CAPITOLO 1 – INTRODUZIONE

- **Broadcast e Multicast**
  Con il termine Multicast, nelle reti di calcolatori, si indica la distribuzione simultanea di informazione verso ***un gruppo*** *di destinatari;*
  in alternativa, un pacchetto destinato ***a tutti*** *i calcolatori di una rete è detto Broadcast.*

- **Cosa è il collo di transito o collo di bottiglia?**
  Il collo di bottiglia è un fenomeno che si verifica quando le prestazioni di una rete o le sue capacità sono fortemente vincolate da un singolo componente. Il componente viene spesso chiamato anch'esso punto del collo di bottiglia.
  Formalmente, un collo di bottiglia è il punto in cui la rete ha le minori performance tra un insieme di punti da percorrere. I colli di bottiglia per definizione devono, ovviamente, essere limitati.

- **Differenze fra una rete a commutazione di circuito e una rete a commutazione di pacchetto** *La commutazione a pacchetto si basa sulla suddivisione del messaggio in più attività autonome (con ID mittente, ID destinatario e N° ordine del pacchetto). Ogni pacchetto viaggia di vita propria (instradato indipendentemente e su percorsi differenti). L'utilizzo ottimale delle risorse viene effettuato con il principio di multiplazione statistica(quando il canale è libero, viene usato da qualche altro per inviare altri pacchetti).*
  E' efficiente(quindi ***più scalabile*** *per il trasporto di* ***pacchetti di piccole dimensioni****(email) La commutazione a circuito avviene tramite commutatori(dispositivi di commutazione) che non sono altro che nodi intermedi(es. DSE o DCE) i quali determinano una connessione fisica diretta tra due stazioni che necessitano di comunicare. Questa connessione è assegnata alla coppia di stazione ed è mantenuta fino al termine della comunicazione. Il difetto è proprio quello di avere bloccato questo canale (quindi anche le risorse) di comunicazione fino a che le due stazioni non hanno finito di comunicare.*
  È efficiente (quindi ***più scalabile****) per il trasporto di* ***grandi volumi*** *di dati.*
  - Qual è la migliore tra le due?
  DIPENDE!!!
  Per la trasmissione a blocchi, tradizionali, quella che caratterizzata la normale vita di Internet è sicuramente migliore la commutazione a pacchetto.
  Se devo, invece, trasmettere molti dati dalla stessa origine alla stessa destinazione, è più vantaggiosa la commutazione a circuito.

- **Cos'è la multiplazione statistica?**
  È un concetto che si usa nella commutazione a pacchetto. La multiplazione statistica permette un'ottimizzazione molto forte dell'utilizzo delle linee di trasmissione. Ogni pacchetto viaggia di vita propria. Se il canale è libero, lo userà qualche altro per trasmettere qualche altro pacchetto.

- **Si può utilizzare una LAN broadcast utilizzando mezzi trasmissivi punto-punto?** *Si ad esempio rete ad anello, rete ad anello cablata a stella, rete a stella o ad albero dotata di centri stella attivi, in grado di ripetere trame a tutti i calcolatori*

CAPITOLO 2 – LIVELLO FISICO

- **Come può essere la fibra ottica? (si basa sulla rifrazione, può essere monomodale e multimodale [è migliore la monomodale perché è diretta])**
  La fibra ottica sfrutta la proprietà della luce di non rifrangersi se l'angolo di incidenza è inferiore ad un certo limite (dipendente dal mezzo fisico). È fatta come il cavo coassiale ma non ha il secondo strato conduttivo e al centro il filo è costituito da una specie di vetro molto trasparente. Si può arrivare ai 100 Gbit/s. È unidirezionale, principalmente per la difficoltà di mettere da una stessa estremità ricevitore e trasmettitore. Le reti in fibre possono essere strutturate ad anello (con interfaccia attiva o passiva) o a stella passiva (con le fibre fuse in un cilindro di silicio), ma il

collegamento più usato è quello punto-punto unidirezionale. Ci sono due tipi di fibre ottiche: - multimodali: il raggio è di circa 50 micron e sono presenti più raggi luminosi contemporaneamente - monomodali: il core ha un raggio di circa 8 micron e la luce viaggia in linea retta, senza riflessioni; è più costosa ma migliore.

- **Differenze tra FDM, TDM, WDM**

Le 3 tecniche di multiplexing sono:
1) FDM: a divisione di frequenza per segnali analogici,
2) WDM: a divisione di lunghezza d'onda per segnali ottici,
3) TDM: a divisione di tempo per segnali digitali.
FDM: in fase di MUX ogni canale logico genera un segnale sulle stesse frequenze, questi segnali vengono modulati dal MUX in un unico segnale. Il DEMUX utilizza una serie di filtri per scomporre il segnale composto ricevuto nei segnali originali.
WDM: le operazioni di divisione dei segnali luminosi possono essere facilmente effettuate attraverso un prisma che devia i raggi in base alla frequenza e all'angolo di incidenza, vengono raggruppati e divisi in questo modo.
TDM: è progettata per condividere un canale digitale. Ogni canale logico occupa un intervallo di tempo. Il MUX divide il canale in intervalli temporali che assegna poi ad ogni canale logico.

- ***Illustrare le differenze tra il TDM sincrono e quello statistico. Quali sono i vantaggi e gli svantaggi di ciascuna tecnica?***

Nel TDM sincrono gli intervalli di tempo vengono allocati in modo fisso, nel TDM statistico vengono al-locati in base alla quantità di dati da spedire.
-Nel SINCRONO è n volte quella dei canali e i dati vengono inviati nell'ordine stabilito. Se un canale non ha nulla da inviare, il tempo e il canale vengono sprecati.
-Nello STATISTICO i turni vengono assegnati dinamicamente ai canali che devono spedire, evitando sprechi, ma la velocità è minore.

- **Quale tecnica di TDM è più adatta per la trasmissione dati su una rete di computer?** *La tecnica TDM più adatta per la trasmissione dei dati su una rete di computer è la STATISTICA poiché allocando dinamicamente i turni evita di sprecare banda nel caso in cui un computer non debba inviare nulla .*

- **Perché preferiamo la fibra ottica al rame?**

La Fibra Ottica è una tecnologia completamente diversa perché invece di trasmettere un segnale elettrico su cave di rame, trasmette un segnale luminoso opportunamente generato. I vantaggi di questa tecnologia sono molti, il primo dei quali è la velocità raggiungibile dal segnale, anche in proporzione alla distanza.
Il segnale luminoso viaggia a velocità estremamente elevate (quasi alla velocità della luce), rispetto al segnale elettrico che ha una velocità di trasmissione enormemente inferiore. Un altro vantaggio è che il segnale non rischia mai di subire interferenze o modifiche durante il tragitto, quindi anche l'affidabilità dei dati inviati è superiore. Un ultimo vantaggio di cui vi faccio cenno è la simmetria della connessione. Due segnali luminosi che si incrociano non creano interferenza l'uno con l'altro, di conseguenza è possibile sfruttare la connessione in fibra ottica in maniera simmetrica sfruttando al massimo sia il download che l'upload.

- **Capacità mezzo trasmissivo: Shannon e Nyquist**

I canali trasmissivi utilizzati per la comunicazione dei dispositivi si suddividono in: Canali ideali: non causano distorsioni o ritardi nella propagazione dei segnali. Canali non distorcenti: causano solo un ritardo costante nella propagazione ed un'attenuazione costante in banda.
Canali distorcenti: causano attenuazioni e ritardi, in funzione della frequenza dei segnali.
***Shannon** e **Nyquist** hanno rispettivamente enunciato teoremi che esprimono la massima velocità di trasmissione per ciascun tipo di canale. Il legame tra la velocità di trasmissione (bit rate) e la*

*larghezza di banda è dato dal **Teorema di Nyquist**.*
*Il massimo bit rate, ovvero la capacità di canale, relativo ai canali reali (con rumore termico) è dato dal **Teorema di Shannon** che considera anche il rumore*

· Multiplazione e demultiplazione

Il multiplexer crea un singolo segnale che verrà spedito sul canale fisico. Quando il segnale arriva a destinazione, un altro dispositivo, chiamato demultiplexer(DEMUX) riconverte il segnale ricevuto nei segnali originali per ognuno dei canali logici.
La tecnica di multiplazione, si divide in:
A divisione di tempo (TDM)
– modalità deterministica (banda dedicata e ritardo fisso)
– modalità statistica (banda e delay variabili e migliore sfruttamento del mezzo)
A divisione di spazio (SDM)
– Dati inviati su media fisicamente separati
A divisione di frequenza (FDM e WDM)
– Usa differenti frequenze o lunghezze d'onda per differenziare i dati trasmessi
Per codifica (CDM)
– La differenziazione dei dati trasportati è ottenuta utilizzando diversi tipi di codifica

· La descrizione di ampiezza, fase e frequenza

Abbiamo un'onda sinusoidale che è la più importante forma di segnale analogico periodico. Ogni ciclo consiste di un arco al di sopra dell'asse del tempo e di un arco al di sotto l'asse del tempo.
*Un'onda sinusoidale può essere rappresentata da tre parametri: **AMPIEZZA MASSIMA**, **FREQUENZA**, **FASE**.*
*L'**AMPIEZZA MASSIMA** di un segnale è il valore assoluto del segnale nella sua intensità massima (il picco massimo) ed è proporzionale all'energia trasportata dal segnale. Si rappresenta in volt.*
*La **FREQUENZA** è il numero di periodi in un 1s. Si indica con **f: 1/T**.*
*Dove T è il periodo (il tempo necessario affinché un segnale completi un ciclo) . La frequenza quindi è la velocità con cui un segnale cambia rispetto al tempo. Cambiamenti veloci quindi implicano una frequenza alta, cambiamenti lenti implicano una frequenza bassa. La **FASE** descrive la posizione dell'onda rispetto al tempo 0. Indica la posizione iniziale del primo ciclo. È misurata in gradi o radianti.*
In conclusione, un'onda sinusoidale semplice non è utile per le reti di comunicazione. Serve un segnale composto, cioè un segnale formato da varie onde sinusoidali.

· La modulazione (ampiezza, fase e frequenza)

***ASK**: MODULAZIONE IN AMPIEZZA*
La modulazione ASK viene normalmente implementata usando solo 2 tipi di elementi del segnale. Un elemento del segnale può assumere due forme: in una la sua ampiezza è nulla, nell'altra la sua ampiezza è uguale all'ampiezza massima del segnale portante. Questi due elementi rappresentano il valore del bit 0 o 1.
***FSK**: MODULAZIONE IN FREQUENZA*
La modulazione FSK utilizza due frequenze portanti. A queste frequenze corrispondono i valori del bit 0 e 1.
La prima frequenza portante viene utilizzata per il valore 0 e la seconda per il valore 1. Un requisito importante nella FSK è la continuità di fase negli istanti di transizione da una frequenza all'altra.
***PSK**: MODULAZIONE IN FASE*
La modulazione PSK è la più utilizzata rispetto alle ASK e FSK. Nella PSK è la fase a determinare il valore del bit. Al cambio di fase si associa il valore 1, viceversa si associa il valore 0.

Vi è poi:
***QPSK**: QUADRATURA PSK*
La quadratura PSK utilizza 4 fasi diverse per ogni elemento del segnale, per questo si possono rappresentare 2 bit per ogni elemento del segnale. In pratica lo schema utilizza due modulazioni BPSK (Binary PSK) seperate che poi vengono sommate in un unico segnale finale.

***QAM**: QUADRATURE AMPLITUDE MODULATION*
Questa tecnica di modulazione mette insieme la modulazione ASK con la modulazione PSK. Si ottiene quindi una modulazione più efficiente rappresentando i bit con la variazione in contemporanea dell'ampiezza e della fase. Questa modulazione determina quindi una grande velocità di trasmissione.

- **Cos'è la diafonia, come si misura e quali mezzi trasmissivi riguarda**
  La diafonia è un fenomeno di accoppiamento elettrico tra mezzi trasmissivi vicini non isolati adeguatamente. Il segnale trasmesso su un cavo genera per induttanza un segnale corrispondente nel cavo vicino, che si sovrappone al segnale trasmesso in quest'ultimo. Si può verificare anche nella trasmissione con mezzi non guidati, quando un segnale emesso da una antenna si disperde durante la propagazione nell'aria; la parte dispersa può giungere in prossimità di un'altra antenna.
- **Nei doppini, si usa una tecnica di trasmissione bilanciata o sbilanciata?** *Nei doppini si usa una tecnica di **trasmissione bilanciata**. La binatura all'interno dei doppini serve a ridurre i disturbi elettromagnetici. Normalmente si utilizzano cavi con più coppie ed è allora necessario adottare passi di binatura differenziati da coppia a coppia per ridurre la diafonia tra le coppie. Infatti, se i passi di binatura fossero uguali, ogni conduttore di una coppia si troverebbe sistematicamente affiancato, ad ogni circuito, con uno dei due conduttori dell'altra coppia, e quindi verrebbe a cadere l'ipotesi di perfetta simmetria della trasmissione bilanciata.*
- **Fisicamente, di che ha bisogno il pc (o cellulare) per la trasmissione dei dati ?**
  Ha bisogno di un ' antenna che serve per la ricezione e trasmissione.

CAPITOLO 3 – LIVELLO DATALINK

- **Rilevamento errori a livello datalink**
  Gli errori di trasmissione sono causati da fenomeni fisici di natura differente: rumore termico di fondo, rumore impulsivo, diafonia fra due fili conduttori fisicamente adiacenti, etc. Il controllo dell'errore si basa su codici di ridondanza, che aggiungono bit alla parola dati per verificarne la correttezza. Tali codici si suddividono in: codici rilevatori: in grado unicamente di rilevare la presenza o meno di errori nel frame, ma non la loro posizione; in questo caso il ricevente può chiedere la ritrasmissione del messaggio. codici correttori: in grado di rilevare una o più posizioni errate nel frame e quindi di correggerle per semplice inversione del bit. Vi sono 3 principali codici a rilevazione d'errore, diversi tra loro:
  *1) **Codici di parità** sono quelli in cui la distanza minima è 2 e sono quindi in grado di rilevare un errore singolo; più precisamente, sono in grado di rilevare la presenza di un numero dispari di errori. Il bit di parità aggiunto assume il valore 0 o 1 per rendere pari il numero di "1" nella sequenza da trasmettere (parità pari) o per renderlo dispari (parità dispari). Per calcolare il bit di parità è sufficiente effettuare l'exclusive OR dei bit di dato nella parola nel caso di parità pari e negare tale risultato nel caso di parità dispari. La parola trasmessa sarà formata dalla parola originale e dal bit di parità. Il ricevitore provvederà a ricalcolare la parità sulla configurazione ricevuta (escludendo il bit di parità aggiunto): confrontando il nuovo bit di parità con quello ricevuto è possibile stabilire se la trasmissione è avvenuta correttamente o no.*
  *2) **Check-sum.** Questa tecnica si basa sull'aggiunta di simboli calcolati non sui singoli codici delle parole che costituiscono la comunicazione, ma valutati su un blocco di parole (ridondanza di un blocco). L'obiettivo è quello di ottenere la più alta possibilità di rilevare errori con la minor ridondanza introdotta. La Check-sum è una delle tecniche di rilevazione errori maggiormente*

utilizzata per trasmissione a breve distanza. Dato un blocco di informazioni da codificare, la parola di controllo si calcola effettuando la somma in algebra modulo 2 (XOR) di tutti i codici delle singole parole. Il risultato è un byte che viene anch'esso trasmesso. Il ricevitore si preoccuperà di ripetere l'operazione sul pacchetto ricevuto confrontando il suo risultato con quello inviatogli dal trasmettitore: se le due somme coincidono significa che la trasmissione è avvenuta senza interferenze.

*3) **Codici di ridondanza ciclica**. È un altro metodo per la rilevazione degli errori è quello dei codici ciclici. Gli n bit del blocco da trasmettere vengono considerati come coefficienti di un polinomio di grado n-1 nella variabile x. Tale polinomio, che chiameremo M(x), viene poi diviso per un altro polinomio fissato dalle convenzioni internazionali, chiamato polinomio generatore e indicato con G(x), le cui caratteristiche sono: - è sempre di grado inferiore al polinomio M(x) da trasmettere; - ha sempre il coefficiente del termine x^0 uguale a 1. In trasmissione, insieme al blocco di bit che costituisce M(x), viene anche mandato il blocco di controllo R(x), ottenuto dividendo M(x) per G(x) con le regole di divisione modulo 2 (effettuando lo XOR delle due stringhe di bit). Le cifre di controllo calcolate vengono dette FCS (Frame Check Sequence) o CRC (Cyclic Redundancy Check). Per rilevare la presenza di un errore il ricevitore divide il messaggio ricevuto per G(x) e verifica che il resto sia nullo. Se non lo è il ricevitore deve chiedere la ripetizione del messaggio.*

- **Che cos'è il Piggy backing?**

Il Piggy backing è la pratica di mandare l'ACK di un frame ricevuto insieme al prossimo frame da inviare, e non in un frame a sé stante; si risparmia banda, ma è utile solo per i canali full-duplex e solo se il nuovo pacchetto da inviare non si fa attendere troppo (altrimenti il mittente, non ricevendo l'ACK, ripeterà l'invio del messaggio).

- **A livello datalink come si gestisce la contesa?**

Tecnicamente una volta che la stazione ha acquisito il canale, con CSMA/CD non ci possono essere collisioni, ma questo problema può ancora presentarsi durante il periodo di contesa. Le collisioni influenzano le prestazioni del sistema, specie quando il prodotto banda-ritardo è grande (cioè CAVO LUNGO e FRAME CORTI), quindi riducendo l'ampiezza di banda. Le collisioni, inoltre, rendono il tempo di trasmissione dei frame variabili. A tal proposito, esistono alcuni protocolli COLLISION FREE in grado di risolvere la contesa. I protocolli di questo tipo sono detti protocolli a PRENOTAZIONE in cui l'intenzione di trasmettere è comunicata a tutti prima ancora di inviare la trasmissione vera e propria. Uno di questi protocolli è il TOKEN RING.

Il Token ring non utilizza un mezzo broadcast ma un insieme di collegamento punto-punto. Tale protocollo permette ad ogni stazione di trasmettere un messaggio a turno in ordine predefinito. Tale breve messaggio prende il nome di Token(gettone). Le stazioni sono collegate l'una all'altra in un anello, passare il Token alla stazione successiva consiste nel riceverlo da una direzione e passarlo nell'altra. Anche i frame sono trasmessi nella direzione del Token, in tal modo circoleranno nell'anello fino a raggiungere la destinazione. Per impedire che un frame circoli all'infinito, come il Token, alcune stazioni devono rimuoverlo dall'anello; questa stazione può essere o la stazione che ha spedito il frame o la stazione che era la destinazione del frame. Il Token rappresenta quindi il permesso di inviare dati, se una stazione ha un frame in coda per la trasmissione, quando riceve il Token essa può spedire quel frame prima di passare il Token alla stazione successiva. Se non ha frame in coda, passerà il Token.

- **Cosa è e come funziona il bit stuffing?**

Esistono diversi metodi di Framing, uno di questi è il Bit Stuffing, il livello data link di chi trasmette ogni volta che incontra cinque bit a 1 consecutivi nei dati, automaticamente inserisce uno 0 nel flusso di bit in uscita. Quando la destinazione riceve cinque bit consecutivi con valore 1 seguiti da uno 0, automaticamente elimina lo 0.

- **Protocolli a finestra scorrevole (GO BACK-N e SELECTIVE REJECT) -**

GO BACK-N:

Per migliorare l'efficienza della trasmissione, e quindi sfruttare al meglio l'intero canale, occorre spedire più frame prima di fermarsi ed aspettare un riscontro.

Questo protocollo spedisce più di un frame prima di ricevere un riscontro cumulativo. Mantiene una copia del frame spediti fino all'arrivo di un riscontro.

I frame vengono numerati per essere identificati dal destinatario.

Il funzionamento di questo protocollo si basa su concetto di finestra scorrevole. Questo protocollo necessità di maggiori risorse di buffer:
In trasmissione devono essere memorizzati i frame inviati in attesa di riscontro, per poterli ritrasmettere in caso di necessità.
Ad ogni riscontro ricevuto vengono liverati i buffer relativi ai frame riscontrati per occuparli con nuovi frame trasmessi.
Ad ogni riscontro inviato, i frame riscontrati vengono passati allo strato di rete ed i relativi buffer vengono liberati per poter accogliere nuovi frame in arrivo.

- ***SELECTIVE REJECT*:**

Prevede che in recezione possano essere accettati anche frame fuori sequenza. Si riduce il numero di frame ritrasmessi. I frame fuori ordine vengono mantenuti nei buffer fino a che non sono stati ricevuti tutti i frame intermedi. Quando si ha un frame perduto, B riceverà il frame successivo fuori sequenza al quale risponderà con un ACK relativo al frame perduto.
A quindi ritrasmetterà solo il frame perduto e proseguirà con la normale sequenza. B memorizza tutti i frame successivi ed alla ricezione del frame perduto ritrasmesso risponderà con un ACK relativo all'ultimo frame ricevuto correttamente. In caso di perdita dell'ACK, sarà il time-out di A a generare un frame di sollecito di ACK per B, che risponderà di conseguenza.

Descrivere il funzionamento di un codice CRC.

Un codice CRC è un codice ciclico che per una parola di "k" bit ne crea un'altra di "n" bit. Vengono aggiunti "n-k" bit a 0 nella parte destra e la parola viene divisa da un generatore che usa un divisore di ordine "n-k+1". Il quoziente viene eliminato, il resto viene aggiunto alla parola al posto degli 0 inseriti in precedenza. Il ricevitore invia gli "n" bit al generatore uguale a quello del mittente che dà in output gli "n-k" bit che saranno la sindrome. Se la sindrome è 0000… allora non ci sono stati errori.

• **Dopo quante trasmissioni si arresta la trasmissione di un frame?** *16 ritrasmissioni.*

PROTOCOLLI DATA LINK LAYER PER RETI LAN

• **CSMA/CD**

Il protocollo opera in tre diverse fasi:
Carrier sense: ogni stazione che deve trasmettere controlla la disponibilità del mezzo e trasmette solo quando è libero.
Multiple-access: Due stazioni trovando il mezzo trasmissivo libero, decidono contemporaneamente di trasmettere; il tempo di propagazione dei segnali sul cavo non è nullo e quindi una stazione può credere che il mezzo sia ancora libero anche quando un'altra ha già iniziato la trasmissione.
Collision detection: se si verifica la sovrapposizione di due trasmissioni si ha una collisione, per rilevare questa collisione ogni stazione mentre trasmette ascolta i segnali sul mezzo trasmissivo confrontandoli con quelli da lei generati.
Le stazioni quando rilevano una collisione fermano le trasmissioni.
A seguito di una collisione:

1. *La stazione trasmittente sospende la trasmissione e trasmette una sequenza di jamming (interferenza trasmissiva). Questa sequenza permette a tutte le stazioni di rilevare l'avvenuta collisione.*
2. *Le stazioni in ascolto riconoscendo il frammento di collisione, formato dal pacchetto + il jamming scartano i bit ricevuti.*
3. *La stazione trasmittente ripete il tentativo di trasmissione, dopo un tempo casuale, per un numero di volte non superiore a 16.*

• **Protocolli a mappa di bit elementare(ACCESSO CONTROLLATO, prenotazione)**

Un esempio di protocollo a prenotazione è il protocollo a mappa di bit elementare: – sulla rete ci sono N stazioni, numerate da 0 a N-1
– alla fine della trasmissione di un frame inizia un periodo di contesa, in cui ogni stazione, andando per ordine di indirizzo, trasmette un bit che vale 1 se la stazione deve trasmettere, 0 altrimenti – al termine del periodo di contesa (privo di collisioni in quanto ogni stazione aspetta il suo turno) tutti

hanno appreso quali stazioni devono trasmettere, e le trasmissioni procedono un frame alla volta sempre andando per ordine
– se una stazione riceve dati da trasmettere quando la fase di prenotazione è terminata, deve attendere il successivo periodo di contesa per prenotare la propria trasmissione. L'efficienza di questo protocollo è bassa per grandi valori di N e basso carico trasmissivo; in queste condizioni una stazione deve attendere tutti gli N bit delle altre stazioni (delle quali la maggior parte o la totalità non desidera trasmettere) prima di poter trasmettere.

- **Token ring**

Il Token ring non utilizza un mezzo broadcast ma un insieme di collegamento punto-punto. Tale protocollo permette ad ogni stazione di trasmettere un messaggio a turno in ordine predefinito. Tale breve messaggio prende il nome di Token(gettone). Le stazioni sono collegate l'una all'altra in un anello, passare il Token alla stazione successiva consiste nel riceverlo da una direzione e passarlo nell'altra. Anche i frame sono trasmessi nella direzione del Token, in tal modo circoleranno nell'anello fino a raggiungere la destinazione. Per impedire che un frame circoli all'infinito, come il Token, alcune stazioni devono rimuoverlo dall'anello; questa stazione può essere o la stazione che ha spedito il frame o la stazione che era la destinazione del frame. Il Token rappresenta quindi il permesso di inviare dati, se una stazione ha un frame in coda per la trasmissione, quando riceve il Token essa può spedire quel frame prima di passare il Token alla stazione successiva. Se non ha frame in coda, passerà il Token.

- **Identificare MAC**

Il sottolivello MAC è specifico di ogni LAN e risolve il problema della condivisione del mezzo trasmissivo.
• Esistono vari tipi di MAC, basati su principi diversi, quali la contesa, il Token, la prenotazione e il round-robin.
• Il MAC è indispensabile in quanto a livello 2 (Data Link) le LAN implementano sempre una sottorete trasmissiva di tipo broadcast in cui ogni sistema riceve tutti i frame inviati dagli altri. Trasmettere in broadcast, cioè far condividere un unico canale trasmissivo a tutti i sistemi, implica la soluzione di due problemi:
• in trasmissione, verificare che il canale sia libero prima di trasmettere e risolvere eventuali conflitti di più sistemi che vogliano utilizzare contemporaneamente il canale;
• in ricezione, determinare a quali sistemi è effettivamente destinato il messaggio e quale sistema lo ha generato.
La soluzione del primo problema è data dai vari algoritmi di MAC
La soluzione del secondo problema implica la presenza di indirizzi a livello MAC (quindi nella MAC-PDU) che trasformino trasmissioni broadcast in:
– trasmissioni punto-a-punto, se l'indirizzo di destinazione indica un singolo sistema; – trasmissioni punto-gruppo, se l'indirizzo di destinazione indica un gruppo di sistemi; – trasmissioni effettivamente broadcast, se l'indirizzo di destinazione indica tutti i sistemi.

- **L'indirizzo MAC ha validità universale?**

No, è possibile trovare 2 MAC address uguali su due differenti segmenti di rete.

- **Illustrare le funzionalità fornite dai sotto strati MAC e LLC dello standard IEEE 802.**

LLC: si occupa di framing, del controllo del flusso e del controllo degli errori,
MAC: specifica un metodo di accesso multiplo da utilizzare per ogni tipo di rete LAN, è responsabile della creazione dei frame ed, inoltre, interagisce con lo strato fisico, quindi esiste uno specifico sotto strato MAC per ogni rete.

DATA LINK LAYER PER RETI LAN

- **Come fa lo switch a sapere su quale porta deve trasmettere?**

Per decidere su quale porta inoltrare un frame ricevuto, lo switch deve possedere una funzione di

*instradamento. La funzione di instradamento viene chiamata **BACKWARD LEARNING**. Questa tecnica è basato sull'apprendimento progressivo degli indirizzi mittenti, contenuti nei frame ricevuti, che lo switch associa univocamente alle porte di provenienza.*

BACKWARD LEARNING

- Al boot le tabelle sono vuote.

- Se un pacchetto ha una destinazione sconosciuta allora viene inoltrato su tutte le porte tranne che su quella di provenienza.

- Quando il destinatario riceverà il frame risponderà al mittente e quindi lo switch memorizzerà l'indirizzo che a lui era prima sconosciuto.

· Switch livello(layer) 2 e livello 3 (differenze)

SWITCH di LIVELLO 2: è un bridge.

SWITCH di LIVELLO 3: è un router o un gateway.

*ULTIMA GENERAZIONE(multilivello): è uno switch che ha la capacità di inoltrare frame a velocità maggiori, hanno anche una memoria interna per poter memorizzare i frame. Come è facile immaginare, quando i pacchetti inviati sono tanti questo processo è oneroso sia in termini di banda utilizzata sia in termini di latenza. **È qui che entrano in gioco gli switch di livello 3, o meglio di livello 2 e 3, chiamati anche switch multilivello. Questi sono difatti in grado di operare scelte di routing, supportando svariati tipi di protocolli (RIP, OSPF, BGP, …)**. In una rete con switch di questo tipo infatti i pacchetti non vengono inviati al router per decidere l'instradamento, ma è lo switch stesso ad avere la logica decisionale e a sapere dove inviare i messaggi. Nel mondo Enterprise ormai ogni switch supporta praticamente anche il livello 3.*

· DIFFERENZA TRA RIPETITORE (livello fisico), SWITCH (livello datalink) E ROUTER (livello rete)

*Un **ripetitore** viene utilizzato per amplificare un segnale, quando necessario. La trasmissione digitale tiene conto del contenuto dei dati se si deve intervenire per amplificare il segnale. Il segnale non viene semplicemente amplificato, ma viene interpretato, si estrae il contenuto informativo e si rigenera il segnale tramite apparati detti ripetitori.*

*Uno **switch** permette di connettere più LAN mantenendo la suddivisione a livello data link del modello IOS/OSI. Lo switch agisce sull'indirizzamento e sull'instradamento all'interno delle reti LAN mediante un indirizzo fisico (MAC), selezionando i frame ricevuti e dirigendoli verso il dispositivo corretto.*

*Un **router** è una stazione intermedia che opera a livello 3, che riceve i pacchetti e li inoltra attraverso la (sotto)rete.*

· Broadcast Storm

Nello switching i collegamenti ridondanti che sono usati per assicurare una connettività con gli altri switch possono causare il BROADCAST STORM.

Abbiamo, ad esempio, un host X che invia un frame ad uno switch A il quale lo invia in broadcast allo switch B che a sua volta lo invia sempre in broadcast. Ma cosa succede? Il frame ritorna a X e, quindi, si crea un LOOP INFINITO. Per risolvere questo problema, si usa lo SPANNING THREE.

· Con lo switch, come si gestiscono i loop nella broadcast storm, c'è un protocollo che usiamo?

Spanning tree protocol.

· Cosa è lo spanning tree? Come funziona?

Lo spanning-tree è basato sull'algoritmo di Prim o Kruskal, tende a costruire quest'albero di copertura. Lavora a layer 2 per mantenere una rete priva di loop fisici, rende una tipologia ridondante "loop free" mettendo in stato di blocco alcune porte.

Creare Spanning tree significa tagliare i collegamenti ridondanti, spegnere certe porte momentaneamente a livello logico. Mi conviene spegnere quei collegamenti meno efficienti. I collegamenti meno efficienti sono quelli con banda elevata e quindi meno costosi, mentre se il collegamento ha una banda limitata più è costa.

La radice dell'albero sarà un root bridge (switch che avrà il più basso Bridge ID, che è un identificativo per l'elezione, ovvero il MAC ADDRESS più basso). Per ogni altro switch della nostra rete avremo diverse porte: ROOT PORT o DESIGNED PORT. Una Root port che mi conduce alla radice dell'albero per NON-ROOT-BRIDGE e invece una DESIGNED PORT per segmento. Questo mi serve a capire le porte che devono essere messe in blocco che diventano porte DESIGNATE. Lo spanning-tree è "Plug-and-play" ovvero senza configurazione, cioè fa tutto da solo.

- **Che cosa è un VCI?**

Il VCI è un numero usato in ogni coppia di switch e serve per identificare i pacchetti appartenenti a una connessione tra due switch.

- **Differenza Matrix e crossbar**

Sono tecnologie di switching.
MATRIX utilizza una matrice a commutazione. In base all'indirizzo e al contenuto della tabella viene attivata la connessione necessaria
CROSSBAR può, invece, gestire più frame contemporaneamente (può quindi attivare più linee)

- **VIRTUAL LAN (VLAN)**

Una VLAN è una rete virtuale configurata via software e non attraverso collegamenti fisici.
L'idea che sta alla base delle reti virtuali è quella di dividere la rete in segmenti logici, anziché fisici. In questo modo una rete LAN viene divisa in varie reti logiche chiamate appunto VLAN.
Con questa configurazione è facile spostare un nodo da una rete virtuale a un'altra rete virtuale poiché non abbiamo bisogno di collegamenti fisici. Una rete VLAN crea un dominio broadcast che è indipendente rispetto alla struttura fisica delle reti sottostanti.
Quindi i nodi di una rete virtuale, sebbene appartenenti a più reti fisiche, possono funzionare come se facessero parte di una singola rete fisica.
L'appartenenza di un nodo a una rete virtuale possiamo gestirla attraverso l'indirizzi di porta, indirizzi fisici, indirizzi logici(IP) e indirizzi Multicast.
Vantaggi VLAN sono la riduzione dei costi e tempi di gestione e maggiore sicurezza. ***Come si può gestire l'appartenenza di un nodo ad una rete virtuale?***
Tramite il numero di porta e l'indirizzo fisico

- **Backword learning**

Per decidere su quale porta inoltrare un frame ricevuto, lo switch deve possedere una funzione di instradamento. La funzione di instradamento viene chiamata BACKWARD LEARNING. Questa tecnica è basato sull'apprendimento progressivo degli indirizzi mittenti, contenuti nei frame ricevuto, che lo switch associa univocamente alla rispettiva porta di provenienza.
FUNZIONAMENTO:
- *Al boot le tabelle dello switch sono vuote.*
- *Se un pacchetto ha una destinazione sconosciuta allora viene inoltrato su tutte le porte tranne che su quella di provenienza.*
- *Quando il destinatario riceverà il frame risponderà al mittente e quindi lo switch memorizzerà l'indirizzo che a lui prima era sconosciuto.*

- **Come collego 2 circuiti VLAN e uno switch?**

Tramite un trunk.

- **(VLAN) A cosa serve il trunk?**

È La propagazione delle informazioni nelle VLAN. Per far comunicare due switch nelle VLAN si usa un mezzo fisico che è proprio il trunk. A questo punto è come se i due switch diventassero un solo switch con le porte a coppia. Sul trunk viaggiano i frame che vengono identificati tramite VLAN ID (TRUNK VLAN) per vedere da quale VLAN arrivano.

- **Come fa lo switch a imparare le informazioni?**

Per sapere su quale porta debba essere trasmesso il frame, lo switch deve creare e mantenere aggiornata una tabella relativa alla associazione tra indirizzo di destinazione e porta. Inizialmente questa tabella è vuota, e lo switch deve inoltrare ciascun frame ricevuto su tutte le porte connesse. Poiché' i frame contengono l'indirizzo del mittente, ad ogni frame che arriva lo switch impara che la stazione che ha inviato il frame è raggiungibile attraverso la porta da cui è arrivato il frame stesso. Con il passare del tempo lo switch riempie la tabella e può svolgere la sua funzione in modo sempre più efficiente.

PROTOCOLLI DATA LINK LAYER PER WIRELESS LAN

- **Descrivere le principali applicazioni delle reti locali wireless**

  Le principali applicazioni delle reti locali wireless, riguardano la diffusione di computer portatili, per offrire mobilità senza perdita di connessione.
  Un altro fattore è l'estensibilità della rete senza necessità di cablaggio.

  Le Modalità operative delle WLAN sono:
  Modalità ad hoc (o infrastructureless)
  I computer possono comunicare direttamente l'uno con l'altro solo grazie alla propria interfaccia di rete wireless
  Modalità AP (o infrastructured)
  La comunicazione in rete avviene grazie ad Access Point (AP) hardware o software che sono parte integrante della rete WLAN, e per mezzo delle interfacce di rete wireless installate e configurate su ciascuna postazione in modo da comunicare con specifici AP per collegarsi a specifiche WLAN.

LIVELLO DI RETE

- **Cosa è la metrica?**

  La metrica definisce l'algoritmo di instradamento. Interviene nella caratterizzazione di un percorso per l'instradamento di pacchetti tra due nodi. Serve per selezionare il percorso migliore tra quello: più corto, meno congestionato, più ampio, meno costoso...
- **Come si costruisce la tavola di routing?**

  Con Dijkstra, ma su reti di grandi dimensioni non funziona e si ricorre al routing gerarchico.

- **Differenze tra LINK STATE e DISTANCE VECTOR**

  La differenza tra il protocollo LINK STATE e quello DISTANCE VECTOR è che i LINK STATE mandano le informazioni riguardando i collegamenti a tutti i router del proprio sistema autonomo, mentre DISTANCE VECTOR solo ai nodi adiacenti.

- **Che differenza c'è, al livello 3, tra l'attività di routing(instradamento) e forwarding(hardware)?**

  Sono due attività tra loro differenti. Con il termine di routing si indica l'operazione che coinvolge tutti i nodi o router della rete che, interagiscono tra di loro, secondo opportune modalità (ALGORITMI DI ROUTING), al fine di determinare i percorsi migliori per ogni coppia sorgente destinazione. Il routing è essenzialmente l'operazione di creazione e aggiornamento delle tabelle di routing, in cui ogni record, per ogni destinazione finale, indica la linea di uscita attraverso cui instradare i pacchetti.
  L'operazione di forwarding è invece l'operazione di ricerca della linea di uscita sulla base di dati già noti, contenuti all'interno delle tabelle e così via.
- **Cosa è la distanza amministrativa?**

  La distanza amministrativa quantifica l'attendibilità dell'informazione di instradamento. Più il valore è basso, più l'informazione è sicura.

- **Cosa è la tavola di routing e come funziona?**

  La tavola di routing o Routing table è una tabella che raccoglie tutte le informazioni necessarie per individuare il percorso ottimale verso tutte le possibili reti.

È costituita da:

1. *INDIRIZZO IP DI DESTINAZIONE: quando un router riceve un pacchetto dati attraverso la sua porta di ingresso, controlla nella propria tabella di routing se esiste già una entry per tale destinazione ed in caso affermativo inoltra il flusso di dati nella corrispondente porta di uscita.*
2. *METRICA: definisce l'algoritmo di instradamento;*
3. *INDIRIZZO DEL ROUTER DI NEXT HOP: è l'indirizzo successivo per raggiungere la rete di destinazione;*
4. *INTERFACE: interfaccia del router attraverso cui deve essere instradato il pacchetto verso il next hop;*
5. *TIMER: scandisce temporalmente ogni quanto tempo inviare gli updates ai router vicini.*

- **Chi è che immette i dati nella tavola di routing?**

Ci sono due casi:

STATICO, li immette l'amministratore di rete;
DINAMICO, attraverso i protocolli di routing.

- **Distance vector (problemi di hop count infinito, split horizon, hold down timer)**

DISTANCE VECTOR

L'idea è quella di partire dal nodo sorgente e cominciare a guardare i nodi adiacenti assegnando loro il valore del costo per raggiungerli (determinato dal costo dell'arco + il valore del nodo da cui si è partiti. Si itera il ragionamento per ciascuno dei nodi raggiunti.
Se il grafo ha |V| nodi dopo |V|-1 iterazioni tutti i nodi avranno assegnato il costo minimo per essere raggiunti dal nodo sorgente.
Nella sua struttura base è molto simile a quello di Dijkstra, ma invece di selezionare il nodo di peso minimo, tra quelli non ancora processati, con tecnica greedy, semplicemente processa tutti gli archi e lo fa |V|-1 volte
Per risolvere il problema dell'HOP COUNT INFINITO in cui un router aggiorna erroneamente la sua routing table riflettendo il nuovo hop count, viene utilizzato lo Split Horizon, in cui non si inviano le informazioni di costo verso la destinazione X sul link al quale vengono inviati i pacchetti per la destinazione X.
L'HOLD DOWN TIMER viene utilizzato per evitare fluttuazioni alla ricezione di un annuncio. Il router setta un timer di hold-down e accetta la modifica solo alla spirazione dello stesso..

- **Differenze tra IPV4 e IPV6 (IPv6 nato per fronteggiare il problema dell'esaurimento degli indirizzi IP)**

IPV6 non è altro che l'evoluzione di IPV4, nata per ovviare al problema rappresentato dall'esiguo numero di classi di indirizzi. Agli inizi degli anni '90, furono effettuate delle previsioni secondo cui, tra il 2008 e il 2018, l'intero spazio di indirizzi si sarebbe esaurito.
La principale differenza risiede nella lunghezza dell'indirizzo:
IPV4 è costituito da 32 bit, 4 byte, ciascuno rappresentato da un numero decimale che può assumere un valore tra 0 e 255, separati da un ".";
IPV6 prevede invece, l'utilizzo di indirizzi a 128 bit, 16 byte, suddivisi in 8 gruppi di 4 cifre alfanumeriche, separate dai ":".
Avendo a disposizione un numero maggiore di bit per rappresentare un indirizzo, di conseguenza, è aumentato di gran lunga, anche il numero di indirizzi e classi per la nuova utenza. Anche la struttura del pacchetto è differente. IPV6 infatti, si avvale di un header di 40 byte e non permette la frammentazione dei pacchetti, perché fa perdere tempo. I nodi IPV6 tentano di identificare la dimensione corretta dei pacchetti da scambiarsi in modo dinamico. Se il router non può inoltrare il pacchetto, invia un messaggio ICMP indietro per notificare il fatto e scarta il pacchetto. In questo modo, risulta molto più efficiente fare in modo che l'host di partenza invii i pacchetti di dimensione corretta che non frammentare nei router.

- **Cosa è il grafo di rete?**

È una rappresentazione della rete, dove ogni nodo del grafo rappresenta un router ed ogni arco

rappresenta una linea di comunicazione, un canale. Per scegliere un percorso tra due router, l'algoritmo cerca nel grafo, il cammino più breve tra essi.

- **Come si costruisce la tavola di routing a partire dal grafo di rete?**

*Una tabella di instradamento (**Routing Table**) raccoglie le informazioni necessarie per individuare il percorso ottimale verso tutte le possibili reti.*

TABELLA DI ROUTING

- INDIRIZZO IP DI DESTINAZIONE:È il campo più importante contenuto nella Routing Table, quando un router riceve un pacchetto dati attraverso la sua porta di IN, controlla nella propria tabella di routing se esiste una entry per tale destinazione, ed in caso affermativo inoltra il flusso dati nella corrispondente porta di OUT.

- METRICA: Definisce l'algoritmo di instradamento (Hop Count, Load, Delay, Bandwith, ecc.) - INDIRIZZO DEL ROUTER DI NEXT HOP: È l'indirizzo del router successivo per raggiungere la rete di destinazione

- INTERFACE: Interfaccia del router attraverso cui deve essere instradato il pacchetto verso il next hop

- TIMER: Scandisce temporalmente ogni quanto tempo inviare gli updates ad i router vicini

Quali sono le informazioni della propria tavola di routing che un nodo dovrebbe spedire ai propri vicini?

La soluzione più semplice è che ogni nodo spedisca l'intera tavola di routing ai propri vicini, lasciando ad essi la scelta di quali informazioni utilizzare. Quando un nodo R riceve le informazioni della tavola di routing da un vicino V, deve aggiornare la propria tavola di routing.

- **Esempi di protocolli di rete**

Al livello di rete esistono:

*-**PROTOCOLLI DI INSTRADAMENTO (RIP e OSPF (per IGP), BGP per(EGP))** che prevedono la soluzione di percorso.*

***(IGP)** Il protocollo originario era il **RIP** (Routing Information Protocol) di tipo distance vector, ormai sostituito da **OSPF** (Open Shortest Path First), che è di tipo link state.*

OSPF consente fra l'altro un routing gerarchico all'interno dell'AS

***(EGP)** IL protocollo **BGP** (Border Gateway Protocol) è un protocollo di routing dinamico usato per connettere tra loro più router che appartengono a "sistemi autonomi" (AS) diversi ed è di tipo distance vector.*

*-**PROTOCOLLO IP** che è un protocollo datagram, quindi non connesso e non affidabile, che opera come segue:*

- riceve i dati dal livello trasporto e li incapsula in pacchetti di dimensione massima pari a 64Kbyte (normalmente circa 1.500 byte);

- instrada i pacchetti sulla subnet, eventualmente frammentandoli lungo il viaggio; •

a destinazione:

- riassembla (se necessario) i frammenti in pacchetti;

- estrae da questi i dati del livello trasporto;

-consegna al livello trasporto i dati nell'ordine in cui sono arrivati (che non è necessariamente quello in cui sono partiti).

*-**PROTOCOLLI DI CONTROLLO (ICMP, ARP e RARP)** che gestiscono la notifica degli errori e le segnalazioni del router.*

***ICMP**: L'operatività della subnet è controllata continuamente dai router, che si scambiano informazioni mediante messaggi conformi al protocollo ICMP (tali messaggi viaggiano dentro pacchetti IP).*

***ARP**: Il protocollo ARP serve per derivare, dall'indirizzo IP dell'host di destinazione, l'indirizzo di livello data link necessario per inviare il frame che incapsulerà il pacchetto destinato all'host di cui all'indirizzo IP.*

***RARP**: Il protocollo RARP risolve il problema inverso, cioè consente di trovare quale indirizzo IP*

corrisponda a un determinato indirizzo data link.

- **Che protocollo usiamo, a livello 3, per la propagazione di informazioni?** *Utilizziamo i protocolli di routing che sono di tipo **link state**, cioè **OSPF** e IS-IS. Questi protocolli sono utilizzati per propagare velocemente e in modo affidabile le informazioni di routing relative a un determinato AS (sistema autonomo). Questi protocolli costruiscono un database link state che vengono sincronizzati con i pacchetti LSA. A questo punto il link state applica l'algoritmo di Dijkstra per stabilire i percorsi migliori che consentono di raggiungere ciascuna rete destinazione, percorsi da installare nella tabella di routing.*

- **Problemi che causano il distance vector? (RISP: *Routing loops e hop count infinito*) Ci sono altre tecniche per ovviare a questi problemi? (RISPOSTA: *SPLIT HORIZON e POISON REVERSE*)**

  I problemi che causano i distance vector sono il Routing loops e conteggio all'infinito(hop count infinito). A tal proposito, deve essere definito un limite sul numero di hops per evitare loops. Una possibile soluzione è fornita dallo SPLIT HORIZON che impedisce di inviare a ritroso un annuncio relativo ad una root sull'interfaccia da cui si è appreso della stessa route. Ciò significa che non vengono inviate le informazioni di costo, verso la destinazione X sul link al quale vengono inviati i pacchetti per la destinazione X.

  Si necessita, però, di un meccanismo per comunicare quando una rete è andata fuori servizio e in tal caso, si usa il POISON REVERSE. Quando una rete si rompe, piuttosto che non inserirla più nel vettore delle distanze, la si inserisce lo stesso, ma con distanza settata ad infinito, comunicando così ai vicini che la rete non c'è più. Ricevuto il poisoning, la rete non viene messa giù, ma probabilmente lo è, pertanto viene messa in una condizione di possibly down e viene inviato il poison reverse, per riscontrare l'avvenuta ricezione del messaggio.

- **IGP e EGP**

  *I router che instradano messaggi all'interno dello stesso AS (Autonomus system) e non hanno diretta connessione con altre reti (network) esterne, sono chiamati Interior Router e scambiano informazioni di instradamento tramite un **IGP** (Interior Gateway Protocol). Protocolli di tale tipo sono ad esempio il RIP, OSPF, IS-IS.*

  I router, che instradano i messaggi tra AS diversi sono detti Exterior Router, scambiano informazioni di instradamento utilizzando un protocollo EGP (Exterior Gateway Protocol). Il più comune protocollo di tale tipo è il BGP.

- **Cos'è il BGP?**

  *IL protocollo BGP (Border Gateway Protocol) è un protocollo di routing dinamico usato per connettere tra loro più router che appartengono a "sistemi autonomi" (AS) diversi. È quindi un **protocollo di routing inter-AS**, classificato come protocollo di "Exterior Gateway" **(EGP)**, ovvero utilizzato per inviare le proprie route a organizzazioni esterne (e per ricevere le route di organizzazioni esterne). Differisce in questo dai protocolli di "Interior Gateway" (IGP), utilizzati per lo scambio di rotte all'interno della stessa organizzazione.*

  *È fondamentalmente di tipo **distance vector**, con due novità:*

  • possiede la capacità di gestire politiche di instradamento (derivanti, ad esempio, da leggi nazionali) che vengono configurate manualmente nei router;

  *• mantiene (e scambia con gli altri router) non solo il costo per raggiungere le altre destinazioni, ma anche il cammino completo. Ciò consente di **risolvere il problema del count to infinity**, perché se una linea va giù il router può subito scartare, senza quindi poi distribuirli, tutti i cammini che ci passano.*

- **Flooding**

  Algoritmo di tipo non adattivo. Si tratta di una tecnica di instradamento generalmente utilizzata nelle reti ad hoc, cioè nelle reti non infrastrutturate. Ogni pacchetto in arrivo viene inoltrato su ogni linea in uscita eccetto quella da cui è arrivato. Per prevenire la duplicazione eccessiva dei pacchetti, gli stessi vengono dotati di un contatore. Quando questo contatore raggiunge lo 0, il

pacchetto viene eliminato. I router tengono traccia dei messaggi ricevuti e ritrasmessi, e non duplicano messaggi già replicati.

*Gli aspetti **negativi** di questo algoritmo sono essenzialmente legati alla inefficienza: – ogni pacchetto va a finire su tutte le linee della rete, provocando un utilizzo inefficiente della rete stessa;*

*– ogni pacchetto va a finire su tutti i router, aumentando il carico di lavoro dei router stessi. Aspetti **positivi** sono:*

– qualsiasi pacchetto arriverà nel tempo più breve possibile (segue tutte le strade, anche la più veloce);

– estremamente resistente a modifiche della topologia;

– anche il malfunzionamento di grandi porzioni della rete permette il recapito del pacchetto se almeno un cammino rimane operativo;

– non richiede una conoscenza a priori della topologia della rete.

- **Protocolli di Routing Gerarchico**

Non potendo gli algoritmi LSP gestire qualsiasi rete di qualsiasi dimensione, occorre organizzare il routing in modo gerarchico, cioè suddividere la rete in aree. A causa della crescita esponenziale di Internet, le tabelle di routing diventano sempre più grandi. Quindi si divide il gruppo di router in regioni. Ogni router conosce i dettagli della propria regione e come comunicare con le altre, ma non conosce la loro struttura interna. Può occasionalmente generare cammini non ottimali, ma il vantaggio in termini di riduzione delle tabelle di routing vale la spesa.

- **Rete gerarchica(OSPF) (per reti di grandi dimensioni)**

OSPF è oggi il più diffuso protocollo IGP utilizzato in Internet.

L'OSPF considera la rete come un grafo con i router come punti, e le linee come archi Ogni linea fisica è costituita da due archi, uno per ogni verso

L'OSPF assegna un costo ad ogni arco, e determina il cammino più breve in base al costo complessivo del tragitto.

***FUNZIONAMENTO OSPF**:*

I nodi di rete invece non hanno peso in OSPF, e la loro connessione al router viene valutata costo 0. Ciascun router invia a tutti gli altri router dell'area lo stato dei suoi collegamenti Ogni router ha una visione della rete memorizzata in un suo database topologico Attraverso l'algoritmo di Dijkstra ogni nodo calcola individualmente il percorso di minor costo da sé verso ogni altro nodo dell'area.

Eventuali modifiche vanno segnalate a tutti i nodi nell'area (broadcast/flooding).

RETE GERARCHICA AL CUI INTERNO ABBIAMO:

Boundary Router: Scambiano informazioni di instradamento con router di altri AS. Backbone Router: Eseguono l'instradamento entro la Backbone ma non sono router di bordo area. Internal routers: Sono all'esterno della Backbone ed eseguono solo l'instradamento intra AS. Area border routers: Appartengono sia ad un'area che alla Backbone, almeno uno per ogni area. Una di queste aree è definita "area di Backbone" che funge da transito verso le altre aree. Le aree saranno in comunicazione fra loro mediante router di "frontiera" che supporteranno il protocollo OSPF. Grazie a questa suddivisione gerarchica è possibile sia ridurre il traffico di routing scambiato fra i nodi della rete OSPF, sia ridurre le dimensioni delle tabelle d'instradamento dei router.

- **RIP**

Il primo protocollo di routing interno utilizzato in Internet è il RIP (Routing Information Protocol), ereditato da ARPANET. RIP è un protocollo basato sull'algoritmo distance vector. Adatto a reti di dimensioni limitate, ha iniziato a mostrare i suoi limiti già alla fine degli anni '70. Attualmente ancora utilizzato come protocollo di routing in qualche piccola rete privata. Caratteristiche del modello distance vector utilizzate da RIP sono:

– Usa numero degli hop come metrica per il costo dei link: tutte le linee hanno costo 1;

– Il costo massimo è fissato a 15, quindi impone il suo uso su reti di estensione limitata (diametro inferiore a 15 hop);
Le tabelle di routing vengono scambiate tra router adiacenti ogni 30s via un messaggio di replica del RIP (RIP response message) o avviso di RIP (RIP advertisment).

- **Significato del protocollo ARP e funzionamento**
  Il protocollo ARP serve per risalire all'indirizzo fisico di un nodo della rete al quale vogliamo inviare i dati.
  Quando un nodo deve spedire un pacchetto, invia una richiesta ARP in broadcast con l'indirizzo IP del nodo che sta cercando, il nodo corrispondente riconosce il proprio IP e invia in una risposta ARP il proprio indirizzo fisico. L'indirizzo fisico del destinatario viene memorizzato in una memoria cache. Ogni volta che un nodo deve spedire ad un indirizzo controlla nella cache se ha già il suo indirizzo fisico o no.

- **Qual è quel protocollo che, nella rete Internet, è utilizzato da qualunque applicazione debba trasmettere una qualsiasi informazione? Che tipo di servizio fornisce?**
  È il PROTOCOLLO IP. Fornisce un servizio DATAGRAM= non connesso, senza riscontro.

- **In un protocollo di routing di tipo distance vector:**
  -cosa contengono i messaggi inviati dai router?
  coppie ID_nodo – distanza (normalmente in numero di hop, o secondo qualche altra metrica) **-a chi sono destinati?**
  soltanto ai router adiacenti
  -come vengono utilizzati?
  mediante l'algoritmo di merge ogni router costruisce la propria tabella di routing e il nuovo distance vector da inviare: per ogni destinazione presente nei distance vector ricevuti

- **Che cosa è il router di default? Come la si rappresenta?**
  Le tavole di routing contengono solo una lista parziale delle possibili destinazioni. Per ndicare tutte le desti-nazioni non presenti si crea una rotta di default 0.0.0.0., presente all'ultima riga della tabella di instradamento.

- **Descrivere il funzionamento dell'applicazione ping.**
  Il comando ping invia all' host (computer che si vuole raggiungere) dei messaggi di Echo Request attraverso il protocollo ICMP, il computer interrogato risponde a queste richieste con altrettanti messaggi di risposta detti di Echo Reply, una volta ricevute queste vengono mostrate riportando preziose indicazioni sul percorso di rete effettuato e sui tempi di invio e ricezione. Ping invia richieste echo finché non viene fermato, esso assegna un valore al campo ID e lo utilizza oppure assegna un valore nel campo numero di sequenza incrementandolo ad ogni richiesta. Inoltre, calcola il tempo di andata e ritorno per ogni richiesta echo.

- **Descrivere il funzionamento dell'applicazione traceroute. Per quale motivo la rotta fornita da questa applicazione potrebbe essere inconsistente?**
  Il comando traceroute permette di scoprire il percorso, cioè la sequenza di router che attraversa un datagram IP dal mittente al destinatario sfruttando i messaggi di tempo scaduto e destina nazione non raggiungibile di ICMP. Ogni volta che il pacchetto attraversa un router viene decrementato il TTL.

LIVELLO TRASPORTO

- **UDP**
  UDP (User Datagram Protocol) permette di inviare datagram IP senza stabilire una connessione. Implementa un servizio di consegna inaffidabile dei dati a destinazione. L'applicazione specifica la porta di destinazione, ed in ricezione UDP recapita il campo dati al destinatario. UDP non si

preoccupa di sapere nulla sul destino del segmento inviato, ne comunica all'applicazione qualsiasi informazione. A differenza del TCP, UDP si occupa di un datagramma per volta ovvero quando un'applicazione passa dati ad UDP, UDP li maneggia in un unico segmento, senza suddividerlo in pezzi. Il segmento viene passato ad IP che eventualmente lo frammenta, ma a destinazione UDP riceverà il datagramma intero. L'applicazione di destinazione riceverà quindi il blocco completo di dati inviato dalla applicazione che li ha trasmessi. Benché inaffidabile UDP può utilizzare trasmissione broadcast o Multicast; è molto leggero, quindi efficiente e la mancanza di meccanismi di controllo rende ancora più rapida l'elaborazione del segmento ed il recapito dei dati.

- **Cos'è una porta effimera?**

Una porta del livello di trasporto (quindi un TSAP) assegnata dinamicamente dal sistema operativo all'applicazione client come porta mittente. Su tale porta il client riceverà le risposte dal server (che invece normalmente usa una "well Known port")

- **TCP**

TCP definisce un protocollo di trasporto orientato alla connessione, progettato per fornire un flusso affidabile end-to-end su una internet affidabile. Il suo funzionamento è molto semplice. In trasmissione, riceve un flusso di dati dall'applicazione, aventi stessa origine e stessa destinazione. Li organizza in unità lunghe al massimo 64Kb, chiamate segmenti e le spedisce come datagram IP. In ricezione invece, ricevuti i datagram IP, ne ricostruisce il flusso di byte originale nella sequenza corretta.

- **Differenze tra UDP E TCP**

*Trasmission Control Protocol (**TCP**) definisce un protocollo di trasporto orientato alla connessione, progettato per fornire un flusso affidabile end-to-end su una internet inaffidabile; viceversa User Data Protocol (**UDP**) definisce un protocollo senza connessione, permettendo infatti, di inviare datagram IP senza stabilire una connessione. Si tratta di un servizio che non ha nessun valore aggiuntivo, invia i pacchetti e basta.*

- **Differenza UDP (livello trasporto) con IP (livello network(rete))**

UDP come sappiamo, implementa un servizio di consegna inaffidabile dei dati a destinazione. UDP riceve i dati dalla applicazione e vi aggiunge un header di 8 byte, costruendo così il segmento da inviare. UDP non si preoccupa di sapere nulla sul destino del segmento inviato, né comunica all'applicazione qualsiasi informazione. Di fatto costituisce semplicemente una interfaccia ad IP (che fornisce lo stesso tipo di servizio), con l'aggiunta di fare multiplexing del traffico delle applicazioni su IP:
– tramite il meccanismo delle porte a cui sono associate le applicazioni, di fatto UDP realizza un multiplexing dei dati delle diverse applicazioni su IP.

- **3 way handshaking**

*Quando il livello di trasporto deve stabilire una connessione TCP, deve mettere su il canale (perchè connection-oriented). Deve quindi, effettuare uno scambio fra le 2 parti, che prende il nome di 3-way-hanshaking. La macchina 1 che vuole stabilire/aprire la connessione manda un segmento TCP, con il bit **SYN (flag sincronizzazione)** alzato ed il suo specifico sequence number. La macchina 2 ricevendo questa richiesta di sincronizzazione, la deve necessariamente riscontrare. Manda così un pacchetto che ha sia il bit SYN alzato, con il proprio sequence number, ma anche il bit ACK. Quando il lato 1, a questo punto, riceve l'ACK del SYN, a sua volta trasmette l'ACK. Solo adesso, le due parti sanno effettivamente di essersi sincronizzate e possono finalmente cominciare a trasmettere i file. Per la chiusura si fa un hanshaking a 4 vie. La connessione è full-duplex e le due direzioni devono essere chiuse indipendentemente. L'host 1 vuole chiudere la connessione, quindi, invia un bit **FIN (flag di chiusura)** con il proprio sequence number ed il riscontro dell'ultimo pacchetto ricevuto. L'host 2 riscontra in tal modo, la chiusura della connessione. Tuttavia, la chiusura, a questo punto, è avvenuta solo dalla parte dell'host 1. L'host 2, infatti, può ancora inviare dati all'host 1, perchè non ha chiuso ancora la connessione. Quando poi decide di chiudere,*

anche l'host 2 invia un bit FIN e ne aspetta il relativo riscontro. Ricevuto il riscontro, la connessione è definitivamente chiusa da ambo i lati.

- **Elencare e spiegare il significato dei parametri necessari per la configurazione di un calcolatore collegato a una rete TCP/IP.**
  Indirizzo IP: è l'indirizzo dell'host, serve, tra l'altro, per rispondere all'ARP e per sapere se un destinatario appartiene alla stessa subnet oppure no.
  Netmask: è la maschera di bit che consente di individuare la parte dell'indirizzo che identifica rete e sottorete di appartenenza.
  Default gateway: è l'indirizzo IP della porta del router che deve essere utilizzato per inoltrare i pacchetti a destinatari esterni alla propria subnet.
  Indirizzo IP del DNS server: è il calcolatore che, nel proprio dominio, fornisce il servizio di traduzione di indirizzi da testuali a numerici.

- **TCP (controllo della congestione)**
  Il TCP adatta la velocità di trasmissione alla capacità della rete utilizzando una finestra di congestione che ha la stessa funzionalità della finestra di trasmissione usata per il ricevente. La dimensione della finestra di congestione è ridotta se scade il time-out di ritrasmissione.

- **Porte TCP**
  Le applicazioni che utilizzano il TCP/IP si registrano sullo strato di trasporto ad un indirizzo specifico, detto porta. La porta è il meccanismo che ha a disposizione una applicazione per identificare l'applicazione remota a cui inviare i dati. La porta è un numero di 16 bit (da 1 a 65535; la porta 0 non è utilizzata). Le porte attive definiscono i servizi TCP disponibili. Per connettersi ad un servizio specifico su un server si deve conoscere il numero di porta su cui il processo server accetta le connessioni. Esiste una autorità centrale, lo ***IANA*** *(Internet Assigned Numbers Authority), che pubblica la raccolta dei numeri di porta assegnati alle applicazioni negli RFC. I numeri delle porte vengono divisi in tre gruppi:*
  • Well-Known-Ports (0 – 1023): Queste porte vengono assegnate univocamente dall'IANA; • Registered Ports (1024 – 49151): L'uso di queste porte viene registrato a beneficio degli utenti della rete, ma non esistono vincoli restrittivi;
  • Dynamic and/or Private Ports (49152 – 65535): Non viene applicato nessun controllo all'uso di queste porte. Si tratta essenzialmente di porte di servizio assegnate agli utenti quando hanno bisogno dinamicamente di stabilire una connessione.
  Le porte valgono sia per TCP che per UDP, ma hanno significati differenti. Pertanto, in realtà si hanno 65535 porte per TCP e altrettante porte UDP, tra loro indipendenti. Non si vedono ne comunicano tra loro.
- **Differenze livello di trasporto e livello network**
  Il livello di trasporto è il primo livello che si usa definire di tipo ***end-to-end****, a differenza dei livelli sottostanti, come il livello di rete, che lavorano* ***peer-to-peer (pari a pari),*** *cioè un hop alla volta. Il livello di trasporto è infatti il primo livello che non gira più sull'infrastruttura di rete vera e propria, bensì direttamente sulle macchine di terminazione.*

- **A livello di trasporto, a cosa serve il sequence number?**
  A specificare il numero d'ordine dei byte di dato contenuti nel pacchetto e ad eliminare i messaggi ricevuti duplicati.

- **TCP implementa un ARQ di tipo Go-Back-N o ritrasmissione selettiva?**
  TCP utilizza una via di mezzo tra GO-BACK-N e la ripetizione selettiva. La finestra scorrevole è simile a quella della GO-BACK-N poiché non vengono utilizzati riscontri negativi ed è simile alla finestra selettiva poiché i dati sono accettati anche se fuori ordine, la dimensione della finestra è determinata dal minimo di due valori:
  1) la dimensione della finestra del ricevitore e 2) la dimensione della finestra di congestione.

La prima comunicata dal destinatario al mittente, la seconda calcolata dalla rete per evitare congestioni. TCP può spedire se la finestra non è nulla. Se la finestra è molto piccola si inviano segmenti di dati piccoli ma si ha un sovraccarico delle intestazioni.

LIVELLO APPLICAZIONE

- **Cosa è il DNS?**

  Poiché la rete in se sa interpretare solo indirizzi numerici, sono necessari meccanismi per convertire i nomi in indirizzi di rete. Il DNS (Domain Name System) quindi non è altro che un meccanismo infrastrutturale che fa una mediazione. Il DNS non è altro che un DATABASE DISTRIBUITO, a cui viene fatta una richiesta con un nome simbolico e questo nome simbolico si chiama FQDN (Fully Qualified Domain Name). La componente più semplice è quella presente sui PC, che si chiama RESOLVER. Questa componente è l'entità che , quando si fa riferimento al FQDN, parte ad effettuare query sul database. Una volta ottenuti i risultati passa al livello di trasposto prima, poi al livello rete, l'indirizzo a 32 bit corretto. Questo resolver lavora poggiandosi sui servizi di trasporto e in particolare utilizza UDP sulla porta 53. In certi casi si può utilizzare anche TCP sempre sulla porta 53. Il resolver quindi invia un pacchetto UDP contenente la richiesta ad un server DNS locale, che cerca il nome e restituisce l'indirizzo IP al DNS locale che a sua volta la restituisce al resolver. Equipaggiato dell'indirizzo IP, il programma può quindi stabilire una connessione TCP con la destinazione oppure inviarle pacchetti UDP.

- **Query ricorsive (interrogazione iterativa e ricorsiva)**

  INTERROGAZIONE RICORSIVA:

  Nella query ricorsiva il resolver propaga la richiesta al Name server(indirizzo IP del DNS Server) di livello superiore che gestisce la stessa negoziando con gli altri Name server nella gerarchia. Le richieste non si propagano ai livelli superiori se un Name server ha la risposta nella cache. I record sono inseriti nella cache con un time -to-live.

  INTERROGAZIONE ITERATIVA:

  Nella query iterativa la negoziazione con i vari name server autoritativi per le zone interessate è gestita direttamente dal resolver.

- **Come funziona la posta elettronica? (SMTP)**

  La posta elettronica è un'applicazione basata sul protocollo SMTP (SYMPLE MAIL TRANSFER PROTOCOL) la posta elettronica viene consegnata costituendo una connessione tra la macchina sorgente e la porta 25 della macchina di destinazione. In ascolto su questa porta esiste un server di posta che usa proprio SMTP. Se un messaggio non può essere consegnato al mittente viene restituito un rapporto di errore. SMTP è un semplice protocollo ASCII, quindi solo testuale. Nelle mail è però possibile inserire contenuti multimediali, perché queste informazioni quando vengono trasmesse attraverso il protocollo SMTP vengono ricodificate e trasformate in una serie di caratteri ASCII, attraverso una codifica base 64. Il servizio di posta elettronica funziona essenzialmente in una logica Client-Server, in cui si ha che i client sono gli AGENTI UTENTI, ossia le applicazioni sul pc dell'utente. Le query richiedono transizioni di trasferimento della posta ad un'altra entità detta: AGENTI DI TRASFERIMENTO DEI MESSAGGI. Quest'ultimi sono dei server che ricevono connessioni, utilizzando questo protocollo SMTP sulla porta 25, che si occupano di accedere e trasferire i contenuti (testo, files,..). Un lavoro importante è svolto dai RELAY AGENTS. Si tratta di server di riferimento per l'invio della posta. Tutti i client inviano la posta al relay che la invia al destinatario.

  - Semplifica la configurazione

  - Sono sempre connessi (possono ritentare in caso di insuccesso).

- **Cos'è l'SNMP? A che livello di ISO/OSI si colloca?**

  Simple Network Management Protocol. È un protocollo di livello applicazione del TCP/IP, si colloca al livello 7 della pila ISO/OSI e serve per la gestione remota e il monitoraggio delle