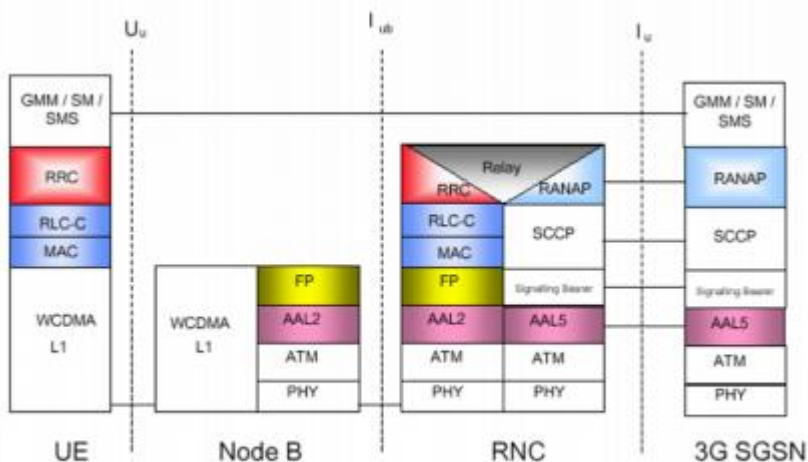


Figura 3.6 Architettura protocollare UMTS nel piano utente

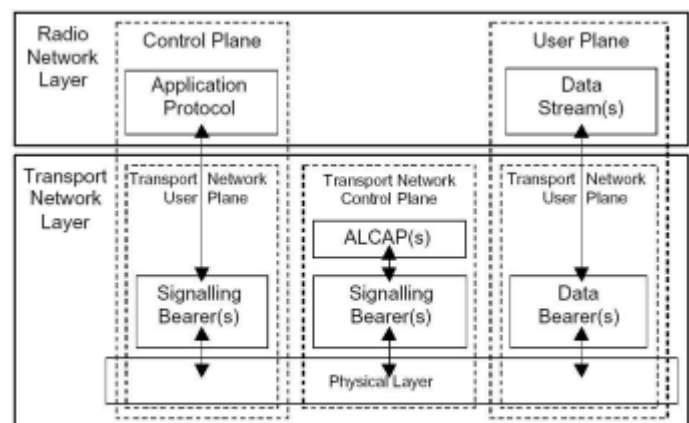


Figura 3.5 Modello protocollare per le interfacce UTRAN

32. Quanti e quali sono i requisiti che deve avere una rete wireless per essere considerata sicura?

Una rete deve avere 5 requisiti:

1. **Autenticazione:** "A è veramente A??" --> è garantito con servizi connection-oriented (password, challenge-response) o con servizi document-oriented (firme digitali, *token*);
2. **Confidenzialità:** i messaggi scambiati tra A e B devono essere letti solo da A e B. --> è garantito con algoritmi che utilizzano chiavi segrete simmetriche (crittografia e de-crittografia con la stessa chiave – es. **DES**) o chiavi pubbliche (crittografia con chiave pubblica e de-crittografia con chiave privata);
3. **Integrità:** il messaggio ricevuto non deve essere stato contraffatto --> è garantito attraverso algoritmi che utilizzano chiavi segrete simmetriche o chiavi pubbliche (– es. **DES**);
4. **No-Repudiation:** nessuno può rinnegare la paternità del documento --> è garantito con le firme digitali (crittografia con chiave privata e de-crittografia con chiave pubblica es. **RSA, DSA**);
5. **Autorizzazione:** per accedere alle risorse bisogna essere autorizzati (controllo di accesso).

33. Che cos' è il WEP?

WEP (Wired Equivalent Privacy) è stato il primo protocollo per garantire la sicurezza nelle reti wireless. Esso garantiva un livello di sicurezza pari a quello delle wired LAN. Per le operazioni di encryption utilizza l' RC4 a chiave segreta simmetrica mentre per l' integrità utilizza CRC-32. WEP non garantisce una sicurezza end-to-end ma solo a livello *data link*.

34. Come avviene l' autenticazione nel WEP?

Nel WEP l' autenticazione può avvenire per:

1. **Identity based:** è un metodo non crittografico e può essere:
 - o *open system authentication* (una stazione può fornire una *stringa vuota* come SSID per unirsi alla rete --> sicurezza = 0);
 - o *closed system authentication* (una stazione deve fornire un *SSID valido* per l' access point per potersi unire alla rete).
2. **Challenge-response:** è un metodo crittografico (la stazione può unirsi alla rete solo se condivide la chiave con l' access point).

35. Come funziona il challenge-response?

Il challenge-response è composto da 4 passi:

1. La stazione richiede all' AP di potersi connettere alla rete;
2. L' AP genera un numero casuale (challenge) e lo invia alla stazione;
3. La stazione lo cripta utilizzando la chiave segreta e lo rinvia all' AP;

4. L' AP lo decripta con la stessa chiave e verifica se il risultato è uguale al numero inviato inizialmente e, in caso affermativo, conferma l' accesso alla stazione.

36. Come viene garantita la confidenzialità nel WEP?

Il WEP utilizza l' algoritmo RC4 a chiave segreta simmetrica. Per evitare di criptare con la stessa chiave tutti i *payloads*, utilizza un *initialization vector*, ovvero un campo di 24 bit con cui concatenare la chiave (mediante l' RC4) e ottenere così chiavi diverse per criptare e decriptare. Il *payload* --> dato in chiaro <--, viene concatenato ad alcuni bit di controllo generati dal CRC-32, formando il *plain text*. Il *plain text* viene XORato con il risultato dell' RC4 generando così una nuova chiave; il risultato che viene inviato prende il nome di *cyphertext*.

37. Come viene garantita l' integrità nel WEP?

Per garantire l' integrità si utilizza CRC-32; esso genera dei bit di controllo che vengono criptati assieme al *payload*. CRC-32 è un algoritmo lineare: questo significa che se un hacker intercetta un frame, modifica il contenuto dei *payload* e ne sistema la *checksum*, il dato finale appare corretto.

38. Quali sono le debolezze del WEP?

Le principali debolezze del protocollo WEP sono:

1. Utilizza una *chiave simmetrica*;
2. L' *initialization vector* è un campo troppo corto: questo significa che dopo un certo tempo, *le chiavi si ripetono* --> un hacker potrebbe quindi trovare due *cyphertext* criptati con la stessa chiave risalendo quindi al *plain text* (IV collision);
3. *Known-plaintext* dovuto all' IV collision --> basta infatti fare lo XOR di due *cypher-text* criptati con la stessa chiave per conoscere il *plain text*.

Un possibile rimedio sarebbe quello di aggiornare la chiave ogni 5 ore, cosa non possibile in quanto le chiavi crittografiche sono condivise e non possono essere aggiornate automaticamente e con frequenza.

Infine, l' integrità è garantita in maniera superficiale e l' autenticazione non è richiesta se non tramite SSID.

39. Descrivi l' evoluzione dei protocolli di sicurezza

WEP --> WEP 2:

1. **WEP 2** utilizza una chiave a 128 bit invece che a 40 bit;
2. Persistono i problemi di WEP:
 - Non estende l' IV;
 - *Known-plaintext* ancora possibili;
 - Non c' è mutua autenticazione Client-Server.

WEP 2 --> IEEE802.1x:

3. Introduce l' EAP (Extensible Authentication Protocol) per gestire la mutua autenticazione;
4. Implica generazione e distribuzione dinamica delle chiavi.

IEEE802.1x --> IEEE802.11i:

5. Utilizza l' EAP per gestire la mutua autenticazione;
6. Utilizza il TKIP (Temporal Key Integrity Protocol) per generare una chiave temporanea a 128 bit ed estende l' IV (initialization vector) con regole di sequenza;
7. È un algoritmo temporaneo che utilizza chiavi di diversa lunghezza (128, 192, 256);
8. Sostituisce l' RC4 con l' AES

IEEE802.11i --> WPA: deriva da IEEE802.11i

9. Include il TKIP;
10. È applicato a SOHO (Small Office And Home), public access e Enterprise.

40. Descrivi il funzionamento di WPA per SOHO

WPA per SOHO lavora utilizzando "pre shared key" ; il meccanismo utilizzato è il seguente:

1. L' home user inserisce la master key per accedere all' AP/home wireless gateway;
2. WPA procede automaticamente: TKIP utilizza la master key solo nella fase iniziale di autenticazione dalla quale deriva matematicamente la chiave da utilizzare per le operazioni di encryption;
3. A questo punto TKIP cambia le chiavi in modo che una stessa chiave non venga utilizzata due volte. Tutto ciò avviene in background in modo trasparente all' utente.

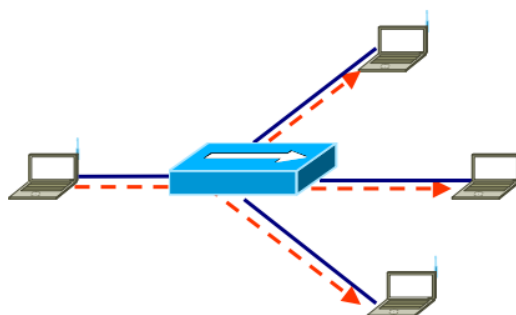
41. Illustra le differenze tra WEP e WPA

Le principali differenze sono:

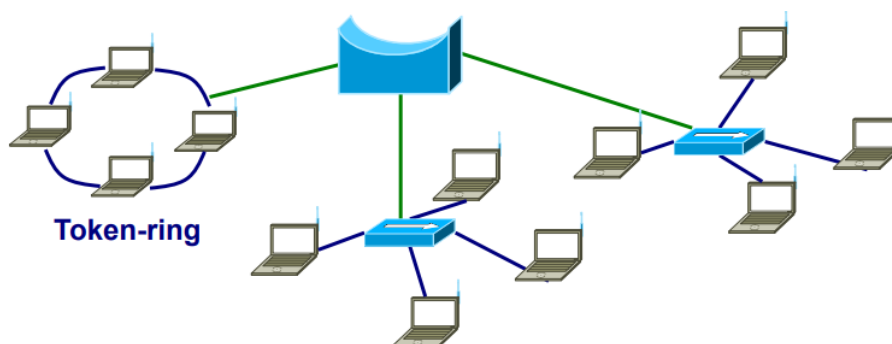
1. **WEP:**
 - Utilizza chiavi a 40 bit;
 - È un protocollo che utilizza una chiave simmetrica statica;
 - L' autenticazione avviene utilizzando la stessa chiave.
2. **WPA:**
 - Utilizza chiavi a 128 bit;
 - È un protocollo che utilizza una chiave segreta dinamica;
 - L' autenticazione avviene tramite EAP.

42. Descrivere brevemente i dispositivi di relaying

- **HUB:** opera a **livello 1**; l' HUB viene utilizzato per realizzare topologie a bus mediante una topologia a stella e questo, garantisce una maggiore affidabilità. Le informazioni che riceve su una porta vengono replicate sulle altre. Le stazioni sono collegate mediante cavi UTP.



- **BRIDGE:** opera a **livello 2**; il BRIDGE è usato per collegare reti LAN (anche con topologie differenti) inoltre, inoltra le informazioni sulla base dell' indirizzo MAC utilizzando **MAC table** (contenente *indirizzo MAC, porta e tempo*) inizialmente vuote e riempita in funzione dei frame in transito;



- **SWITCH:** opera anch' esso a **livello 2**; collega LAN omogenee e inoltre, abilita la comunicazione *full-duplex* --> **NESSUNA COLLISIONE**. Può essere SWITCH centrale o SWITCH di piano e ha 3 modalità di funzionamento:
 - **Store & Forward** --> lo switch riceve il frame, **controlla il CRC** per individuare eventuali errori; se non ce ne sono, lo memorizza nel buffer associato alla porta di uscita trasmettendolo quando la linea si libera;
 - **Cut & Through** --> lo SWITCH controlla solo che non ci siano **errori** nell' *header* e poi lo inoltra;
 - **Fragment Free** --> lo SWITCH controlla solo i primi **64 Byte**, se il frame non li occupa tutti viene scartato, altrimenti viene inoltrato.

- **ROUTER:** opera a **livello 3**; è un dispositivo di rete che, in una rete informatica a commutazione di pacchetto, si occupa di instradare i dati, suddivisi in pacchetti, fra sotto-reti diverse;
- **GATEWAY:** è un dispositivo di rete che **collega 2 reti informatiche di tipo diverso operando al livello di rete e superiori**. Il suo scopo principale è quello di veicolare i pacchetti di rete all' esterno della rete locale.

43. Descrivi il protocollo spanning tree

È un **protocollo utilizzato** per evitare che si formino anelli di BRIDGE e quindi **per evitare che un frame rimbalzi da un BRIDGE all' altro entrando in un loop**.

Realizza un albero di attraversamento in cui **ogni BRIDGE ha un ID univoco (ID = BRIDGE priority + MAC address)** e si definisce *root BRIDGE* dell' albero, il BRIDGE con ID più basso. Le porte di un BRIDGE si dividono in:

- **root:** porta nella quale si ricevono i frame provenienti dal *root BRIDGE*;
- **designated:** porta dalla quale deve essere inoltrato il frame per raggiungere la destinazione;
- **blocked:** porta bloccata.

Lo spanning tree si realizza mediante lo **scambio di BPDU** (Bridge Protocol Data Unit) che è **composto da 3 campi**:

- **ID BRIDGE** che ha emesso la BPDU;
- **ID del root BRIDGE** secondo il BRIDGE che ha emesso la BPDU;
- **Costo** in numero di LAN attraversate per passare da C1 a C2.

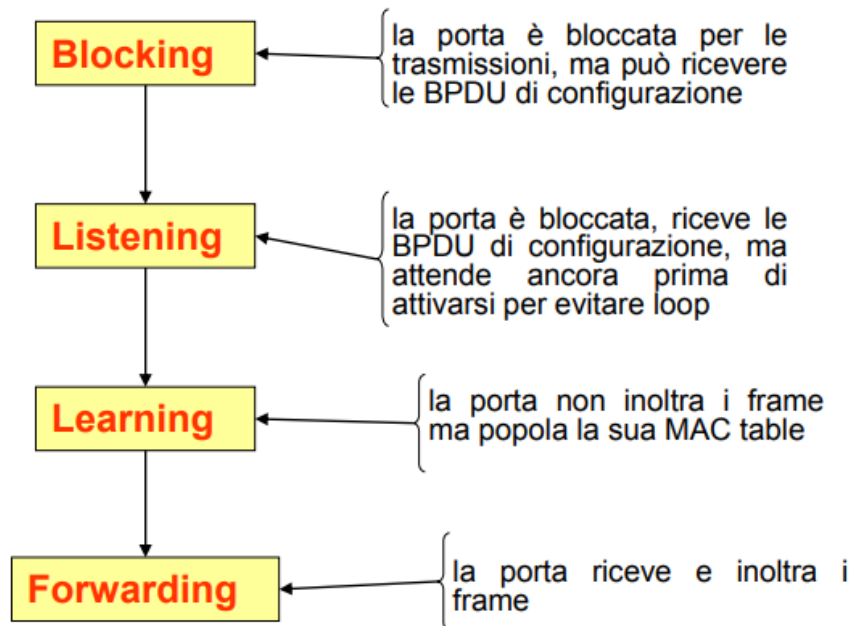
Inizialmente ogni BRIDGE si elegge *root BRIDGE* ed emette BPDU con $C1 = C2 = \text{ID proprio}$ e $C3 = 0$. Quando riceve una BPDU, il BRIDGE controlla se $C2$ è $<$ del proprio ID: in caso affermativo smette di trasmettere la propria BPDU ed etichetta con R la porta dalla quale ha ricevuto la BPDU. A questo punto ritrasmette la BPDU ricevuta sostituendo $C1$ con il proprio ID ed incrementando $C3$. Alla fine ci sarà un solo *root BRIDGE* con tutte le porte etichettate con D e gli altri BRIDGE avranno la porta dalla quale hanno ricevuto la BPDU con $C2 = \text{ID root BRIDGE}$ e con il più piccolo valore di $C3$ etichettata con R.

Per eliminare il loop basterà etichettare tra tutte le porte che si affacciano su un segmento LAN, una con D e le altre con B. Per scegliere quale porta etichettare con D, i BRIDGE ritrasmettono le BPDU di configurazione --> se su una LAN si affacciano più BRIDGE, questi riceveranno più BPDU da porta non *root* (R) e, se il valore di $C3$ della BPDU ricevuta è $<$ di $C3$ della BPDU che emette, allora etichetterà la porta dalla quale ha ricevuto la BPDU con B, altrimenti la etichetterà con D.

Quando un BRIDGE non riceve BPDU da una porta, significa che è l' unico BRIDGE ad affacciarsi su quel segmento LAN e quindi etichetterà la sua porta con D.

44. Quali sono gli stati intermedi per passare da B a D (in riferimento al funzionamento dello spanning tree protocol)?

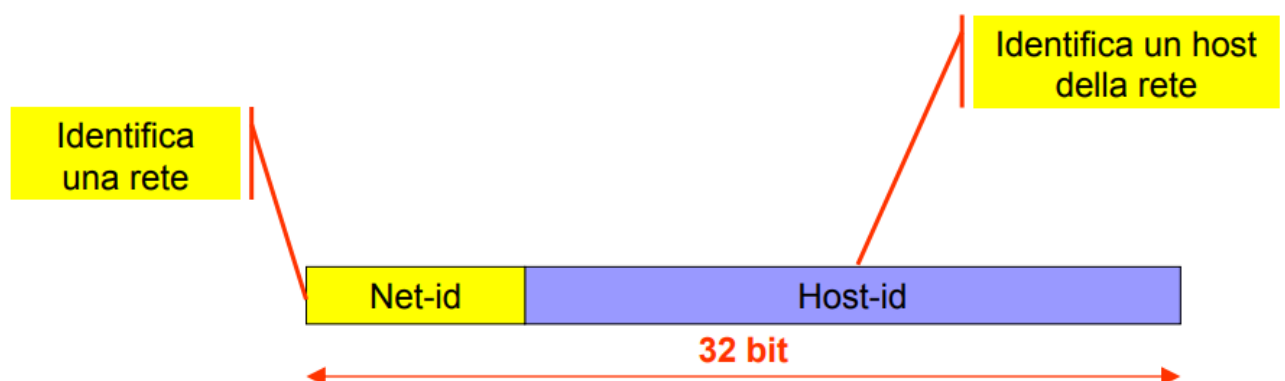
Per passare da B a D vi sono diversi stati intermedi:



Questi passaggi avvengono, ad esempio, quando si cambia la topologia.

45. Descrivi il protocollo IP

Il protocollo IP è il protocollo responsabile dell' instradamento delle informazioni immesse nella rete e fornisce un servizio inaffidabile non orientato alla connessione; ogni nodo della rete è identificato da almeno un indirizzo IP e, nelle PDU di livello 3 sono contenuti gli indirizzi IP dell' host mittente e destinatario.



L' indirizzo IP è un campo composto da 32 bit ed espresso in forma decimale puntata; la prima parte individua la rete, la seconda individua la sottorete (se c' è), mentre l' ultima parte identifica l' host della rete ($rete + sottorete = subnet\ mask$). Gli indirizzi IP sono assegnati da

un ente chiamato IANA (**Internet Assigned Numbers Authority**) e vengono suddivisi in 4 categorie:

- **Pubblici:** utilizzati per instradare i pacchetti in internet. Può essere utilizzato esclusivamente da una specifica organizzazione
- **Privati:** possono essere usati solo in una rete privata e non possono essere usati per instradare i pacchetti in internet;
- **Statici:** l' IP dell' host non varia nel tempo;
- **Dinamici:** l' IP dell' host varia nel tempo (es. connessione non permanente ad internet tramite ISP).

Nel datagramma IP è specificata: la versione (IPv4, IPv6), la lunghezza dell' header, il TOS che analizza la qualità del servizio, la lunghezza totale del datagramma, il flag (quando è **DF**, il datagramma non è frammentato, quando è **MF**, devono arrivare altri frammenti), il TTL (Time To Live) che all' inizio vale 128 e ad ogni *hop* si decrementa fino ad arrivare a 0 --> il datagramma viene scartato --> questo serve ad evitare che il pacchetto resti troppo sulla rete, il tipo di protocollo usato dall' applicazione (TCP o UDP), header checksum per controllare gli errori nell' header, l' indirizzo IP del mittente e l' indirizzo IP del destinatario.

46. A cosa serve il DHCP (Dynamic Host Configuration Protocol) e lo ZCN (Zero Configuration Networking)?

il DHCP consente ad un host di ottenere da un DHCP server un indirizzo IP privato, l' indirizzo IP del router di default o l' indirizzo IP del server DNS. L' host invia in broadcast sulla rete locale la richiesta e il primo server DHCP che riceve la richiesta fornisce l' indirizzo.

Lo ZCN invece è utilizzato nelle piccole reti dove non ci sono DHCP server o DNS server; serve per assegnare un indirizzo IP ad un host che si connette a tale rete. Il suo funzionamento è il seguente:

- L' host che si collega alla rete, necessita di un indirizzo IP privato e utilizza lo ZCN per ottenerlo;
- Lo ZCN seleziona un indirizzo IP casuale dal set di indirizzi che possiede (forniti dallo IANA), dopodiché invia in broadcast, nella rete locale, un *ARP probe* per verificare che l' indirizzo IP sia libero;
 - Nell' *ARP request* è indicato: **sender IP address** (tutti 0), **target hardware address** (tutti 0), **target IP address** --> l' indirizzo da verificare;
- Se è libero si comunica tale indirizzo attraverso un *ARP announcement* con sender IP address = target IP address = IP scelto.

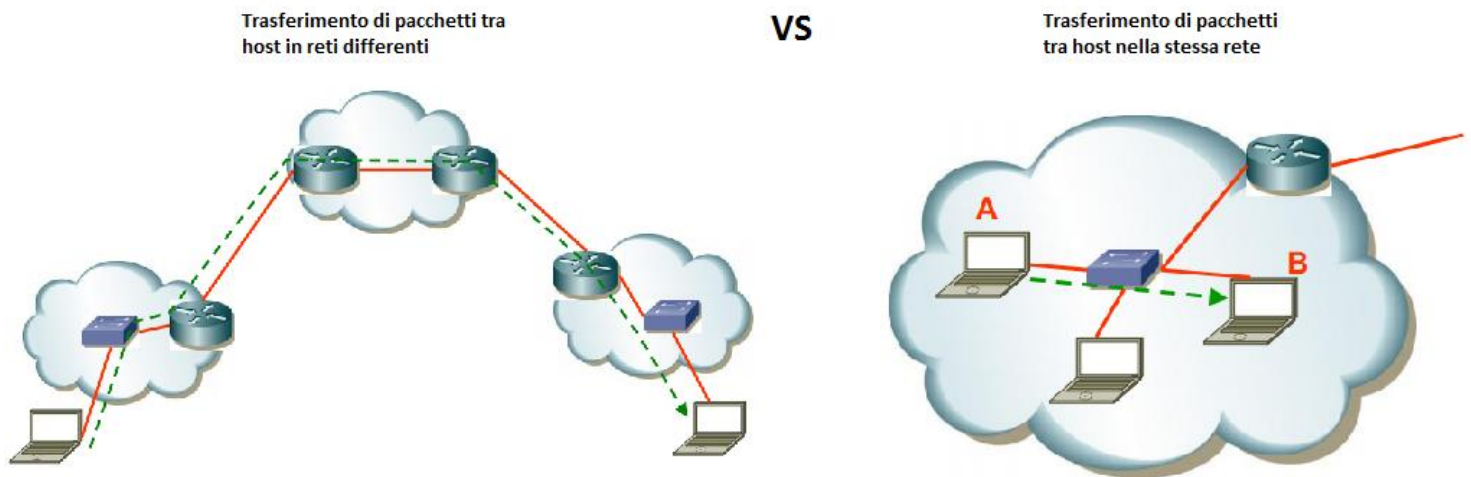
47. Che cos' è l' ARP?

ARP è l' acronimo di **Address Resolution Protocol** ed è un protocollo utilizzato per conoscere l' indirizzo MAC di una macchina corrispondente ad un determinato indirizzo IP. Se l' host A vuole conoscere il MAC address di un host B, esso invierà in **broadcast**, sulla rete locale, un **ARP**

probe indicando l' indirizzo IP dell' host B, il quale risponderà con un *reply unicast* indicando ad A il proprio MAC address.

48. Come funziona il trasferimento dei pacchetti sulla stessa rete? E come funziona su reti differenti?

Per il trasferimento di pacchetti sulla stessa rete si risale sino al Liv. 2 per conoscere il MAC address del destinatario; mentre quando si devono trasferire pacchetti su reti differenti, occorre conoscere l' indirizzo IP del destinatario.



49. Che cos' è il NAT? E quali funzioni svolge?

Il NAT è un software installato sul router di frontiera che utilizza una tabella di traduzione per tradurre un indirizzo IP privato in indirizzo IP pubblico per i pacchetti in uscita e selezionare un *host* dalla rete locale (indirizzo IP privato) in base ad un indirizzo pubblico per i pacchetti in entrata.

Se all' interno della LAN è presente un server, il NAT è detto **statico** --> il NAT invia i pacchetti al server e il server li smista agli host alleggerendo il compito al NAT. I compiti e usi del NAT sono:

- **Pooling of IP address:** il NAT possiede infatti un indirizzo IP pubblico per gestire più *host*;
- **Supporta la migrazione tra internet providers:** semplicemente aggiornando la lista degli indirizzi pubblici che possiede;
- Nel caso ci siano più *host* che indirizzi IP pubblici disponibili, il **NAT mappa più indirizzi IP privati con lo stesso indirizzo IP pubblico** aggiungendo alla mappatura il numero di porta;
- **Bilancia il carico di lavoro ai server:** ogni server possiede un IP privato; se arrivano molte richieste ad un solo server, il NAT può modificare l' indirizzo IP di destinazione e inviare il pacchetto ad un altro server che lavora sulla stessa rete.

Diremo infine che *host* di due reti diverse non comunicano tra di loro perché le informazioni passano per il NAT.

===== ALGORITMI DI ROUTING =====

50. A cosa servono gli algoritmi di routing e com'è la loro tassonomia?

Gli *algoritmi di routing* servono ad individuare il percorso migliore per instradare i pacchetti in internet. Possono essere:

- **Senza tabella:** per esempio: *random, flooding, source routing*;
- **Gerarchici**;
- **Con tabella:** i quali si dividono in:
 - **Statici**;
 - **Dinamici:** possono essere di tipo *vektor* oppure *link state*. (Sono i maggiormente utilizzati);

51. Spiegare il funzionamento di un router

Ogni router consulta la propria tabella di routing per scegliere verso quale porta instradare il datagramma; nella tabella di routing è indicato l' **indirizzo IP di destinazione**, il **costo** (calcolato in base ad alcune metriche tipo: *banda disponibile, ritardo, carico di lavoro* degli elementi di rete come router o link, *tasso di errore* di ogni singolo link, *hop count* --> ovvero il numero di router che il pacchetto deve attraversare prima che arrivi a destinazione) e la **linea di uscita** (*next hop*). La linea di uscita viene calcolata in base in base agli algoritmi di routing. Quando un router riceve un datagramma, esso ricerca all' interno della propria tabella, una *entry* con lo stesso indirizzo IP del destinatario del datagramma ricevuto: se la entry corrisponde ad una rete connessa al router ne viene individuata la sottorete e il datagramma viene inoltrato; se invece non vi è nessuna entry con lo stesso indirizzo IP, il datagramma viene inoltrato verso il *default route*.

52. Spiegare gli algoritmi di routing

L' insieme dei router amministrati dallo stesso gestore prende il nome di **AS** (Autonomous System). Gli algoritmi di routing si dividono in:

- **Intra AS:** ovvero quelli che individuano il percorso migliore all' interno dello stesso AS;
- **Inter AS:** ovvero quelli che individuano il percorso migliore tra diversi AS.

Tra gli algoritmi **intra AS** troviamo:

- **RIP:** è un algoritmo di routing con tabella dinamico di tipo distance vector ovvero, ogni router invia periodicamente o ad ogni cambiamento topologico la propria tabella di routing ai router vicini i quali, scelgono il percorso migliore confrontando i distance vector ricevuti. **RIP** è adatto a piccole reti ed utilizza come metrica gli hop count. Il valore massimo è 15, il valore 16 invece indica "rete irraggiungibile" (evita il counting to infinity). Per quanto riguarda il funzionamento del **RIP**, ogni router invia la propria

tabella ogni 30s o ad ogni cambiamento topologico e l' hold down counter è fissato a 120s (significa che se un pacchetto ci impiega più di 120s ad arrivare a destinazione, la entry è cancellata dalla tabella). Il protocollo utilizzato da **RIP** è l' UDP inoltre, ne esistono 2 versioni differenti a seconda del formato dei pacchetti.

- **OSPF**: è un algoritmo di routing con tabella dinamico di tipo link state. Con **OSPF** ogni nodo conosce la topologia della propria area; il miglior percorso è calcolato attraverso l' algoritmo di *Dijkstra*. Con l' **OSPF** l' AS viene suddiviso in 4 aree e i router in 3 tipologie:

- **Internal router**: quelli con interfacce solo verso l' interno della propria area;
- **Area border router**: quelli che hanno un' interfaccia verso la *backbone area*;
- **Boundary router**: quelli che hanno un' interfaccia verso la rete esterna.

Periodicamente ogni nodo invia lo stato dei suoi collegamenti (*link state advertisement*) inoltre, i pacchetti tra due aree diverse transitano nella *backbone area* attraverso gli *area border router* e al fine di far sì che i router conoscano la topologia della propria area.

I pacchetti **OSPF** sono incapsulati in pacchetti IP.

Per quanto riguarda invece gli algoritmi **inter AS**:

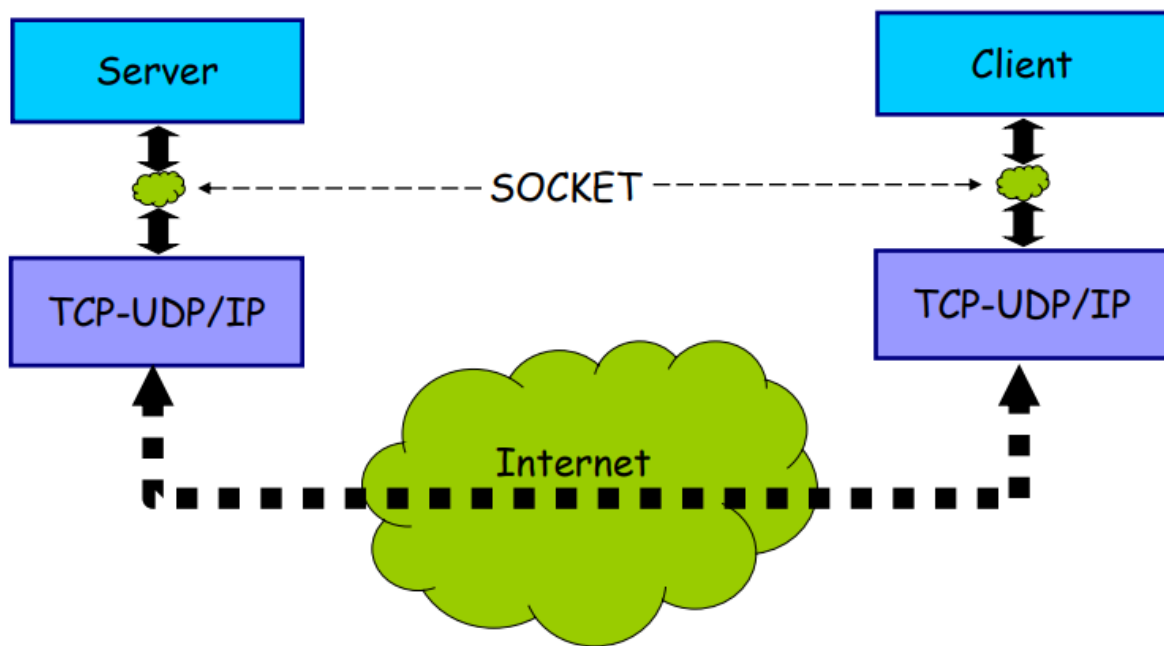
- **BGP**: è un algoritmo di routing con tabella dinamico. Esso consente di scambiare informazioni per l' instradamento tra router di diversi AS, utilizzando il protocollo TCP per lo scambio di messaggi. Ogni router di frontiera comunica la sua disponibilità ad accettare tabelle di routing contenenti, per ogni rete raggiungibile, la sequenza di AS da attraversare.

53. Come si crea una socket?

Una socket è un' interfaccia tra l' *application level* e il *transport level*; per crearne una, occorre che l' applicazione specifichi:

1. n° di porta del *localhost*;
2. l' indirizzo IP del *localhost*;
3. n° di porta dell' host remoto;
4. l' indirizzo IP dell' host remoto;
5. il protocollo di trasporto;
6. opzioni aggiuntive.





===== LIVELLO 4: TCP =====

54. Descrivi il protocollo TCP e indica a cosa serve il controllo di flusso

TCP, acronimo di Transmission Control Protocol, è un protocollo che offre un servizio affidabile **connection oriented**. Le connessioni sono **full-duplex** e garantisce: **controllo di flusso** (*per garantire che una sorgente veloce non possa sommergere un ricevitore lento con una quantità di messaggi superiore a quelli che sa gestire*), **controllo di congestione**, **consegna ordinata dei pacchetti** e **ritrasmissione dei pacchetti persi**; inoltre garantisce la **conferma di avvenuta ricezione** attraverso ACK. Nel segmento TCP è contenuto:

- Il n° di porta del localhost;
- Il n° di porta dell' host remoto;
- Il n° di sequenza del segmento;
- Il n° di sequenza del prossimo segmento;
- La lunghezza dell' header;
- I **flags**:
 - URG se il segmento contiene dati urgenti;
 - ACK se il segmento contiene informazioni di riscontro;
 - SYN per stabilire una connessione;
 - FIN per interrompere una connessione.
- AW (Advertised Window): utilizzata per il controllo di flusso, indica lo spazio disponibile nel buffer del ricevitore; questo valore è aggiornato ad ogni ACK ricevuto;
- Checksum;
- Urgent pointer.

55. Descrivi il processo di creazione e di interruzione di una connessione TCP

Per la creazione di una connessione, il client invia un segmento TCP al server con indicato il **numero di sequenza del segmento** (ad es. x) e con il campo **flags** settato a SYN. Il server risponde con un SYN + ACK nel nuovo segmento (ad es. $nr y$) e comunica al client di essere in attesa del segmento ($x + 1$). Il client risponde con un ACK nel segmento ($x + 1$) e comunica al server di essere in attesa del segmento ($y + 1$). Questa procedura prende il nome di **three way handshake**. Per il rilascio della connessione invece, il client invia al server un segmento con **flags** settato a FIN; il server, di conseguenza risponde con un ACK e con un altro segmento settato a FIN. Infine il client risponde con un ACK.

56. Indica come avviene la trasmissione dei segmenti in una connessione TCP e a cosa serve la sliding window

La **sliding window** è il meccanismo che regola il traffico, ovvero il *rate di trasmissione* dei segmenti. È utilizzata per gestire il controllo di flusso e di congestione: il controllo di flusso regola il rate di trasmissione in funzione della dimensione del buffer del ricevitore, mentre il controllo di congestione regola il rate di trasmissione in funzione del traffico nella rete. **Sliding window** è una finestra dinamica e il suo valore indica quanti pacchetti per volta inviare prima di verificare se tutti sono giunti a destinazione. La dimensione (il suo valore), è pari al minimo tra il valore dell' *advertisement window* e della *congestion window* -->

$W = \min(AW, CW)$, dove:

- Il valore AW è comunicato ad ogni ACK ricevuto e rappresenta il limite superiore della sliding window,
- Il valore CW è calcolato da un algoritmo di controllo di congestione. Questo algoritmo, prevede 2 fasi:
 - **Additive increase**: incrementa progressivamente la CW fino a quando non si verifica congestione;
 - **Multiplicative decrease**: riduce drasticamente la dimensione della CW dopo che si è verificata congestione (ovvero quando si ricevono 3 ACK duplicati oppure allo scadere di un *retransmission time out RTO*).

Con il meccanismo di **sliding window** vengono inviati n pacchetti per volta prima di controllare se tutti sono giunti a destinazione. La ritrasmissione dei pacchetti avviene quando si ricevono 3 ACK duplicati oppure allo scadere di un RTO --> non attendo i 3 ACK duplicati ma ritrasmetto allo scadere del timer.

Cos'è il meccanismo di sliding window (o descrivere)

Il meccanismo di sliding window stabilisce il rate della trasmissione, ossia il numero di pacchetti che possono essere inviati senza riscontro, cioè senza attendere conferma (ACK).

La finestra è self-clocking, cioè che la finestra avanza autonomamente man mano che riceve gli ACK, quindi conta da sola i pacchetti inviati. La sua dimensione è variabile durante tutta la trasmissione: dipende dalla congestione. Finché non vengono ricevuti tutti gli ACK, la finestra non va avanti. Se si riceve per almeno tre volte la richiesta di uno stesso ACK number da parte del server significa che il pacchetto è andato perso, e si attivano i meccanismi di controllo di congestione. Un pacchetto si dà per perso anche nel caso di scadenza di un retransmission timeout RTO, nel caso in cui non ci sia possibilità di mandare tre ACK (esempio: penultimo pacchetto perso, finestra più piccola di tre...). Si ritrasmette il pacchetto perso alla fine della finestra. In caso di congestione, ci si accorge che il rate di pacchetti che si possono inviare senza conferma di ricezione deve essere ridotto.

Descrivere e cos'è controllo di flusso

Il controllo di flusso stabilisce e misura la capacità del buffer in ricezione. L'advertised window è la dimensione residua nel buffer del ricevente e dipende dal traffico. La dimensione della sliding window è influenzata dalla dimensione dell'advertised window. Non si può mai avere advertised window maggiore della sliding window perché significa che verrebbero sicuramente persi i pacchetti di differenza tra advertised e sliding. Il controllo di flusso regola il tasso di trasmissione dei pacchetti per non saturare il buffer di ricezione ma non è un rate.

Descrivere il controllo di congestione nel TCP e come viene gestito da Tahoe e Reno (o differenze tra Tahoe e Reno)

Il controllo di congestione significa guardare lo stato di traffico e di collasso dell'intera rete. Viene implementato tramite un campo che si chiama congestion window, che viene valutata di continuo per monitorare lo stato della rete: la misura della sliding window è data dal minimo tra advertised window e congestion window. Il paradigma usato è AIMD (additive increase multiplicative decrease): fin quando non c'è congestione si aumenta in modo lineare, lentamente, la finestra di congestione; quando si verifica la congestione la finestra di congestione si riduce drasticamente in modo moltiplicativo e di conseguenza si riduce anche la sliding. La congestione è percepita grazie a 3 ACK duplicati o allo scadere di RTO. Si ha bisogno della congestion window perché misura lo stato di congestione dell'intera rete: tenendola monitorata si evita di inviare n pacchetti senza attendere conferma col rischio che tutti questi n pacchetti vadano persi a causa del collasso della rete in un certo punto.

===== APPLICATION LEVEL =====

58. Descrivi il WWW (World Wide Web)

Il Web è un servizio che richiede affidabilità, quindi utilizza come protocollo di trasporto il TCP. WWW è una collezione distribuita di documenti ipertestuali e ipermediali collegati tra loro; se non fosse distribuita infatti, non sarebbe possibile accedere alle risorse in quanto i tempi di attesa sarebbero troppo lunghi. I documenti possono essere statici, dinamici o attivi e sono accessibili attraverso pagine web. Queste pagine, possono essere create attraverso un linguaggio chiamato HTML e visitate attraverso il browser. Un browser è un' applicazione che interpreta e visualizza una pagina web. È composto da 3 moduli:

- **Controller:** che riceve l' input da parte del client e seleziona i protocolli applicativi necessari per accedere ai contenuti delle pagine web (fa comunicare il browser con il server);
- **Protocolli applicativi** (http e ftp);
- **Interprete:** interpreta il contenuto delle pagine web e lo riproduce a schermo.

I documenti presenti sul web sono identificati univocamente attraverso l' URL (Uniform Resource Locator); esso è composto da 4 parti: **protocollo applicativo** (per visualizzare la risorsa), **host** sul quale risiede la risorsa (www), **porta** sulla quale è in ascolto il protocollo remoto e **percorso** nel *file system* remoto. Es. --> <http://www.porta/path>

59. Descrivi i protocolli applicativi

- **http:** consente lo scambio tra client e server web; il client fa una richiesta al proprio browser, il quale invia una *http request* al server web in cui viene specificato l' oggetto cercato dal client; a questo punto il server invia una *http response* che contiene l' oggetto cercato. Esistono 2 versioni di http:
 - **http1.0** --> è stateless e non persistente;
 - **http1.1** --> è stateless e persistente.

Stateless significa che http non tiene conto delle richieste fatte in passato (non ha memoria); mentre non persistente significa che viene creata una nuova connessione TCP per ogni oggetto scambiato. Questo significa che con **HTTP1.1** possono essere scambiati più oggetti con la stessa connessione --> è più veloce rispetto a **HTTP1.0**.
Una connessione persistente può essere:

- Con parallelismo --> più richieste consecutivamente;
- Senza parallelismo --> prima di poter fare una nuova richiesta devo aver ricevuto la risposta.

Per risolvere la natura stateless di **HTTP** sono stati introdotti i cookies attraverso i quali è possibile tenere traccia del comportamento degli utenti: quando un utente visita un sito per la prima volta, il server genera uno UID univoco che viene aggiunto nel file di cookie presente lato client; nel momento in cui l'utente riconsulterà quel sito, lo UID viene comunicato al server.

- **FTP (File Transfer Protocol)**: utilizza due connessioni TCP: una di controllo per lo scambio di informazioni di controllo tra client e server ed una di dati per lo scambio di file. La connessione non è persistente e, a differenza di http, ftp non è stateless perché per avviare una connessione con il server, il client deve possedere un account sul server (che ne richiede l'autenticazione).

60. Descrivi il DNS ed il suo funzionamento

Il DNS (Domain Name System) è un database distribuito formato da una gerarchia di server dei nomi sparsi in tutto il mondo e che cooperano tra di loro utilizzando un protocollo applicativo (DNS/UDP) che consente lo scambio di informazioni tra il server dei nomi e i client. La funzione del DNS è quella di tradurre un nome logico in un indirizzo IP e viceversa. Ogni internet service provider ha un server dei nomi di default al quale i client sotto quella rete inoltrano le proprie richieste e, se il server non è in grado di tradurre la richiesta ricevuta, la inoltra ad un altro server.

I DNS hanno 2 diverse modalità di funzionamento:

- **Risoluzione ricorsiva**: il client invia la richiesta al server dei nomi locale e, se quest'ultimo non è in grado di tradurla, la inoltra al server con maggior controllo fino ad arrivare all'*authoritative name server*. Quando un server è in grado di tradurre la richiesta, manda la risposta al server che ha inoltrato la richiesta fino a raggiungere il client. È possibile che i server implementino meccanismi di caching per tener traccia dei siti più visitati dall'utente;
- **Risoluzione iterativa**: il client inoltra la richiesta al *local name server* e, se questo non è in grado di tradurre la richiesta, risponderà al client il quale dovrà inoltrare la richiesta ad un server con maggior controllo.

61. Descrivi il Resource Record

Il Resource Record è composto da 4 campi.

Name	Value	Type	TTL
------	-------	------	-----

In base al contenuto di *type* cambierà il contenuto informativo di *name* e *values*. SE:

- **Type = A** --> Name è un host-name e Value è l' indirizzo IP dell' host-name;
- **Type = NS** --> Name è un dominio e Value è l' host-name di un server dei nomi assoluto per quel dominio;
- **Type = CNAME** --> Value è l' alias name canonico per il valore Name;
- **Type = MX** --> Value è un host-name di un server di posta che ha alias Name.

62. Descrivi l' electronic mail (e-mail)

L' email è basata su 4 componenti: *user agents*, *mail servers* (che contengono tutti i messaggi in ingresso e uscita degli utenti e gestiscono le mail box), *SMTP* (che è il protocollo utilizzato dai *mail servers* per trasferire i messaggi), *POP3/IMAP* (per accedere alle mail box). Quando una mail è pronta e viene spedita, viene messa in coda ad un server mail che a sua volta la spedisce utilizzando SMTP (che utilizza il protocollo TCP). La mail raggiungerà il server mail del destinatario che potrà scaricarla attraverso POP3. L' header delle mail contengono: *indirizzo mail di mittente e destinatario* e *oggetto della mail*. Dall' indirizzo mail si conosce l' indirizzo IP grazie al DNS. Nell' header del TCP viene quindi aggiunto l' indirizzo IP del mittente, la porta dell' host del mittente, l' indirizzo IP del destinatario mentre, nell' header IP viene aggiunto di nuovo l' indirizzo IP del mittente e l' indirizzo IP del destinatario.

il MIME è un' estensione che consente lo scambio di file multimediali attraverso l' aggiunta di headers che caratterizzano il contenuto del messaggio.

il POP3 (Post Office Protocol) consente di accedere ad una mailbox. Opera in 3 fasi:

autenticazione, transazione e aggiornamento della mailbox.

L' IMAP infine, associa ad ogni messaggio una cartella e consente all' utente di creare cartelle sul server, spostare i messaggi da una cartella ad un' altra e ricercare messaggi/recuperarne parte di essi.

63. Descrivi la pila dei protocolli per il trasferimento di contenuti multimediali e indica cos' è l' RTP

La pila dei protocolli è la seguente:

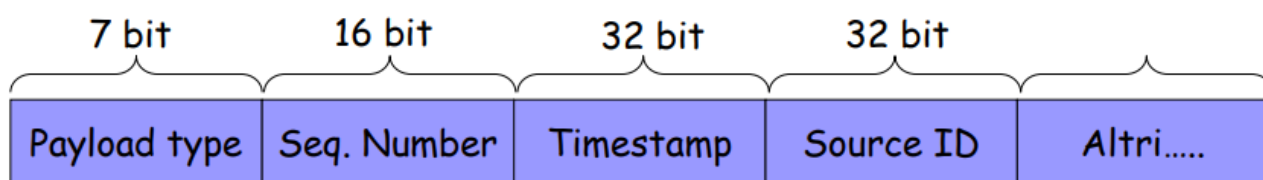
- Livello applicazione multimediale;
- Livello RTP;
- Livello UDP;
- Livello IP;
- Livello network interface.

Per trasferire contenuti multimediali come streaming di audio/video e per i servizi real-time si utilizza l' UDP. Infatti, l' RTP è un protocollo per il trasporto di contenuti multimediali ed utilizza l' UDP.

RTP è utilizzato congiuntamente all' RTCP che consente lo scambio di informazioni di controllo tra client e server.

RTP supporta diversi flussi quindi, per ogni classe di applicazione, definisce un profilo e più formati. Il profilo descrive l'header mentre il formato indica come interpretare i contenuti di un pacchetto RTP.

Nei messaggi RTCP **da client a server** sono contenuti: *l' ultimo numero di sequenza, il jitter degli arrivi e il numero dei pacchetti persi*; Nei messaggi RTCP **da server a client** invece, sono contenuti: *timestamp e ora effettiva, numero dei pacchetti inviati e numero di byte inviati*.



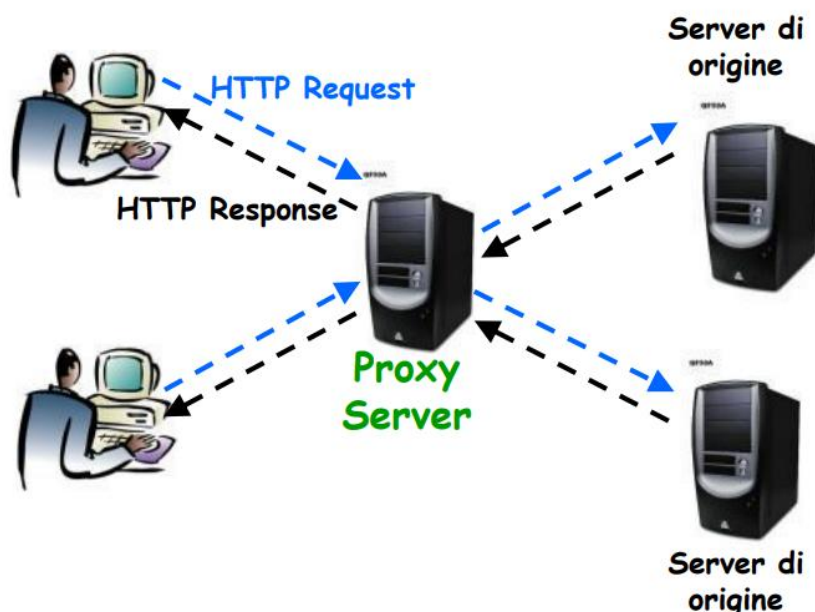
64. Indica le soluzioni per ridurre la World Wide Wait

Per ridurre la World Wide Wait ci sono 2 possibili soluzioni:

1. Replicare i contenuti su una molteplicità di server;
2. Scegliere il server più idoneo (utilizzo dei proxy server e dei CDN (Content Distribution Networks)).

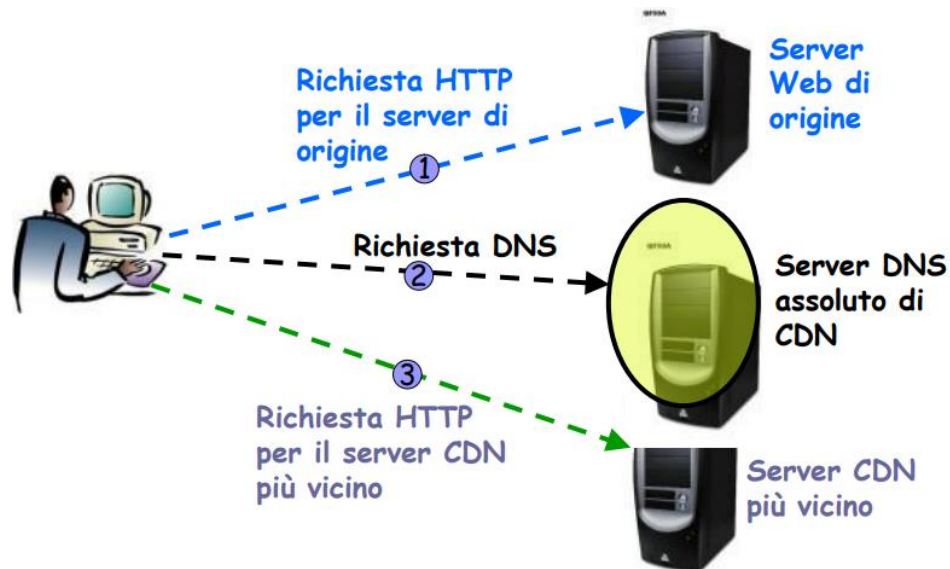
65. Che cos' è e a cosa serve il proxy server

Il proxy server è un server di prossimità che contiene i link ai siti più visitati. Se una richiesta da parte di un client può essere soddisfatta dal proxy server, non c' è bisogno di scalare su internet e i tempi di attesa saranno minori. Il funzionamento del proxy server è il seguente:



66. Che cos' è il CDN (Content Distribution Networks)

CDN è una gerarchia di server che riproduce i contenuti dei loro client su più server CDN e inoltre, implementano meccanismi per selezionare il server più idoneo. Il funzionamento del CDN è il seguente:



===== SENSOR NETWORK =====

67. Che cosa sono le sensor networks?

Le sensor networks sono reti di sensori; ogni sensor network è costituita da migliaia di sensori che comunicano tra di loro via wireless. Le informazioni raccolte da ciascun snodo vengono convogliate in un nodo di raccolta detto *sink*. Utilizzano una tecnologia transfer multi-hop, questo significa che le informazioni raggiungono la sink attraverso più salti.

I nodi hanno energia limitata (più trasmettono/ricevono e più si scaricano), bassi costi, piccole dimensioni, basso peso, bassa potenza (devono essere vicini), basso bit rate e sono autonomi. Le sensor networks possono essere impiegate in svariate applicazioni.

68. Quali sono i fattori che influenzano la progettazione di una sensor network?

I principali fattori influenzanti sono:

- *Reliability;*
- *Scalabilità;*
- *Costi di produzione;*
- *Topologia;*
- *Ambiente applicativo;*
- *Consumo di potenza.*

La *reliability* è la capacità di una rete di mantenere le funzionalità senza interruzioni causate, ad esempio, dalla rottura di un nodo.

La progettazione di una SN dipende molto dall' *ambiente applicativo*; una rete inoltre si dice *scalabile* quando il suo comportamento non varia significativamente in base al numero di nodi.

I *costi di un nodo* devono essere bassi ed infine, è importante tenere conto che i nodi *consumano maggiormente in fase di trasmissione/ricezione*.

69. Perché non è possibile utilizzare l' indirizzo IP nelle sensor networks?

Nelle SN non è possibile utilizzare l' indirizzo IP per far comunicare i nodi tra loro in quanto vi sono migliaia di nodi e quindi non ci sarebbero gli indirizzi IP disponibili; inoltre i nodi hanno una potenza limitata e, in ultimo, perché sono molto frequenti i cambiamenti topologici. I nodi quindi, utilizzano nuovi protocolli per lo scambio di informazioni.

70. Quali sono i protocolli di routing nelle SN (livello di trasporto)?

I protocolli di routing si dividono in:

- **Data centric protocols:** (flooding, gossiping, SPIN, direct diffusion); I protocolli non necessitano di un' identità, il dato è identificato in base ai suoi attributi;
 - **Flooding**: i dati vengono inviati da un nodo in broadcast verso tutti i vicini;
 - **VANTAGGI**: è semplice da utilizzare e non c' è ritardo;
 - **SVANTAGGI**: elevato consumo di energia, implosion della rete (rete intasata) ed infine, i nodi ricevono più volte lo stesso dato.
 - **Gossiping**: un nodo invia i dati verso un nodo vicino scelto a caso; risolve alcuni problemi del flooding (risparmia energia, evita implosion) ma distribuisce le informazioni più lentamente;
 - **SPIN-1**: utilizza 3 messaggi: ADV (*advertisement*), REQ (*request*) e DATA. Un nodo, quando ha un dato da trasmettere, invia in broadcast un ADV packet; i nodi interessati al dato inviano una REQ packet, di conseguenza il nodo invierà le informazioni solo ai nodi interessati.
 - **VANTAGGI**: è semplice da utilizzare ed evita implosion;
 - **SVANTAGGI**: consuma molta potenza per inviare i 3 messaggi.
 - **SPIN-2**: funziona come il precedente SPIN-1 ma tiene conto dell' energia residua al nodo; se il livello di energia è troppo basso per completare le 3 fasi, il nodo si mette nello stato dormiente inoltrando semplicemente le informazioni verso gli altri nodi. SPIN, rispetto ai 2 protocolli precedenti, riduce l' energia impiegata e non genera messaggi duplicati.
 - **Direct diffusion**: in questo protocollo, è la sink a dichiarare interesse per un dato mediante delle query. I dati generati da un sensore sono identificati dalla coppia *attributi-valore*, la sink utilizza questa coppia per creare delle query ed interrogare i sensori.
 - **VANTAGGI**: risparmio energetico;
 - **SVANTAGGI**: non può essere sempre applicato, inoltre non è indicato per applicazioni con elevato *data delivery*, infine, genera overhead.

- **Protocolli gerarchici: (LEACH):**
 - **LEACH**: vengono creati dei *clusters*; i nodi si aggregano ad un cluster heads e inviano dati. I cluster heads comunicano con la sink. LEACH prevede 2 fasi:
 - **Set-up**: i sensori si eleggono cluster head e scelgono un numero casuale tra 0 e 1; successivamente, per ogni zona, viene eletto un cluster head (quello che ha scelto il numero più basso di una certa soglia). Dopodiché il cluster head comunica in broadcast agli altri sensori di essere un cluster head. Gli altri sensori, si aggregano al cluster head che richiede meno energia per essere raggiunto e, i cluster heads assegnano un intervallo di tempo entro cui i nodi possono trasmettere. Scaduto tale tempo viene scelto un nuovo cluster head.
 - **Steady**: i nodi inviano i loro dati criptati al cluster head, il quale li aggrega e li invia alla sink che poi li decifrerà. Dopo un certo periodo si tornerà alla fase di set-up.
Se ci sono pochi clusters, i nodi saranno lontani dal proprio cluster head mentre se vi sono molti cluster, molti cluster head invieranno dati alla sink.
 - **VANTAGGI**: risparmio energetico, è un sistema totalmente distribuito in cui i nodi muoiono casualmente e single hop per raggiungere il cluster head;
 - **SVANTAGGI**: non è applicabile in reti installate in ampie regioni.

71. Quali sono le funzioni svolte da un protocollo di trasporto?

le principali funzioni svolte da un protocollo di trasporto sono:

- **Reliability;**
- **Controllo di gestione;**
- **Self-configuration** (adattarsi alla topologia dinamica);
- **Risparmio energetico.**
- **Buffer size limitato**
- **Supporto di connessioni uniche;**
- **NB: nelle SN non è utilizzabile il TCP perché i sensori hanno risorse limitate.**

72. Descrivi come possono essere le query

le query sono suddivise in 3 classi:

- **Continuous**: collezionano dati per lunghi intervalli di tempo;
- **Snapshot**: collezionano dati relativi ad un certo istante di tempo;
- **Historical**: collezionano dati riassuntivi del passato.

Inoltre possono essere **data-centric**, **geographical** o **real-time**. SCTL permette di gestire i nodi.