PISSIR – PROGETTAZIONE E IMPLEMENTAZIONE DI SISTEMI SOFTWARE IN RETE

DATA LINK LAYER

INTRODUZIONE

- Nodo: qualunque dispositivo che opera a livello di collegamento
- Collegamenti: canali di comunicazione che collegano i nodi adiacenti

Su ogni collegamento un nodo incapsula il datagramma in un frame del livello collegamento e lo trasmette lungo il collegamento stesso, il data link layer ha la responsabilità di trasferire i datagrammi da un nodo al suo adiacente attraverso il collegamento.

SERVIZI

- Farming: i datagrammi vengono incapsulati dal protocollo a livello di rete in frame a livello di collegamento prima di essere trasmessi, c'è un campo dati che viene usato per incapsulare il datagramma e diversi campi di intestazione
- Accesso al collegamento: il protocollo MAC – medium access control controlla l'accesso al mezzo trasmissivo nel caso in cui diversi nodi condividono lo stesso collegamento, il protocollo MAC coordina la trasmissione da parte dei frame
- Consegna affidabile: viene garantito il trasporto senza errori di ciascun datagramma, ciò può essere implementato attraverso ACK e ritrasmissioni; viene utilizzato solitamente su collegamenti con elevati tassi di errore (wireless) con lo scopo di correggere localmente l'errore ed evitare la propagazione dell'errore fino al trasporto / applicazione.
- Rilevazione e correzione degli errori: gli errori sui bit sono causati dall'attenuazione di segnale e dai disturbi elettromagnetici, per rilevare e correggere gli errori il nodo mittente inserisce un bit di controllo nel frame e il ricevente controllerà il valore (fatto in hardware)

DOVE VIENE IMPLEMENTATO

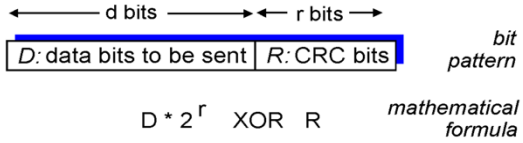
Per un dato collegamento il protocollo di livello collegamento è realizzato da un **adattatore di rete** noto anche come **scheda di rete,** il controller della scheda di rete è un chip dedicato e implementa i servizi prima descritti in hardware; lato mittente il controller prende un datagram nella memoria dell'host su cui risiede e lo incapsula i un frame inserendo anche gli opportuni campi e lo trasmette sul canale di comunicazione, lato ricevente estrae il datagram dal frame e lo consegna a livello di rete effettua se presente il controllo degli errori.

RILEVAZIONE E CORREZIONE ERRORI

Ai dati che devono essere protetti da errori vengono aggiunti dei bit EDC – error detection and correction bits, vengono anche protetti dati come gli indirizzi, numeri di sequenza ecc... Anche con le attuali tecniche il nodo ricevente potrebbe (raro) non accorgersi che si sono verificati degli errori, le tecniche più sofisticate implementano un'elevate ridondanza:

- Controllo di parità: nella sua forma più semplice viene utilizzato un **singolo bit** di parità, il ricevente conta il numero di bit a 1 tra quelli ricevuti, se trova un numero dispari di bit 1 sa che si è verificato un numero dispari di errori nei bit. in caso di numero pari di errori la presenza di un errore non verrebbe rilevata.
  Viene quindi utilizzata una **parità bidimensionale**: i bit del dato sono suddivisi in i righe e j colonne per ognuna delle quali è stato calcolato un valore di parità; il ricevente può quindi non solo rilevare che si è verificato un errore ma può utilizzando indici di colonne di riga identificare il bit alterato e correggerlo.

- Checksum: i dati sono trattati come interi di 16 bit e sommati, il complemento a 1 di questa somma costituisce il checksum che viene trasportato nell'intestazione dei segmenti; Il ricevente controlla il checksum calcolando il complemento a 1 della somma dei dati ricevuti e verifica che tutti i bit del risultato siano uno se non è così viene segnalato un errore.
- Cyclic Redundancy Check – CRC: è una tecnica basata sui **codici di controllo a ridondanza ciclica**, i codici CRC sono detti anche **codici polinomiali** in quanto è possibile vedere la stringa di bit da trasmettere come un polinomio i cui coefficienti sono i bit della stringa.
  Generatore g = stringa di r + 1 bit (in accoro tra mittente e destinatario), il bit più significativo di g (più a sx) deve essere 1; il mittente sceglie r bit addizionali e li aggiunge ai dati d ottenendo una stringa d + r che sia divisibile per g!
  Se la divisione (d + r) / g in modulo 2 ha un resto diverso da 0 (effettuato dal destinatario) si sono verificati errori, **R** viene calcolato dal mittente come: **R = resto(D x 2^r/G).**
  Sono stati definiti dei generatori standard di 8,12, 16 e 32 bit, lo standard CRC- 32 a 32 bit in numerosi protocolli IEEE del livello di collegamento usa il generatore G_{CRC-32} =10000010011000001000111011011011 1.
  CRC può rilevare errori a burst inferiori r + 1 bit ovvero tutti gli errori consecutivi di non oltre r bit saranno rilevati ma non possono essere corretti.
  È un algoritmo complesso e quindi viene fatto spesso in hardware (protocollo Ethernet, (802.11 WiFi) e non in software come nei protocolli TCP ecc...



PROTOCOLLI DI ACCESSO MULTIPLO

Ci sono due tipi di Link (collegamento)

Collegamenti punto-punto: un trasmittente e un ricevente connessi da un collegamento a loro riservato, diversi protocolli --> PPP, HDCL

Collegamenti broadcast: sono usati nelle reti WiFi 802.11, reti satellitari e possono avere più nodi trasmittenti e riceventi connessi allo stesso canale broadcast condiviso; le reti di calcolatori usano i **protocolli di accesso multiplo** che fissano le modalità con cui i nodi regolano le loro trasmissioni sul canale condiviso, sono algoritmi prevalentemente di tipo distribuito.
Se due o più nodi trasmettono nello stesso istante si genera una **collisione** a causa della quale nessuno dei nodi riceventi riuscirà a interpretare i frame -> perdita di frame.
Le caratteristiche ideali del protocollo dovrebbero essere:

1- Quando un solo nodo deve inviare dati questo dispone di troughput pari a R bps (tutta la banda)
2- Quando M nodi inviano dati questi dispongono di un throughput medio pari a R/M bps
3- Il protocollo è decentralizzato ovvero non ci sono nodi principali che qualora non funzionassero correttamente potrebbero rendere inattivo l'intero sistema.
4- Il protocollo è semplice ed economico da implementare

MAC PROTOCOLS

- Protocolli a suddivisione del canale
  TDMA – Time division multiple access: viene suddiviso il tempo in intervalli di tempo (time frame) e poi divide ciascun intervallo di tempo in N slot temporali (time slot), ogni slot viene assegnato a uno degli N nodi (assegnamento statico).
  Ogni nodo invierà il proprio frame nel suo slot di tempo a turno in ordine secondo una sequenza, questo permette di evitare le collisioni e di essere imparziali --> ogni nodo

durante il suo intervallo di tempo ha un tasso trasmissivo di R/N bps, il lato negativo è che quando non vi sono altri nodi che devono inviare un pacchetto il nodo che lo vuole inviare è vincolato ad attendere il suo turno.

FDMA – Frequency division multiple access: suddivide il canale condiviso in frequenze differenti e assegna a ciascuna frequenza ad un nodo; a partire da un canale di R bps crea N canali di R/N bps anche qui il lato negativo e che la larghezza di banda è limitata a R/N bps anche quando vi è un solo nodo che ha un pacchetto da spedire (assegnamento statico).

CDMA – Code Division Multiple Access: assegna un codice ai nodi, ogni nodo utilizza quel codice per codificare i propri dati da inviare; se i codici sono scelti accuratamente queste reti consentono a nodi differenti di trasmettere simultaneamente e ai rispettivi destinatari di ricevere correttamente i bit dei dati codificati nonostante le interferenze delle trasmissioni degli altri nodi (il ricevente deve conoscere il codice CDMA corretto).
Viene utilizzato nella telefonia mobile

*Banda di guardia: porzione di banda in cui nessuno trasmette per evitare che i segnali si sovrappongano

- Protocolli ad accesso casuale: un nodo trasmette sempre alla massima velocità consentita dal canale cioè R bps, in caso di collisione i nodi coinvolti ritrasmettono ripetutamente i loro frame fino a quando raggiungono la destinazione senza collisioni.
  La ritrasmissione del frame non è immediata il nodo calcola un tempo casuale (**random delay**) e ogni nodo coinvolto nella collisione ne calcolerà uno indipendente dagli altri nodi.

  Slotted ALOHA: è stato riutilizzato di recente per gli RFID
  - frame lunghi L bit
  - tempo suddiviso in slot da L/R secondi
  - i nodi iniziano la trasmissione dei frame solo all'inizio degli slot
  - i nodi sono sincronizzati tra loro in modo da sapere quando iniziano/concludono gli slot
  - se avviene una collisione in uno slot tutti i nodi della rete la rilevano prima della fine dello slot
  - p è la probabilità ed è un numero tra 0 e 1

  Le operazioni dei nodi slotted ALOHA sono:
  - quando un nodo ha un nuovo frame da spedire attende fino all'inizio dello slot successivo e poi trasmette l'intero frame
  - se non si verifica collisione l'operazione ha avuto successo il nodo può predisporre l'invio di un nuovo frame
  - se si verifica una collisione il nodo la rileva prima del termine dello slot e ritrasmette con probabilità p il suo frame durante gli slot successivi fino a quando l'operazione non ha successo (comportamento casuale).

  PRO: un singolo nodo attivo può continuamente trasmettere alla massima velocità sul canale, è decentralizzato anche se ogni slot richiede una sincronizzazione, è semplice.
  CONTRO: quando si verificano le collisioni vengono sprecati slot, è un protocollo particolarmente inefficiente.

  CSMA – Carrier sense multiple access: un nodo ascolta il canale prima di trasmettere (rilevamento della portante) se il canale sta già trasmettendo un frame in modo aspetta finché rileva che il canale è libero per un intervallo di tempo e quindi inizia a trasmettere.
  Il nodo mentre trasmette rimane in ascolto del canale se osserva che un altro nodo sta trasmettendo un frame che interferisce col suo arresta la propria trasmissione (rilevamento

della collisione).
Il ritardo di propagazione da un estremo all'altro del canale broadcast ha un ruolo cruciale nel determinare le prestazioni, maggiore questo ritardo maggiore sarà la possibilità che il nodo pur attento a rilevare la portante non si accorga che è già cominciata la trasmissione da parte di un altro nodo.

CSMA/CD – Carrier sense multiple access / collision detection:
Il rilevamento delle collisioni è semplice nelle LAN cablate mentre nelle LAN wireless non può essere utilizzato perché ci vorrebbe un hardware molto costoso (motivo tecnico).
Operazioni dal punto vista di una scheda di rete collegata ad un canale broadcast
1 - la scheda ottiene direttamente un datagram dal livello di rete prepara un frame a livello di collegamento e lo sistema in un suo buffer
2 - quando riscontra che il canale libero inizia la trasmissione del frame, se il canale risulta occupato resta in attesa
3 - durante la trasmissione verifica la presenza di eventuali altre trasmissioni
4 - se viene trasmesso l'intero frame senza rilevare altre trasmissioni il lavoro è concluso altrimenti interrompe immediatamente la trasmissione del frame
5 - dopo aver annullato la trasmissione la scheda di rete aspetta per un tempo casuale tra 0 e 2^N-1 dove N è il numero di collisioni (**tempo di backoff**) e poi ritorna al passo 2.
Efficienza = 1 / (1 + 5 t_{prop} /t_{trans}) con t_{prop} = ritardo massimo di propagazione tra 2 nodi nella LAN e t_{trans} = tempo per trasmettere un frame di dimensioni massime.

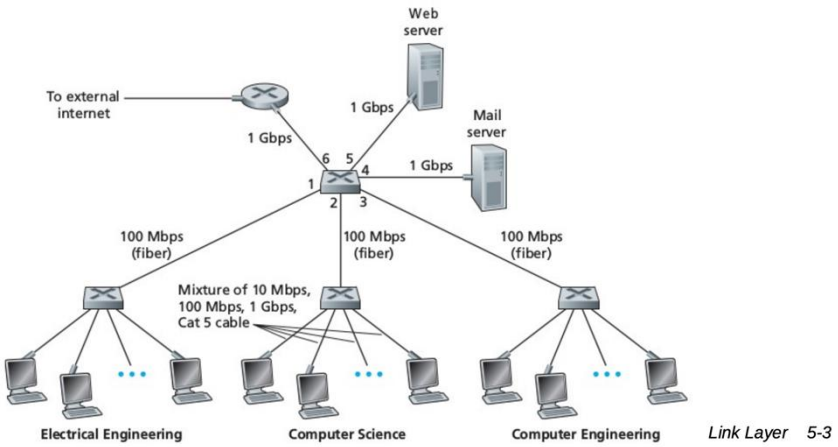
- Protocolli a rotazione

Protocollo Polling: uno dei nodi designato come principale (master) interpella a turno gli altri, in particolare invia un messaggio ad un nodo 1 comunicandogli che può trasmettere fino a un dato numero massimo di frame, successivamente avviserà il nodo 2 ecc...
Il nodo principale interpella in modo ciclico tutti gli altri nodi.
PRO: elimina le collisioni e gli slot vuoti
CONTRO: introduce il ritardo di polling -> tempo richiesto per notificare a un nodo il permesso di trasmettere, in caso di unico nodo attivo questo trasmetterà a tasso inferiore a R bps in quanto il nodo principale deve contattare ciclicamente i nodi inattivi.
Se il nodo principale si guasta l'intero canale diventa inattivo (single point of failure).

Protocollo Token-Passing: non esiste un nodo principale ma un "messaggio" un frame di controllo detto token (gettone) che circola fra i nodi seguendo un ordine prefissato.
Se il nodo che riceve il token non ha pacchetti da inviare lo inoltra immediatamente al successivo altrimenti procede a trasmettere il numero massimo di frame consentito.
PRO: decentralizzato e altamente efficiente
CONTRO: il guasto di un nodo può mettere fuori servizio l'intero canale oppure se un nodo non riesce a inoltrare il token occorre invocare procedure di recupero.

SWITCHED NETWORK

Gli switch sono apparati che lavorano a livello collegamento, a questo livello non vengono utilizzati indirizzi IP e non si utilizzano gli algoritmi di routing del livello IP (OSPF, RIP, …) mentre un router implementa entrambi i livelli.



MAC ADDRESS

È utilizzato per riuscire ad inviare da un frame da un nodo ad un altro della sottorete, è un indirizzo univoco associato alla scheda di rete del nodo -> viene individuato così lo specifico nodo.
Se un nodo ha più interfaccia di rete ciascuna avrà un MAC differente

Sono formati da 48 bit, sono nella ROM nella scheda di rete -> anche se nelle schede di rete più moderne è possibile cambiare il MAC via software.

La IEEE concede ai produttori un certo spazio di indirizzi MAC per evitare che due schede di rete abbiano lo stesso codice (viene gestito in modo analogo all'assegnazione degli IP) anche se non viene utilizzata una gerarchia come in IP (è piatto) è un codice che una volta assegnato non viene più cambiato (o molto raramente)

ARP – ADDRESS RESOLUTION PROTOCOL

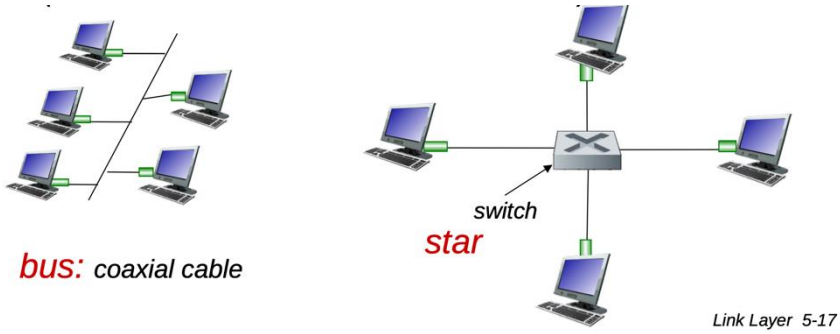
È un protocollo che permette al router di "tradurre" gli indirizzi IP in indirizzi MAC per poter inoltrare il frame al giusto nodo: ogni nodo IP ha una tabella ARP che mantiene l'associazione
< IP address; MAC address; TTL > (TTL tipico = 20 minuti)
Per popolare le tabelle ARP una soluzione statica non è ideale e si utilizza quindi il protocollo ARP che effettua un broadcast sulla rete in cui specifica come destinazione un particolare MAC per la trasmissione in broadcast = FF-FF-FF-FF-FF-FF -> tutti i nodi ricevono la richiesta nella quale è specificato l'indirizzo IP desiderato, i nodi con IP diverso lo scartano mentre quello con indirizzo IP corretto risponde in unicast alla query (non più broadcast) specificando il suo indirizzo MAC che verrà salvato dal nodo che ha fatto la richiesta nella sua tabella ARP.

ETHERNET

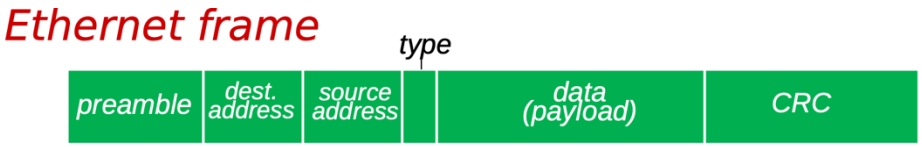
È lo standard per le reti LAN poiché è stata la prima tecnologia sviluppata, inizialmente pensata con una topologia a BUS più semplice ed economica rispetto alle token ring LAN (o altre).
Velocità comprese tra 10 Mbps – 10 Gbps migliorando e ottenendo ottime velocità.

TOPOLOGIA FISICA

- **BUS**: popolare negli anni 90': tutti i nodi sono nello stesso dominio di collisione (ci possono essere collisioni fra i nodi)
- **Star**: il più utilizzato oggi: uno switch attivo al centro con N "spoke" che eseguono un protocollo Ethernet (separato) -> i nodi non entrano in collisione tra loro



STRUTTURA DEL FRAME



- **Preambolo**: 7 bytes con pattern 10101010 seguiti da un byte con pattern 10101011, viene utilizzato per sincronizzare il ricevitore con il clock rate del mittente
- **Indirizzi**: 6 bytes per sorgente e 6 byte per destinazione MAC address
- **Tipo**: 2 byte, indica qual è il protocollo di livello superiore del payload (tipicamente IP)
- **Payload**: è prevista una dimensione minima e massima (1500 byte) MTU a livello IP
- **CRC**: cyclic redundancy check dal ricevente, se c'è un errore il frame viene scartato

CONNECTIONLESS: non c'è handshaking

UNRELIABLE: La ricezione della scheda NIC non invia conferme ACK o NACK, i dati nei frame persi sono recuperati solo se il mittente iniziale utilizza a un livello superiore rdt (es.: TCP), altrimenti andranno persi.

SWITCH

È un dispositivo a livello di collegamento e assume un ruolo attivo (comportamento trasparente):

- memorizza, inoltra frame Ethernet
- esaminare il MAC del frame in arrivo e inoltra selettivamente il frame a uno o più collegamenti in uscita

Sono self-learning: non hanno bisogno di essere configurati poiché “imparano” da soli dove inoltrare i frame sul collegamento corretto in base agli indirizzi MAC

FORWARDING TABLE e SELF LEARNING

ogni switch ha una sua tabella di inoltro che contiene un mapping tra

<MAC address dell’host; interfaccia per raggiungere l’host; TTL>

Lo switch apprende quali host possono essere raggiunti attraverso quali interfacce:

- quando il frame viene ricevuto, lo switch "apprende" la posizione del mittente: in arrivo dal segmento LAN
- Aggiunge il record alla sua tabella contenete la coppia mittente/posizione

```
1. record incoming link, MAC address of sending host
2. index switch table using MAC destination address
3. if entry found for destination
    then {
    if destination on segment from which frame arrived
        then drop frame
        else forward frame on interface indicated by entry
     }
    else flood  /* forward on all interfaces except arriving
                   interface */
```

Multi-switch: gli switch possono essere interconnessi fra di loro sempre in una topologia gerarchica perché non bisogna creare loop nelle connessioni tra switch perché in caso di flooding ci sarebbe un loop infinito (negli switch più intelligenti può essere implementata una topologia mesh per il fault tollerance, lo switch impara un minimun spanning tree e si comporta come un albero)

Switch vs Router: entrambi sono di tipo store and forward

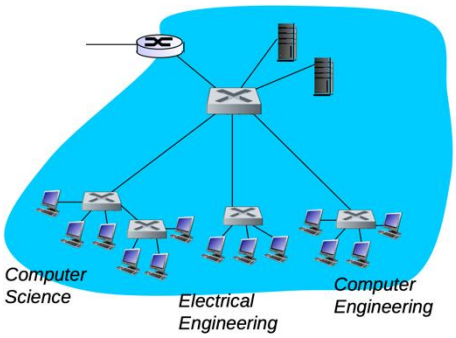
- Router: lavora a livello 3: rete e esamina le intestazioni dei pacchetti a quel livello
- Switch: lavora a livello 2: collegamento e esamina le intestazioni dei pacchetti a quel livello

Entrambi hanno delle tabelle di inoltro:

- Router: calcola le tabelle tramite gli algoritmi di routing distribuiti, IP address
- Switch: popola le tabelle di inoltro attraverso il flooding, learning, MAC address

VLANS – VIRTUAL LAN

Per limitare i problemi degli switch si utilizzano le VLAN, ad esempio problema del singolo dominio di broadcast i pacchetti in uscita in un singolo dipartimento potenzialmente possono raggiungere tutti gli altri host e viceversa (problema di cybersecurity), oltre che ha un eccessivo carico dovuto al traffico broadcast all'interno di un'unica LAN.

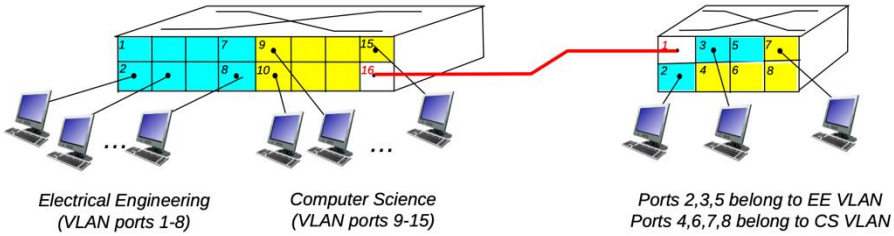


Le VLAN devono essere supportate dagli switch, le VLAN possono essere configurato per definire più VLAN su una singola LAN fisica.

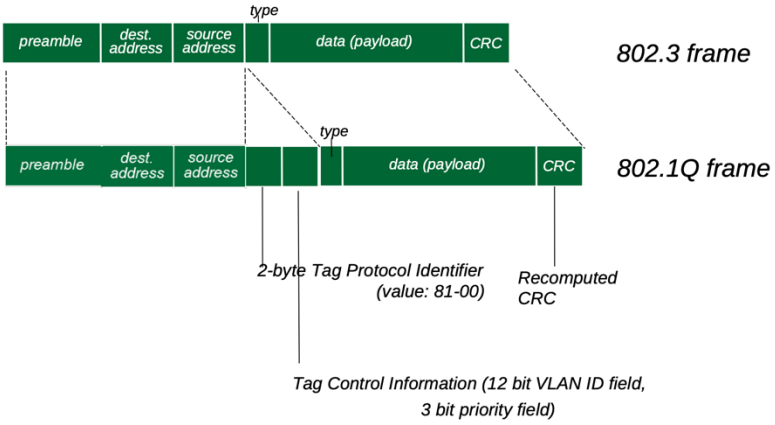
PORT BASED VLAN

- **Isolamento del traffico**: tutti i dispositivi all'interno di una VLAN possono comunicare soltanto con i dispositivi all'interno della stessa VLAN*
- **Dynamic membership**: posso configurare in modo dinamico lo switch per configurare un nuovo nodo assegnando una VLAN ad una certa porta via software
- **Forwarding between VLANS**: viene effettuato da un router

TRUNK PORT



È una porta particolare dello switch che permette di interconnettere più switch, per distinguere a quale VLAN appartiene un frame lo switch controlla nei campi header del frame il VLAN id viene standardizzato nel protocollo 802.1q, il frame viene quindi etichettato con il nome della VLAN corrispondente così che lo switch lo possa inoltrare in modo corretto eliminando l'header dal frame e tornando al frame 802.3 (serve solo agli switch, per i nodi è trasparente, così è anche possibile utilizzare switch che non gestiscono le VLAN)

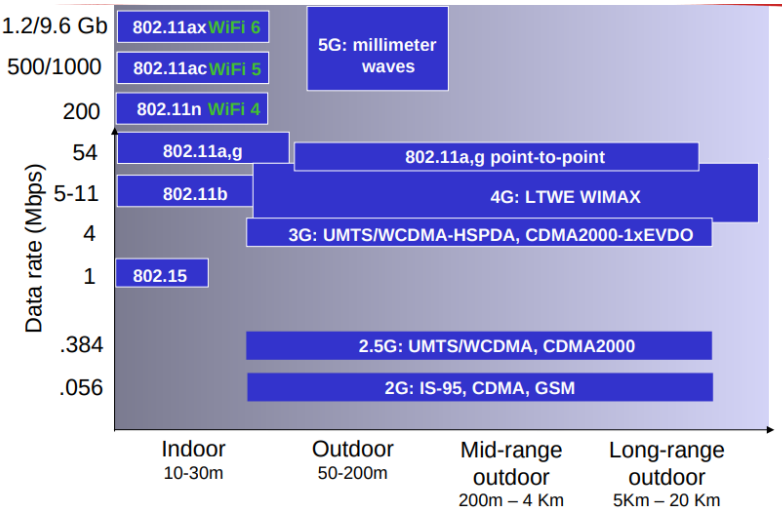


LE RETI WIRELESS

ELEMENTI DI UNA RETE WIRELESS

Possono essere laptop, smartphone, run applications -> possono essere stazionari (non mobile) o mobili, wireless non significa per forza mobilità.

I canali wireless sono tipicamente utilizzati per connettere i device alla **base station** (access point, isp repeater, …), ci sono diversi protocolli di accesso per coordinare l'accesso con diversi data rate dipendenti dalle distanze.



Due modalità per organizzare una rete wireless:

- Modalità con infrastruttura: la base station connette i device all'interno di una rete wireless con l'infrastruttura (rete cablata) e viene anche definito **l'handoff** ovvero un nodo può passare da una base station ad un'altra per supportare la mobilità degli host
- Modalità ad hoc: senza infrastruttura non c'è una base station, i nodi possono trasmettere tra loro se c'è una copertura fra di loro le antenne dei nodi devono raggiungere l'altro per poter comunicare o passare attraverso nodi intermedi (potrebbero non avere accesso ad Internet se tutti sono sconnessi da internet)

Diverse tassonomie

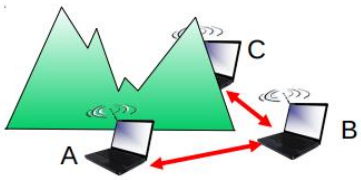
	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

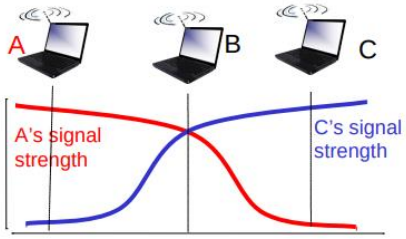
- **decreased signal strength**: il segnale radio diminuisce/degrada con l'aumentare della distanza, della propagazione in base ai materiali che attraversa (path loss)
- **interference**: le frequenze delle reti wireless (e.g., 2.4 GHz) sono condivise da diversi device (es., phone); capita spesso che possano avvenire interferenze
- **multipath propagation**: il segnale radio viene riflesso da oggetti a terra, arrivando a destinazione in tempi leggermente differenti

Creare una comunicazione attraverso (anche punto a punto) tramite un collegamento wireless è molto più "difficile" rispetto ad un collegamento cablato

HIDDEN TERMINAL PROBLEM

Se A non sente C non potrà rilevare delle collisioni e comunicherà lo stesso con B, quindi non è possibile utilizzare CSMA/CD



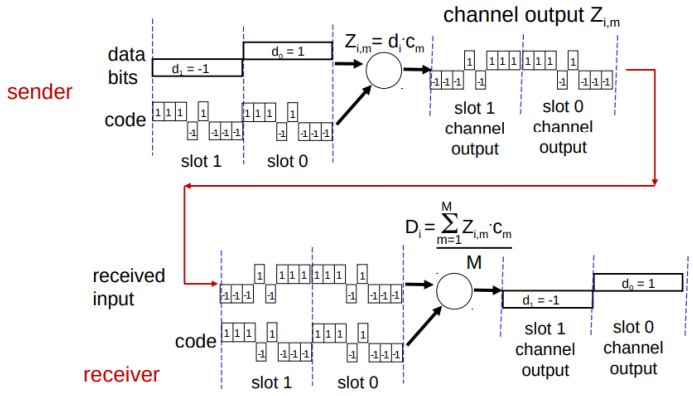


CODE DIVISION MULTIPLE ACCESS (CDMA)

Viene assegnato un codice univoco "chipping sequence" ad ogni utente, la frequenza viene condivisa tra tutti gli utenti ma viene effettuata una partizione del code set e assegnato ad ogni utente.

Il codice viene utilizzato da ogni utente per codificare i dati da trasmettere permettendo l'invio di informazioni in contemporanea, il ricevente sarà in grado di decodificare le informazioni corrette.

- **Codifica** = dati sorgente x chipping sequence
- **Decodifica** = segnale codificato x chipping sequence



Il problema di questa soluzione è la velocità di trasmissione perché aumento la dimensione dei dati trasmessi perché sono codificati-> perdo in velocità di trasmissione ma tutti possono trasmettere contemporaneamente

IEEE 802.11 WIRELESS LAN

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2020 (exp.)	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz

- all use CSMA/CA for multiple access, and have base-station and ad-hoc network versions

ARCHITETTURA

L'**host** comunica con la base station che in questo caso corrisponde all'**access point** che viene connesso a Internet da un router e/o switch, la **basic service set** (o cella) è l'insieme di nodi "coperto" da un certo access point e nel caso di modalità infrastruttura contiene: host wireless e access point.

CHANNELS, ASSOCIATION

Lo spettro viene diviso in **canali** a diverse frequenze, l'amministratore di rete sceglie le frequenze di utilizzo dei vari canali; in caso di canali sovrapposti con altri AP potrebbero capitare collisioni.
Un host deve **associarsi** con un particolare AP per connettersi a Internet:

MODALITA' PASSIVA

- L'host ascolta nei diversi canali i beacon frames che comunicano che un certo AP è attivo e contengono l'SSID (il nome della rete) e il suo MAC address, l'host deve essere configurato per ascoltare i canali
- L'host seleziona un AP a cui collegarsi (ci può essere negoziazione sui protocolli / velocità)
- L'AP può richiedere autenticazione e fornire indirizzi tramite DHCP

MODALITA' ATTIVA

- L'host fa una richiesta in broadcast
- Uno o più AP ricevono la richiesta e rispondono con le loro caratteristiche (SSID, MAC, …)
- L'host sceglie l'AP a cui collegarsi

La latenza della connessione di un host all'AP è dovuta all'invio periodico dei beacon frames da parte degli AP (può essere configurato)

MULTIPLE ACCESS

802.11 utilizza CSMA/CA per l'accesso multiplo ma bisogna evitare il più possibile le collisioni poiché è difficoltoso trasmettere e contemporaneamente ascoltare per evitare le collisioni, sia dal punto di vista tecnologico che hardware ma anche risolvendo questo problema c'è sempre il problema dell'**hidden terminal.**

Funzionamento di CSMA/CA in 802.11:

Viene utilizzato un ACK, dopo aver inviato un frame il sender attende un ACK e in caso di mancata ricezione (in un certo timeout) si è verificato un errore (meccanismo a ritrasmissione).

SENDER

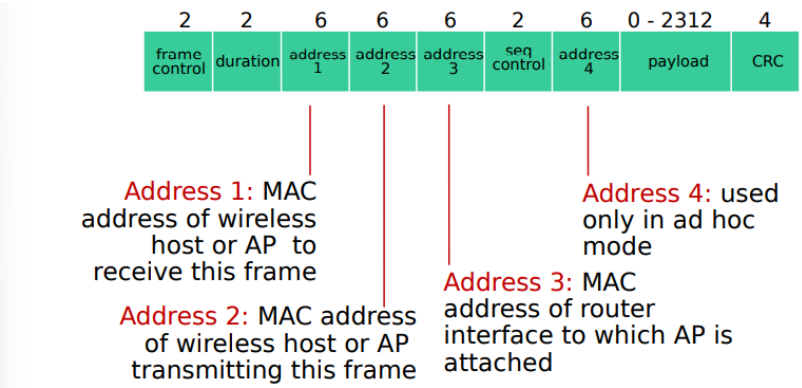
- Il sender in ascolto su un canale se esso è disponibile attende un tempo **DIFS** e poi trasmette
- Se il canale invece è occupato si comporta come CSMA attendo un **tempo di backoff** random e attende questo tempo solo se il canale è idle viceversa ferma il cronometro del backoff (per assicurarsi che nessun'altro usi il canale), se il tempo di backoff termina trasmette il frame e attende ACK

RECEIVER

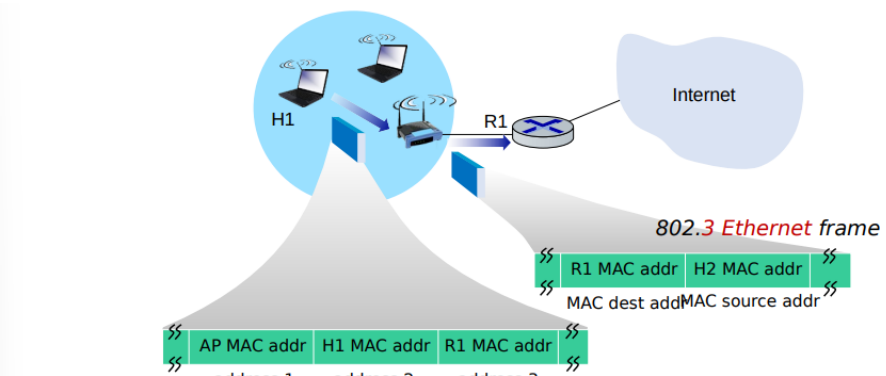
- Se il frame viene ricevuto correttamente (e supera il check degli errori) allora restituisce un **ACK** dopo un certo **SIFS** (intervallo di tempo)

MODALITA' CON PRENOTAZIONE: il sender invia una piccola richiesta **RTS** all'AP usando CSMA, se il canale è disponibile l'AP risponde in broadcast con un **CTS** dicendo che un canale è riservato per un particolare nodo per un dato tempo, il sender trasmette i suoi data frames e gli altri aspettano. Nella pratica questa modalità non è molto utilizzata

802.11 FRAME: ADDRESSING



L'AP ha un suo indirizzo MAC a cui l'HOST deve indirizzare i suoi frame (in caso in cui un host è coperto da più AP bisogna sempre specificare l'indirizzo MAC dell'AP), per il router è trasparente se c'è o meno un AP mentre per l'host non lo è perché viene specificato il MAC dell'AP



CARATTERISTICHE AVANZATE

- **Rate adaptation**: la base station dinamicamente modifica la velocità di trasmissione per adattarmi all'host e mantenere la probabilità di errore bassa
- **Power management**: spesso i nodi wireless utilizzano una batteria e per preservare la batteria un nodo può comunicare all'AP che entra in sleep fino al prossimo beacon frame e l'AP non invia pacchetti al nodo, al risveglio il beacon frame contiene una lista di frame arrivati mentre il nodo era in sleep e il nodo rimane sveglio altrimenti torna a dormire

802.15: PERSONAL AREA NETWORK

Pensate per avere una copertura limitata (meno di 20m) sono un'evoluzione della specifica Bluetooth che era proprietaria per sostituire piccole connessioni con cavo (mouse, tastiera, cuffie, …), si crea una rete ad hoc senza utilizzare un'infrastruttura esterna.
Ci sono due tipologie di nodi:

- Master: permette o meno agli slave di inviare informazioni
- Slaves: richiedono il permesso al master di inviare le informazioni

BLUETOOTH

Sviluppato nel '94 dalla Ericsson, nato per rimpiazzare i cavi non ha infrastruttura la rete è ad hoc, il range è limitato anche perché il consumo di energia deve essere molto basso per salvaguardare la batteria dei device.
Queste reti sono organizzare in **Piconet** che includono al massimo 8 device (1 master e 7 slave) e supportano al massimo 200 dispositivi però inattivi.
Gli slave devono essere sincronizzati con il master e fanno le richieste, il master permette la comunicazione o il risveglio di dispositivi inattivi.

Si possono organizzare più reti Piconet in reti **Scatternet** facendo in modo che un master connetta più Piconet mettendo in comunicazione nodi di più piconet tra loro

COMMUNICATION

Utilizza la tecnica frequency hopping spread spectrum divide la banda in 79 canali (**FDM**), un device cambia il canale di trasmissione 1600 ch/sec, la sequenza pseudocasuale è comune a tutti i membri della piconet -> il seed per la generazione casuale è definito dal Master e questa organizzazione serve per evitare le interferenze; gli slave devono essere sincronizzati sullo stesso canale in uso in quel momento.

Nell'intervallo in cui viene utilizzato un certo canale viene utilizzato **TDM** ovvero il master definisce slot da 625 usec, gli slot pari vengono utilizzati dal master e i dispari dallo slave.

ZIGBEE 802.15.4

Sono nati per mettere in comunicazione IoT (internet of things) come ad esempio dei sensori, dispositivi per la domotica, …
Hanno dei requisiti particolari nello specifico consumano poca energia, hanno spesso una batteria propria e non sono connessi alla rete elettrica quindi il protocollo deve consumare poco, il troughtput può essere più basso e avere una minore latenza perché non fondamentali.

Utilizza una topologia mesh: tipologie di tipo star e può essere estesa ad albero o mesh per avere più percorsi e fault tollerance.

ARCHITETTURA

Ci sono due tipologie di indirizzi:

- 64 bit: che identifica lo specifico dispositivo
- 16 bit: viene assegnato dinamicamente quando un dispositivo si connette alla WPAN e identifica il servizio

Tre tipologie di nodi:

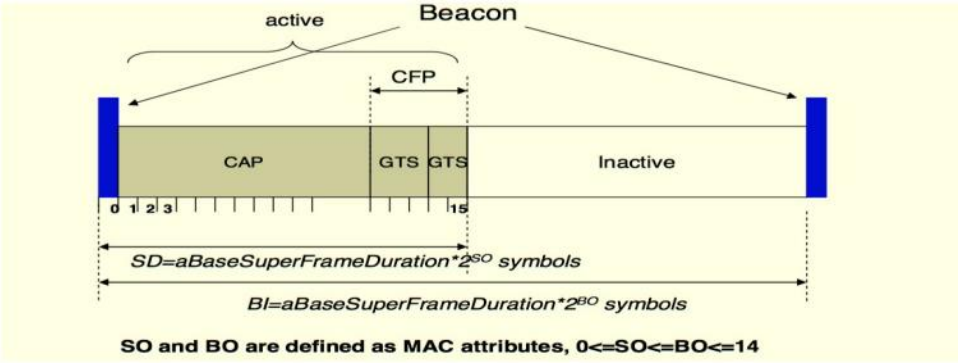
- PAN Coordinator: mantiene la rete, inserisce e configura i dispositivi che chiedono accesso
- Full function devices (FFDs): lavorano anche come router e istradano pacchetti
- Reduced function devices (RFDs): lavorano solo come end-point non fanno da router

MEDIUM ACCESS CONTROL

Essendo una rete con diversi device al suo interno bisogna implementare delle politiche di controllo degli accessi: il MAC layer stabilisce e gestisce i **superframes** e controlla gli accessi al canale, specifica come sono fatti i frame e invia ACK.
Due soluzioni:

- **Slotted CSMA/CA**
- **CSMA/CA**

Il superframe



Z-WAVE

È un protocollo proprietario basato su una **topologia mesh** dove ogni dispositivo (non alimentato a batteria) diventa un repeater di segnale.
I device possono comunicare Point-to-Point fino a 35 metri, le reti Z-WAVE possono essere interconnesse tra loro e ogni rete può supportare fino a 232 devices (In Europe, lavorano a 868,42 MHz).

Tutti i messaggi scambiati tra i dispostivi vengono chiamati **comandi** e sono organizzati in classi con funzionalità correlati questo permette di assegnare le classi di comandi a certi dispositivi; quindi, dispositivi progettati da aziende diverse ma che supportano la stessa classe di comandi possono comunicare tra loro.

RETI MOBILI

ARCHITETTURA RETE 4G-LTE

Viene prevista sempre una **base station** dell'ISP (tim, vodafone, ecc..) che è collegata a device che fanno da **switch** e fornisce porzioni di canali radio ai device mobili, un **dispositivo mobile** si collega alle base station, che coprono una certa area detta **cella,** e quando si sposta effettua **handoff** per collegarsi alla nuova base station.
Componenti della rete

- **eNodeB:** corrisponde alla base station il suo ruolo nel piano dei dati è quello di trasmettere i datagrammi tra UE (attraverso la rete di accesso radio LTE) e **P-GW.** I datagrammi dell'UE sono incapsulati nell'eNodeB e inviati in tunneling al P-GW attraverso il nucleo di rete completamente basato su IP; inoltre gestisce le segnalazioni di controllo registrazione e mobilità per conto dell'UE.
- il **Packet Data Network Gateway** (**P-GW**) assegna gli indirizzi IP agli UE e volge le operazioni di incapsulamento/decapsulamento durante l'inoltro di un datagramma a / da un UE.
- Il **Serving Gateway (S-GW)** è il nodo di appoggio della mobilità nel piano dei dati: tutto il traffico UE passerà attraverso il S-GW, che svolge anche le funzioni di fatturazione e intercettazione del traffico.
- Il **Mobility Management Entity (MME)** esegue la connessione e la gestione della mobilità per conto dell'UE residente nella cella che controlla. Riceve informazioni sulla sottoscrizione UE dall'HHS.
- **Home Subscriber Server (HSS)** contiene le informazioni dell'UE quali la capacità di roaming, il profilo della qualità di servizio e le informazioni di autenticazione, l'HSS ottiene queste informazioni dal fornitore dell'UE.

Separazione tra:

- **Control Plane**: costituito da Base station, MME, HSS, P-GW
- **Data plane**: base station, S-GW, P-GW -> vengono utilizzati protocolli specifici sia a livello link che fisico

Il Packet Data Convergence effettua la compressione degli header per velocizzare la trasmissione e la cifratura dei dati, il Radio Link control: frammentazione e ricostruzione del pacchetto con trasferimento affidabile basato su ACK

Medium Access: gestisce il canale e la loro assegnazione a dispositivi mobili

OFDM – orthogonal frequency division multiplexing: a livello fisico si usa soluzioni basate su una combinazione di FDM e TDM, all'interno di ogni canale viene diviso il tempo in slot e assegnato ad ogni device (posso assegnarli più slot per velocizzare il servizio).
È asimmetrico i canali possono essere downstream o upstream, sono separati perché nella maggior parte dei casi è richiesta più capacità di downstream.
Ogni device alloca due o più time slot su 12 frequenze diverse, l'algoritmo di schedulazione è stabilito dal provider dei servizi.

Tunneling: i datagram sono incapsulati utilizzando il GPRS tunneling protocol dentro datagram UDP, questo permette di gestire la mobilità cambiando gli endpoint (estremi) dei tunnel passando ad esempio da una base station ad un'altra mantenendo invariati gli indirizzi.

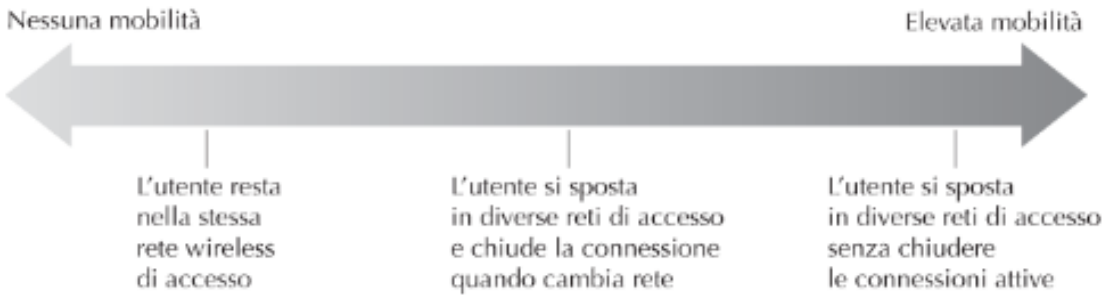
EVOLUZIONE DELLE TIPOLOGIE DI RETI MOBILI

- **RETE 2G**: inizialmente era solo voce
- **RETE 3G:** voce + dati, si è suddivisa l'infrastruttura di rete in due parti -> rete telefonica vera e propria doveva veniva inoltrata la comunicazione voce e la rete dati veniva dirottata sulla rete di internet (vantaggio di non modificare la rete telefonica già esistente)
- **RETE 4G-LTE**: sono state integrate le due infrastrutture -> rete pubblica telefonica e rete internet, la stessa informazione telefonica viene inglobata nella rete internet (rete IP)

RETE 5G: L'obiettivo è aumentare di 10 volte il picco di trasmissione e decrementare la latenza di 10 volte e aumentare la capacità di traffico di 100 voltre
Utilizza segnali a frequenze molto elevate e quindi una maggiore capacità di trasmissione / velocità / banda (nuove radio FR1 da 450 Mhz a 6 GHz e FR2 da 24GHz a 52GHz).
Utilizza antenne MIMO: multiple directional antennae con frequenze di onda millimetriche con difficoltà perché più ci si avvicina a frequenze vicine alla luce più è un problema far attraversare il segnale a materiali come edifici ad esempio: il protocollo, quindi, gestisce la frequenza per garantire la copertura (antenne con copertura minore rispetto al 4G), il diametro di queste pico-cells è di 10-100 metri -> è necessari aumentare notevolmente il numero di base station.

PRINCIPI DELLA MOBILITA'

COS'E LA MOBILITA' E COME VIENE GESTITA



La mobilità non viene gestita a livello globale ma viene gestita sulla edge network o rete di accesso questo permette di scalare la soluzione (routing indiretto / diretto).

Home network: è la rete IP di appartenenza del dispositivo mobile, tipicamente la rete a cui si collega attraverso un provider (rete cablata) o telefonia mobile per i telefoni, su questa rete vi è

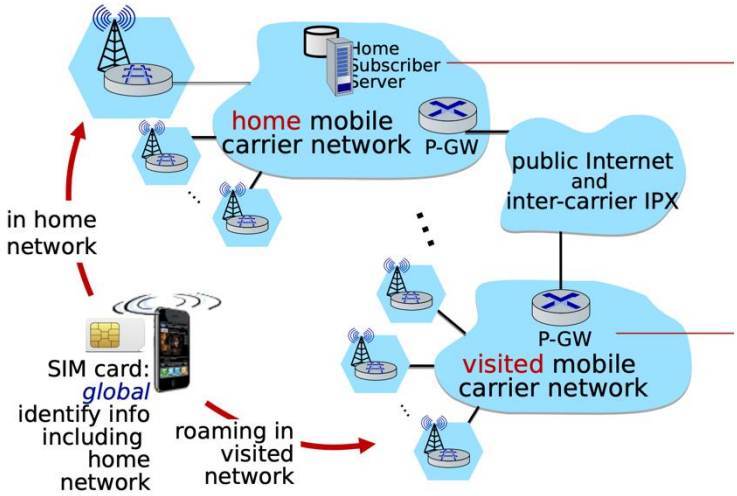
associato un **indirizzo permanente** (SIM card) ed infine l'**home agent** che si occupa di gestire la mobilità in modo trasparente per il nodo (HSS mantiene le informazioni del dispositivo).

Foreign / Visited Network: rete a cui si collega un host quando si sposta su un'altra rete (esempio roaming) dove viene assegnato un care-of-address, il **Foreign agent** implementa la trasparenza ovvero permette di mantenere lo stesso IP/numero di telefono anche in Foreign network attraverso l'utilizzo del **COA care-of-address**.

Il COA può essere assegnato dal foreign agent e comunicato poi all'home agent oppure il nodo mobile può apprendere tramite DHCP il suo COA e comunicarlo lui stesso al suo home agent.

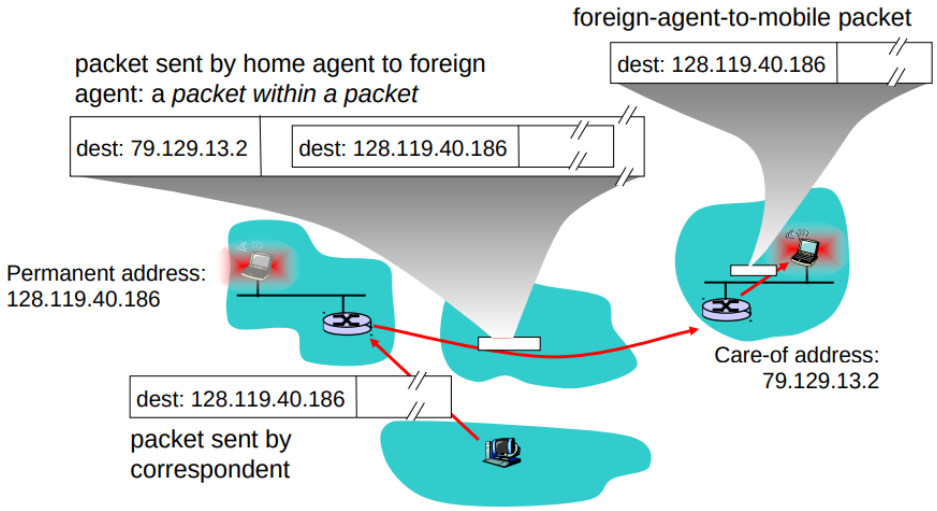
Registrazione: quando un nodo mobile si sposta dalla home network alla visited network richiede di connettersi alla rete tramite il Foreign agent che fornisce indirizzo (DHCP) e ne tiene traccia poi contatta l'**home agent** per "avvisarlo" che il nodo mobile risiede nella sua rete.
Un host che vuole inviare un messaggio contatta tramite IP l'home network:

- **Indirect Routing**: mobilità completamente trasparente -> se il nodo mobile si è spostato si registra presso il foreign agent che gli assegna un COA e lo comunica all'home agent del nodo mobile, successivamente i pacchetti diretti all'home network verranno re-instradati dall'home agent al foreign agent della foreign network attraverso il COA e i pacchetti saranno incapsulati (home agent incapsula il pacchetto con IP permanente in un datagram più grande con COA) per mantenere questa architettura trasparente ai livelli superiori Problema dell'istradamento triangolare: questa triangolazione diventa inefficiente se i due nodi mobili sono nella stessa rete, perché esistono percorsi più efficienti.
- **Direct Routing**: supera il problema dell'istradamento triangolare ma introducendo una maggiore complessità -> il corrispondete fa la richiesta verso la home network (home agent) che risponde dando il nuovo indirizzo care-of-address del nodo mobile permettendogli di contattarlo direttamente (sempre tramite tunneling).

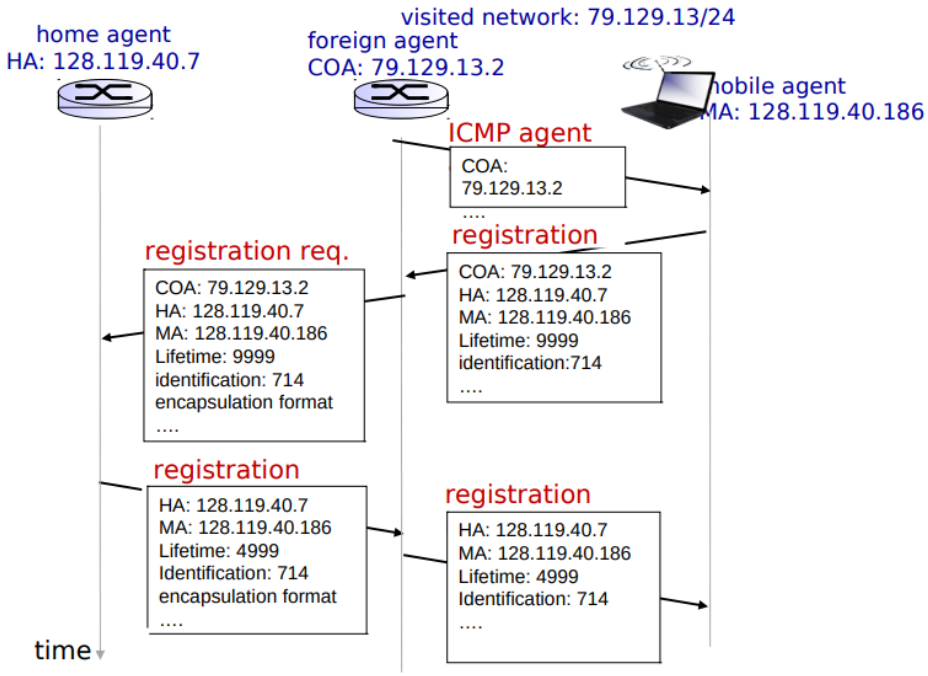


MOBILE IP

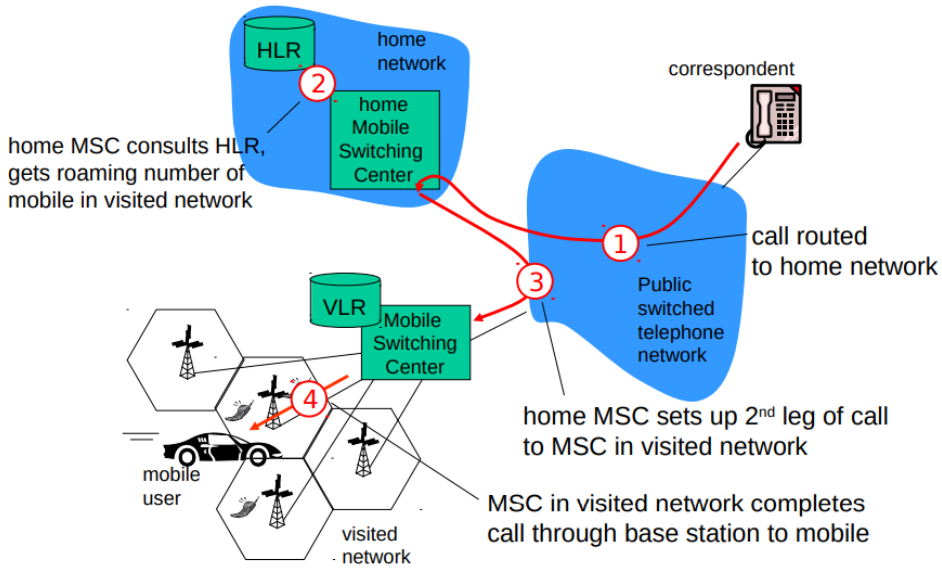
Utilizza **l'Indirect Routing**:



Agent advertisement: quando un nodo entra in una nuova rete il protocollo prevede che gli agent mandino in broadcast un messaggio ICMP con tipo 9 che prevede l'indirizzo sorgente di chi invia il messaggio (agent)



GSM



HANDOFF: l'host si sposta da una base station ad un'altra, l'handoff deve fare in modo che non venga persa la chiamata.
Oppure si effettua handoff per bilanciare il carico tra base station ed evitare il sovraccarico, il protocollo definisce solo i meccanismi non le politiche.

È iniziato dalla vecchia base station (BSS) che avvisa il mobile switch center (MSC) che fornisce una lista di base station disponibili per il nodo mobile e alloca le risorse (porzione di canale e frequenze) segnala che è pronta per l'handoff che viene inoltrata alla vecchia BSS che informa il nodo mobile che si assocerà alla nuova BSS.

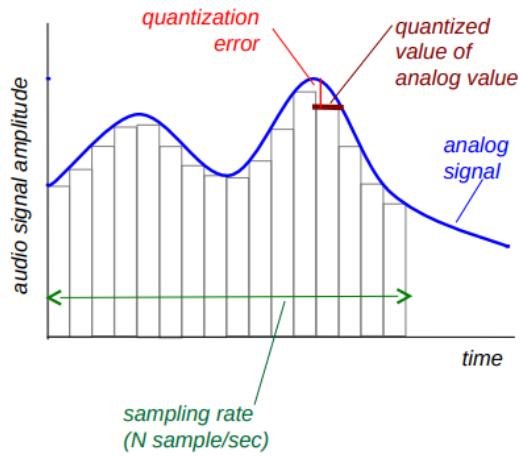
MULTIMEDIA NETWORKING

APPLICAZIONI

AUDIO

Il segnale audio analogico, che varia con continuità e che deriva da un discorso o da della musica, viene normalmente convertito in un segnale digitale secondo il seguente schema:

- si procede al **campionamento** del segnale analogico a una frequenza fissata
  - Telefoni: 8000 samples/sec
  - CD music: 44100 samples/sec
- si procede poi con l'operazione di **quantizzazione**, durante la quale i campioni sono arrotondati a numeri interi in un intervallo finito di valori (solitamente potenze di due)
- Tutti i valori di quantizzazione sono rappresentati dallo stesso numero di bit. Per esempio, se ci sono 256 valori di quantizzazione, tutti i valori (e quindi tutti i campioni audio) sono rappresentati da 1 byte. Le rappresentazioni in bit di tutti i campioni vengono poi concatenate a formare la rappresentazione digitale del segnale; maggiori sono i bit migliore sarà l'accuratezza del campionamento del segnale



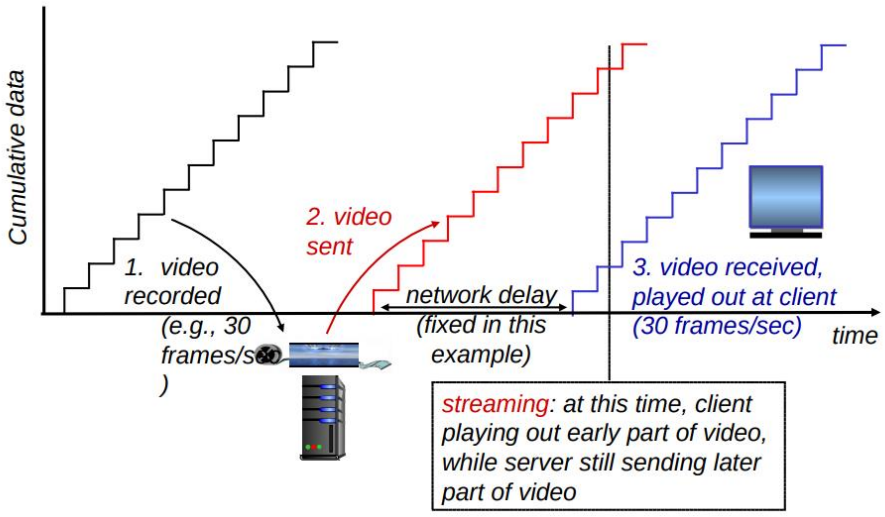
VIDEO

La sequenza di immagini / frame viene campionata ad un livello costante e ogni immagine viene codificata in un array di pixel ed ogni pixel viene rappresentato da un certo numero di bit che darà l'accuratezza dei colori; queste immagini vengono campionati ad una frequenza di 24, 30, 60 frame/sec.
Viene sfruttata la ridondanza all'interno dell'immagine per trasmettere una volta sola, ad esempio, una certa tonalità di colore per una certa area -> algoritmi per la compressione delle immagini perdo di qualità ma ho il vantaggio di utilizzare meno bit.

TRE TIPOLOGIE DI APPLICAZIONI

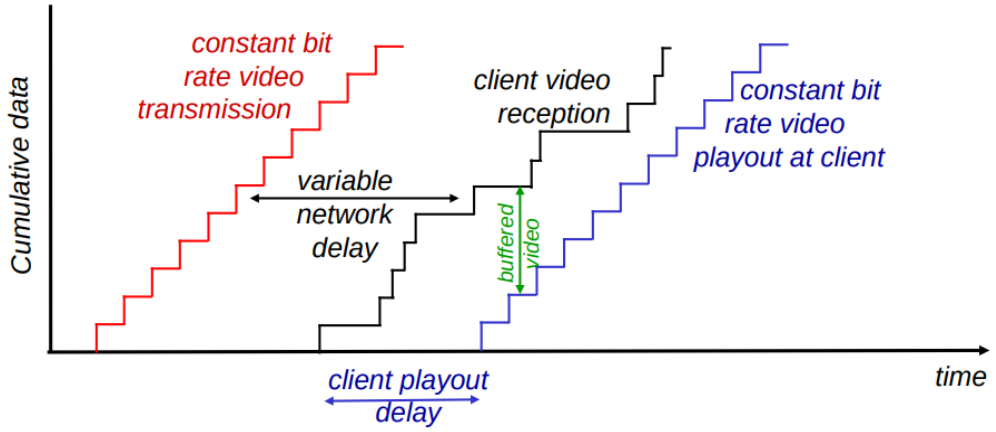
1 - STREAMING STORED

In questa classe di applicazioni i contenuti sono video, quali film, trasmissioni televisive, eventi sportivi o YouTube, memorizzati su server a disposizione degli utenti su richiesta (on demand).
Il client fa richiesta e man mano che viene scaricato il video viene visualizzato dal player è immagazzinato nei server e può essere trasmesso molto velocemente, gli utenti possono guardare i video dall'inizio alla fine senza interruzioni, possono fermare la visione prima della fine o interrompere il video mettendolo in pausa e ricominciando da una scena passata o successiva

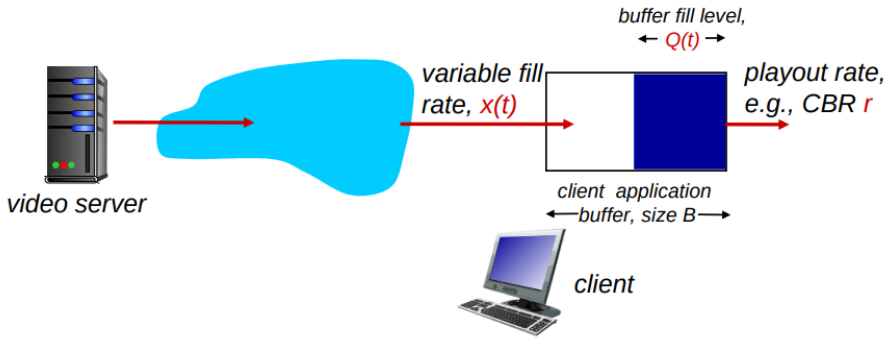


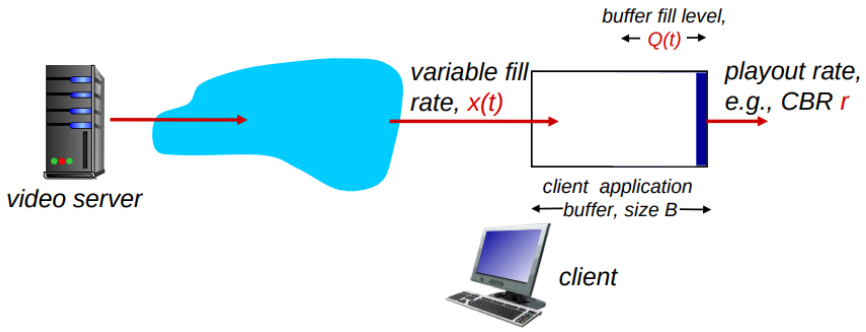
Bisogna far in modo di riprodurre in modo continuo un video mantenendo lo stesso rate di produzione dei vari frame ma il ritardo non è fisso (congestione, perdite, …) quindi il client per

gestire i ritardi utilizza un buffer per immagazzinare i frames e poi riprodurli.
Il server deve poter percepire le eventuali pause di riproduzione / avanzamenti / o le perdite di pacchetto da parte del client.



Una soluzione è attendere prima dell'inizio del video nel quale il client bufferizza dei frame per poter rendere fluida la visualizzazione del video e compensare eventuali perdite o ritardi (**bufferizzazione**)



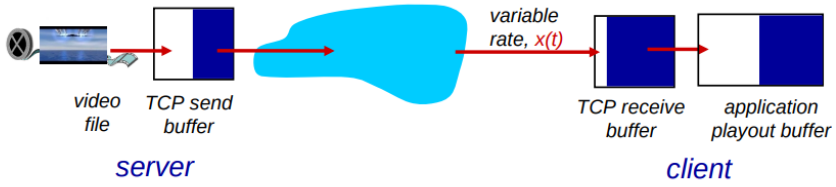


UDP

È un protocollo che viene utilizzato per lo streaming, il sender invia i frames al client con un tasso costante nella speranza che il client li riceva e riesca a gestirli senza perdite; non viene garantito controllo di errori, ritardi -> politica best effort, un'altra problematica è che molte volte UDP non viene fatto passare dai firewall.
Client e Server mantengono oltre al flusso video anche, in parallelo, una connessione di controllo separata sulla quale il client invia i comandi riguardanti i cambiamenti di stato della sessione, quali la pausa, la ripresa della riproduzione, il riposizionamento e così via

HTTP

Il video viene semplicemente memorizzato in un server HTTP come un file ordinario con un URL specifico -> utilizza TCP, viene fatta una HTTP GET per richiede un video, il server viene inviato al massimo rate possibile ma essendo su TCP la velocità di trasmissione viene gestita per evitare congestioni e controllo di flusso.
Nel caso in cui il client metta in pausa il video il buffer del ricevente verrà riempito ma TCP avvertirà il server sul tasso trasmissivo da tenere (nel caso di fermarsi) -> controllo di flusso.
Un'altro vantaggio è "saltare" ad un punto del video perché nella richiesta è possibile specificare il range di byte richiesto (byte-range).



DASH - Dynamic Adaptive Streaming over HTTP: il server divide il file in chunck ognuno salvato, codificato a differenti rates; il file manifest fornisce gli url per i differenti chunck a seconda della qualità (bts/frame) mentre il client misura periodicamente la banda di ricezione e richiede di conseguenza chunck che può gestire in basa alla banda disponibile in quel momento.

CDN – Content Distribution Networks
Avere un unico grosso datacenter non è sostenibile e presenta diversi problemi come la lontana degli host, il troughput sarà strozzato dal collegamento con throughput minore (bottleneck), ci sarà un singolo punto di rottura in caso di crash del datacenter non sarà possibile accedere ai contenuti.
Per ovviare a questi problemi quasi tutte le aziende di video streaming usano le CDN che gestiscono server distribuiti in molti posti diversi memorizzano copy dei video e cercano di dirigere le richieste degli utenti al punto della CDN in grado di offrire servizio migliore.
Ci possono essere CDN private ovvero del fornitore dei contenuti o CDN di terze parti che forniscono contenuti per molte aziende di streaming, adottano le seguenti politiche:

- Enter deep: proposta da Akamai si entra in profondità nelle reti di accesso degli SP installando gruppi di server detti cluster, l'obiettivo è quello di essere vicini agli utenti finali in modo da migliorare il ritardo percepito e il troughput; più complicato gestire e fare manutenzione a tutti i server
- Bring Home: vengono costruiti grandi cluster in pochi punti chiave e interconnessi usando una rete privata ad alta velocità, invece di entrare negli ISP, gli stessi ISP vengono attirati in questa rete perché i cluster sono posti vicino ai PoP di molti ISP di primo livello

Come funziona: quando un host chiede il recupero di uno specifico video identificato da un URL, la CDN deve intercettare la richiesta in modo da poter determinare il cluster più appropriato e dirigere la richiesta del client a uno dei server di quel cluster.
Molte CDN sfruttano il servizio di NS per intercettare e ridirigere le richieste. Strategie di scelta dei cluster: la CDN apprende l'indirizzo IP del server LDNS del client attraverso la richiesta DNS del client successivamente seleziona un cluster appropriato basandosi sull'indirizzo IP appena appreso:

- Cluster geograficamente più vicino: viene usato un database di geo localizzazione funziona abbastanza bene per una buona parte dei client però per alcuni client potrebbe non andar bene perché il percorso più vicino geograficamente potrebbe essere diverso da quello più vicino dal punto di vista del percorso di rete; inoltre, alcuni utenti utilizzano LDNS remoti falsando così la geo localizzazione

- Controllo del traffico: vengono effettuate misure in tempo reale delle prestazioni di ritardo e perdita tra i loro cluster e loro cliente attraverso ping o interrogazioni DNS; un problema di questo approccio è che molti LDNS sono configurati per non rispondere a tali richieste.
-

2- CONVERSATIONAL

VoIP

voice/video over IP il requisito è il poter interagire quindi il ritardo deve essere minimo altrimenti il servizio sarà percepito in modo negativo.
Quasi tutte le applicazioni di VoIP fanno uso per default di UDP, senza curarsi della ritrasmissione dei pacchetti persi. UDP viene usato da Skype a meno che l'utente sia dietro un NAT o un firewall che blocca i segmenti UDP, nel qual caso usa TCP.
Per un'applicazione VoIP, ritardi end-to end complessivi inferiori a 150 ms non sono percepiti dall'orecchio umano, fra 150 e 400 ms possono essere accettabili ma non ideali, se invece superano i 400 ms possono limitare seriamente l'interattività nella conversazione.

Jitter: Un aspetto cruciale del ritardo end-to-end è costituito dalla variabilità nelle code dei router, che può generare sostanziali differenze nel tempo impiegato da ciascun pacchetto tra origine e destinazione, da quando viene creato a quando viene ricevuto.
Se il ricevente ignora il jitter, e riproduce i blocchi man mano che sopraggiungono, la qualità audio può risultare non intelligibile. Fortunatamente, spesso il jitter può essere rimosso tramite numeri di sequenza (**sequence number**), marcature temporali (**timestamp**) e ritardo di riproduzione (**playout delay**).
Per rimuovere il Jitter al ricevente si utilizzano due strategie:

- Facendo precedere i blocchi da una marcatura temporale. Il trasmittente contrassegna ciascun blocco con l'indicazione dell'istante in cui è stato generato.
- Inserendo un ritardo nella riproduzione del blocco al suo ricevimento, che deve essere abbastanza lungo da consentire la ricezione della maggior parte dei pacchetti prima di iniziare la loro riproduzione

Ritardo di riproduzione fisso:il ricevente tenta di riprodurre ciascun blocco esattamente q millisecondi dopo che è stato generato;se un blocco è contrassegnato da un tempo di generazione t, il ricevente lo riproduce nell'istante t + q.
Scelta di q: sebbene la qualità sia migliore con valori minori di q. D'altra parte, se q è molto inferiore a 400 ms, molti pacchetti arriverebbero troppo tardi rispetto all'istante in cui sono programmati per la riproduzione a causa del jitter. In presenza di ampie variazioni nel ritardo end-to-end, è preferibile utilizzare un elevato valore di q; se invece i ritardi sono minimi, è meglio utilizzare un valore di q inferiore a 150 ms.

Ritardo di riproduzione adattativo: viene stimato il ritardo della rete e le sue variazioni, regolando conseguentemente il ritardo di riproduzione con l'inizio di ciascun periodo di attività vocale; algoritmo generale:

- t_i = marcatura temporale dell'i-esimo pacchetto = istante in cui il pacchetto è generato dal mittente;
- r_i = istante in cui il pacchetto i è ricevuto;
- p_i = istante in cui il pacchetto i è riprodotto.

d_i è una stima del valore medio del ritardo alla ricezione dell'i-esimo pacchetto

$$d_i = (1 - u)\, d_{i-1} + u\, (r_i - t_i)$$

v_i una stima della deviazione media dal ritardo medio stimato

$$v_i = (1 - u)\, v_{i-1} + u \mid r_i - t_i - d_i \mid$$

Una volta calcolate queste stime, il ricevente impiega il seguente algoritmo per la riproduzione dei pacchetti. Se i è il primo pacchetto di un periodo di attività, il suo istante di riproduzione è dato da:

$$p_i = t_i + d_i + Kv_i$$

il punto di riproduzione per ogni pacchetto successivo è calcolato come lo spostamento dal momento in cui è riprodotto il primo pacchetto.
Questo algoritmo funziona perfettamente quando il ricevente sa se il pacchetto è il primo di un periodo di attività vocale; e questo può essere dedotto attraverso l'esame dell'energia del segnale in ogni pacchetto.

Recupero dei pacchetti persi: le applicazioni VoIP utilizzano spesso alcuni schemi di anticipazione delle perdite, due tipi di questi schemi sono:

correzione anticipata degli errori (FEC, forward error correction): L'idea base di questo schema è quella di aggiungere informazioni ridondanti al flusso originale dei pacchetti. In cambio di un aumento marginale nel tasso trasmissivo dell'audio, la ridondanza può essere utilizzata per fornire un'approssimazione dell'esatta versione di alcuni pacchetti persi, due meccanismi:

- 1: invia, dopo ogni n blocchi, un blocco ridondante ottenuto da un'operazione di OR esclusivo degli n blocchi originali, In questo modo, se qualche pacchetto del gruppo degli n + 1 pacchetti va perso, il ricevente lo può ricostruire integralmente
- 2: consiste nell'inviare uno stream audio a bassa risoluzione come informazione ridondante. Per esempio, il trasmittente può creare un flusso audio nominale e un corrispondente flusso a bassa risoluzione con bit rate più basso, in questo schema al ricevente sono sufficienti due pacchetti prima della riproduzione e questo, quindi, fa in modo che l'aumento del ritardo di riproduzione sia piccolo. Inoltre, se la codifica a bassa velocità è molto inferiore alla codifica nominale, allora anche l'aumento marginale della frequenza trasmissiva sarà contenuto.

l'interfogliazione (interleaving): il trasmittente pone in sequenza le unità dati audio, in modo che quelle adiacenti siano separate da una data distanza nel flusso trasmesso, la perdita di un singolo pacchetto da un flusso interfogliato genera numerose piccole lacune nel flusso ricostruito, invece di una più vasta che si sarebbe verificata in uno flusso sequenziale.

3- STREAMING LIVE: audio video, ad esempio eventi sportivi live

PROTOCOLLI PER APPLICAZIONI IN TEMPO REALE

RTP

Può essere utilizzato per trasportare formati comuni come PCM, ACC e MP3 per l'audio e MPEG e H.263 per il video, ma anche per formati proprietari:

Normalmente RTP utilizza UDP: il lato trasmittente incapsula un blocco di dati audio o video in un pacchetto RTP, incapsula poi quest'ultimo in un segmento UDP e lo affida a IP. Il lato ricevente estrae il pacchetto RTP dal segmento UDP, recupera il contenuto multimediale dal pacchetto e lo passa al media player per la decodifica e la riproduzione.

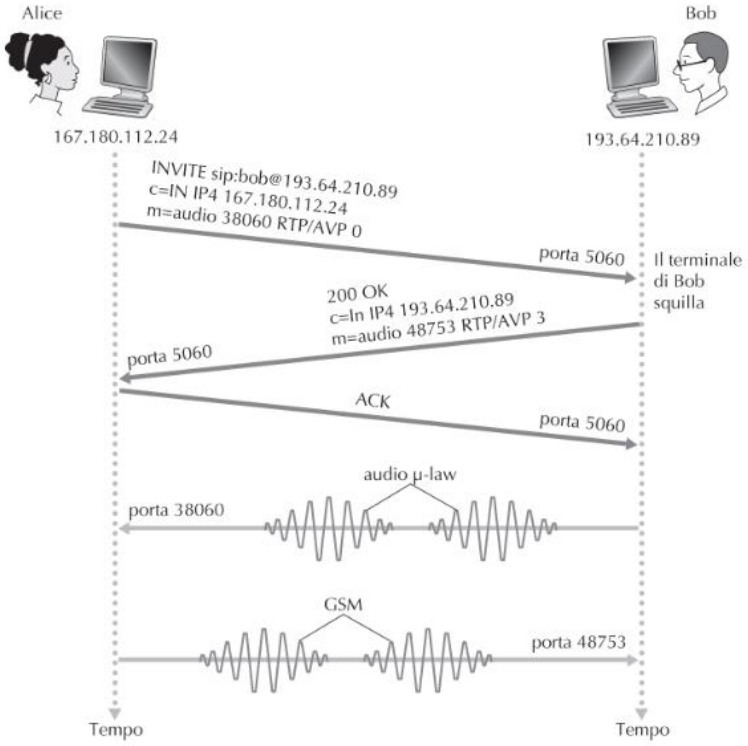
Figura 9.8 Campi di intestazione RTP.

- Numero di sequenza (16 bit). incrementato di un'unità per ogni pacchetto RTP inviato e può essere utilizzato dal ricevente per rilevare le perdite e ricostruire la sequenza dei pacchetti.
- Marcatura temporale (32 bit). Riporta l'istante del campionamento del primo byte nel pacchetto dati RTP, il ricevente la può utilizzare per rimuovere il jitter dei pacchetti introdotto dalla rete e per fornire una riproduzione sincronizzata. Nel caso dell'audio, l'orologio è incrementato di un'unità a ogni campionamento.
- Identificatore della sorgente di sincronizzazione (32 bit). Identifica la sorgente del flusso RTP. Di solito ogni flusso di una sessione RTP ha il proprio SSRC (synchronization source identifier). Questo indicatore non è l'indirizzo IP del trasmittente, ma un numero che la sorgente assegna arbitrariamente quando inizializza un nuovo flusso. La probabilità che a due flussi venga assegnato lo stesso SSRC è molto bassa. Qualora dovesse accadere, le due sorgenti sceglierebbero un nuovo valore.

SIP

Servizi offerti:

- Fornisce i meccanismi che consentono al chiamante di connettersi al chiamato su una rete IP e notificargli che vuole iniziare una chiamata; permette ai partecipanti di accordarsi sulle codifiche dei contenuti multimediali e di terminare le chiamate
- Fornisce al chiamante i meccanismi necessari per determinare l'attuale indirizzo IP del chiamato. Gli utenti non hanno un unico indirizzo IP fisso, in quanto questo può essere assegnato dinamicamente (utilizzando DHCP) e gli utenti possono avere più dispositivi IP, ciascuno con un diverso indirizzo
- Fornisce le procedure per la gestione della chiamata, durante la quale è possibile aggiungere nuovi flussi multimediali, cambiare la codifica, invitare nuovi partecipanti, trasferirla o metterla in attesa.



CARATTERISTICHE

- i messaggi SIP sono inviati e ricevuti su socket diverse da quelle utilizzate per inviare e ricevere i dati audio (o video).
- i messaggi SIP sono in ASCII leggibile e assomigliano ai messaggi HTTP.
- SIP richiede che tutti i messaggi abbiano un acknowledgement, quindi può funzionare sia con UDP sia con TCP.

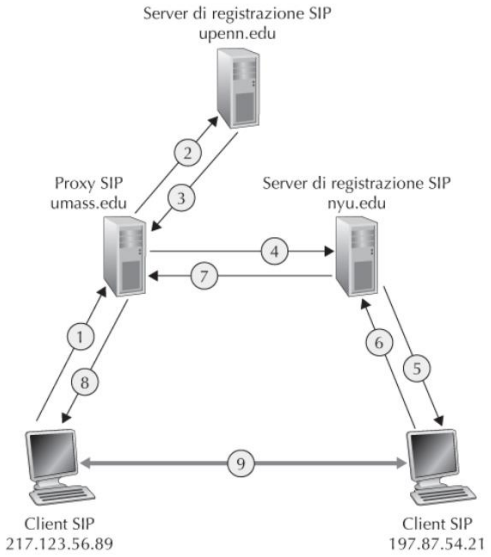
MESSAGGIO SIP: INVITE

```
INVITE sip:bob@domain.com SIP/2.0
Via: SIP/2.0/UDP 167.180.112.24
From: sip:alice@hereway.com
To: sip:bob@domain.com
Call-ID: a2e3a@pigeon.hereway.com
Content-Type: application/sdp
Content-Length: 885
c=IN IP4 167.180.112.24
m=audio 38060 RTP/AVP 0
```

TRADUZIONE DEI NOMI E LOCALIZZAZIONE DEGLI UTENTI

Il mittente invia un INVITE a un SIP proxy. Questo fornirà una risposta che potrebbe includere l'indirizzo IP del dispositivo o, in alternativa, l'indirizzo IP della sua casella vocale oltre all'URL di una pagina web.
A ciascun utente è associato un server di registrazione SIP (**SIP registrar**) al quale l'applicazione SIP su un dispositivo, quando viene lanciata, invia un messaggio di registrazione contenente l'attuale indirizzo IP presso cui l'utente può essere contattato.

Il server di registrazione è simile a un DNS autoritativo: traspone gli identificativi fissi in linguaggio corrente (per esempio, sip:bob@domain.com) in indirizzi IP dinamici, l'altro traduce i nomi fissi degli host in indirizzi IP fissi. Spesso, server di registrazione SIP e proxy SIP sono eseguiti sulla stessa macchina.



SUPPORTO DI INTERNET ALLE APPLICAZIONI MULTIMEDIALI

Tre diversi approcci per supportare applicazioni multimediali a livello rete.

Approccio	Granularità	Garanzie	Meccanismo	Complessità	Adozione
Utilizzare al meglio il servizio best-effort	Tutto il traffico ovunque trattato allo stesso modo	Nessuna o lasche	Supporto al livello di applicazione CDN, overlay, erogazione, delle risorse a livello di rete	Minimale	Ovunque
Servizi differenziati	Classi di traffico differenti trattate diversamente	Nessuna o lasche	Marcatura dei pacchetti, controllo del profilo di traffico, scheduling	Media	Moderata
QoS garantita per singola connessione	Flussi individuali minimi trattati diversamente	Lasche e stringenti, una volta che il flusso è stato ammesso	Marcatura dei pacchetti, controllo del profilo di traffico, scheduling, call admission e segnalazione di eventi	Bassa	Minima

DIMENSIONAMENTO DELLE RETI BEST-EFFORT

Un approccio definitivo per migliorare la qualità delle applicazioni multimediali, che può essere spesso usato per risolvere qualsiasi problema dove le risorse sono limitate, è l'investimento di denaro per evitare contesa sulle risorse.

Significa fornire sufficiente capacità sui collegamenti in tutta la rete, in modo che la congestione della rete e le sue conseguenze di ritardo e perdita dei pacchetti non capitino mai, o almeno molto raramente, ciò potrebbe essere raggiunto senza cambiamenti all'architettura best-effort di Internet.

FORNITURA DI PIÙ CLASSI DI SERVIZIO

Un semplice modello di servizio migliore del best-effort consiste nel dividere il traffico in classi e fornire loro diversi livelli di servizio, a seconda della classe

Principi per la garanzia della qualità del servizio:

- **Principio 1**: La marcatura dei pacchetti (packet marking) consente ai router di distinguerli in base alla loro classe di traffico.
- **Principio 2**: È auspicabile che sia fornito un grado di isolamento tra le classi di traffico, in modo che una classe non subisca gli effetti negativi derivanti dal comportamento non conforme di un'altra.
- **Principio 3**: È auspicabile che l'utilizzo delle risorse (per esempio, buffer e larghezza di banda) sia quanto più efficiente possibile anche in presenza di isolamento delle classi, ad esempio usare la banda nella maniera più efficiente possibile, senza sprecarla quando è disponibile.

sono implementati entrambi al bordo della rete: in un sistema periferico o un router di bordo.

ARCHITETTURA INTERNET DIFFSERV

Fornisce una differenziazione dei servizi, vale a dire, la possibilità di gestire in maniera scalabile differenti classi di traffico in maniere distinte su Internet.
Il protocollo e l'architettura non forniscono le classi di servizio ma i componenti per gestirle/crearle.
L'architettura Diffserv è costituita da due gruppi di elementi funzionali:

- Funzioni periferiche (edge): classificazione dei pacchetti (marcatura) e condizionamento del traffico. All'ingresso della rete (cioè, o nell'host o nel primo router incontrato sul percorso), i pacchetti sono contrassegnati con un dato valore nel campo DS dell'intestazione IPv4 o IPv6 che sostituisce il campo ToS
- Funzioni interne (core): inoltro. Quando un pacchetto, con marcatura DS, giunge a un router Diffserv-compatibile viene inoltrato in base al cosiddetto comportamento ad ogni hop (PHB, per-hop behavior) associato alla classe del pacchetto. Questa funzione determina come buffer e larghezza di banda sono condivisi dalle classi di traffico.

Il secondo componente chiave dell'architettura Diffserv riguarda il PHB fornito dai router Diffserv-compatibili:

- Un PHB può fornire diverse prestazioni (cioè, distinti comportamenti di instradamento osservabili dall'esterno) a differenti classi di traffico.
- Un PHB definisce diverse prestazioni (comportamenti) per le classi, ma non impone alcuna particolare procedura per raggiungere questi comportamenti. Può essere utilizzata qualunque tecnica e qualsiasi politica di allocazione di buffer e larghezza di banda (black box).
- Le differenze nelle prestazioni devono essere osservabili e quindi misurabili.

Attualmente sono state definite due tipologie di PHB:

- Expedited forwarding specifica che il tasso trasmissivo di una classe di traffico dal router deve essere uguale o superiore a un valore prestabilito
- assured -forwarding suddivide il traffico in quattro classi, dove a ciascuna classe AF è garantita la fornitura di un quantitativo minimo di banda e di memorizzazione nei buffer.

FORNIRE GARANZIE DI QUALITÀ DEL SERVIZIO (QOS) PER OGNI CONNESSIONE: PRENOTAZIONE DELLE RISORSE E AMMISSIONE DELLE CHIAMATE

la rete non può garantire che un flusso in corso in una classe di traffico ad alta priorità continuerà a ricevere quel tipo di servizio per tutta la durata del flusso usando solo il meccanismo precedentemente descritto

- **Principio 4**. È necessario un processo di ammissione di chiamata durante il quale vengono confrontati i requisiti di servizio dei flussi (QoS richiesta) con le risorse disponibili in quel dato momento. Se la richiesta può essere soddisfatta il flusso potrà accedere alla rete, altrimenti il suo ingresso sarà negato.

Si rendono quindi necessari nuovi meccanismi e protocolli:

- Prenotazione di risorse: l'unico modo per garantire che una chiamata avrà le risorse necessarie (spazio nel buffer e banda sui collegamenti) per soddisfare la QoS desiderata è di allocare esplicitamente quelle risorse per la chiamata, (esource reservation). Una volta che le risorse sono state allocate, la chiamata ha accesso a richiesta a queste risorse per tutta la sua durata, indipendentemente dalle richieste di altre chiamate.
- Call admission: se le risorse sono riservate, allora la rete deve avere un meccanismo tramite il quale le chiamate richiedono e riservano le risorse, un processo noto come call admission. Poiché le risorse non sono infinite, a una chiamata sarà negata la sua richiesta di ammissione, cioè sarà bloccata, se le risorse richieste non sono disponibili.
- Segnalazione per l'instaurazione della chiamata: il processo di call admission descritto precedentemente richiede che la chiamata possa riservare le risorse sufficienti per assicurarsi che i requisiti di QoS end-to-end di cui necessita possano essere soddisfatti dai router collocati sul percorso tra sorgente e destinazione. Questo processo di instaurazione della chiamata (call setup) richiede che i router determinino le risorse locali richieste dalla sessione, considerino quelle già impegnate e stabiliscano se dispongono di risorse sufficienti per soddisfare i requisiti di QoS, ovviamente senza sottrarle a sessioni già in corso. Per coordinare queste attività si utilizza un protocollo di segnalazione (call setup protocol) -> protocollo RSVP

ZEROCONF – ZERO CONFIGURATION NETWORKING

È nato per far interagire dispositivi differenti connessi in rete con il minimo sforzo di configurazione della rete e dei dispositivi

ORIGINI

È stato sviluppato da Apple che cercava un modo semplice per l'utente per trovare le stampanti in modo semplice e per condividere file (Apple Talk) ma poi è stato utilizzato anche con altri scopi. Attraverso l'IETF si è standardizzato il protocollo con l'obiettivo di permette la comunicazione in rete senza alcuna configurazione da parte dell'utente e anche dell'amministratore di rete.

DI COSA SI NECESSITA

- Essere connessi alla rete, via ethernet o wireless
- Indirizzo IP
- Nome (per trovare l'ip)
- Un modo per reperire i service di rete: DHCP, DNS, …

Questi servizi comportano la necessità di un amministratore di rete che gestisca e configuri questi servizi mentre in una rete ad HOC potrebbe essere più complicato e si vuole ridurre questa complessità, vengono quindi utilizzati metodi alternativi:

IP CONFIGURATION

Si ottiene l'IP in modo automatico senza DHCP server, si permette l'indirizzamento dei dispositivi solo in una rete locale (sullo stesso link) viene quindi scelto un indirizzo casuale IPv4/IPv6 nella sottorete 169.254/16 e si assicura che questo indirizzo non venga utilizzato da altri (la probabilità è bassa sono circa 2^{16} indirizzi diversi circa 65.000 indirizzi diversi).
Per ottenere l'IP causale si utilizza un seme (tipicamente derivata dal MAC address del dispositivo), successivamente attraverso il meccanismo ARP: si invia una richiesta ARP con l'indirizzo generato e se non si riceve risposta allora nessuno avrà lo stesso IP altrimenti viene rigenerato l'IP; gli altri device salvano l'informazione ricevuta in broadcast con IP/MAC per utilizzarla poi per comunicare.

HOSTNAME RESOLUTION

Viene utilizzato il mMNS (multicast) con lo stesso formato di richieste del DNS unicast ma la differenza è che viene effettuato in broadcast (senza server) il device deve aggiungersi al gruppo multicast (224.0.0.251 perIPv4) e ogni host deve essere in grado di rispondere alle richieste DNS.
L'host name viene scelto dall'host/user e viene effettuato un procedimento di "difesa" dell'hostname come per l'ip (tramite protocollo ARP).
Ci possono essere due risposte DNS (le risposte vengono ricevute da tutte i client del gruppo):

- Singola: si richiede un particolare nome a fronte di un indirizzo IP (risoluzione del nome)
- Multipla: estende la semantica delle richieste DNS aggiungendo la possibilità di richiedere un certo servizio, per esempio, i device che possono stampare (possono essere più di uno e quindi ricevo risposte multiple) oppure in caso di conflitto nei nomi.

SERVICE DISCOVERY

È un modo per trovare tutte le istanze di un servizio nella rete, non c'è necessità di utilizzare porte standard perché nelle risposte (che utilizzano mDNS) viene specificata la porta.
Il sistema operativo propone a un utente (o processo) un elenco di istanze che implementano un determinato servizio per esempio: stampanti, FS condivise o directory...
È il vero punto di forza dell'architettura zeroconf perché permette di "scoprire" servizi senza

conoscere gli standard come le porte, gli indirizzi IP o le identità dei server -> questo grazie alle estemsioni delle richieste dei DNS

Il protocollo zeroconf non gestisce la sicurezza, infatti, non vengono verificate autenticità e controllo degli accessi -> questi problemi sono risolti in modo alternativo utilizzando protocolli già noti.

ESEMPI DI APPLICAZIONE

- Printer configuration
- Music sharing
- Peer to peer chat
- Gaming
- Apple TV with AirPlay