Telecomunicazioni al nocciolo

Strato di collegamento

- **Framing**
  - Flag: 01111110
  - bit stuffing/destuffing (si inserisce uno 0 ogni cinque 1, flag esclusi)
  - byte stuffing/destuffing (si inserisce 01111101 prima di 01111110 nel codice o di un 01111101)
- **Rilevazione errori**
  - Controllo a parità singola (un solo bit avente valore 1 – quando il numero di bit 1 nel codice è dispari – altrimenti 0. Bit di parità+codice da proteggere = codeword)
  - Controllo parità bidimensionale (maggiore rilevazione di errore, non vengono rilevate alcune configurazioni con 4 o più errori, molto overhead)
  - Internet Checksum ($x = b_0 + b_1 + b_2 + ... + b_{L-1}$ modulo$(2^{bitPerParola}-1)$; $b_L = -x$ modulo$(2^{bitPerParola}-1)$ – il messaggio si scompone in più parti di tot bit)
  - Codice CRC (si utilizza un polinomio generatore che deve essere noto tra mittente e destinatario. Un codice polinomiale, in cui il polinomio generatore contiene x+1 come fattore primo, è in grado di rivelare: tutti gli tutti gli errori singoli errori singoli o doppi; tutti gli errori isolati con una molteplicità dispari; tutti gli errori a burst di lunghezza $\leq Z$)
  - FEC (Forward Error Correction – posto W(A) il numero di bit 1 nella stringa A, si definisce la distanza di Hamming H(X,Y) = W(X xor Y) ove X e Y sono stringhe binarie)
- **Protocolli Mac**
  - Protocolli di accesso multiplo a suddivisione del canale (slot di tempo, frequenza, codice)
  - Protocolli di accesso multiplo dinamico, divisi in
    - Accesso controllato
      - Token Passing
      - Protocollo polling
    - Accesso casuale
      - Possibili collisioni
      - Diversi protocolli (Aloha, Slotted Aloha, CSMA, CSMA/CD, CSMA/CA)
  - Prodotto banda ritardo: PBR = R * d (banda * ritardo end to end; è il numero di bit che attraversano contemporaneamente un canale
  - Protocollo ALOHA
    - Intervallo vulnerabilità (to-X, to+X)
    - Il nodo trasmette la frame appena pronta, si attende un tempo di timeout to+X+2tprop, in attesa di verificare eventuali collisioni. In caso di collisione si stabilisce un backoff time casuale e si riprova a trasmettere.
  - Slotted ALOHA
    - Tutti i pacchetti hanno la stessa dimensione

        - Il tempo è suddiviso in slot; ogni slot equivale al tempo di trasmissione di un pacchetto
        - I nodi iniziano la trasmissione dei pacchetti solo all'inizio dello slot. Tutti gli slot dei nodi sono sincronizzati.
        - L'intervallo di vulnerabilità è pari a X
        - Nel migliore dei casi solo il 36% degli slot sono utilizzati in modo utile
    - Accesso multiplo a rilevazione della portante (CSMA)
        - Un nodo ascolta prima di trasmettere. Se rileva che il canale è libero, trasmette l'intera frame. Se il canale è occupato, il nodo aspetta un altro intervallo di tempo.
        - L'intervallo di vulnerabilità è pari a $2*t_{prop}$
        - Quando un nodo rileva un canale occupato.
            - 1 persistent, ritrasmette appena si libera il canale
            - Non persistent, si applica un backoff time e poi si effettua un nuovo carrier sensing
            - P-persisten, con una certa percentuale p trasmette; con una percentuale 1-p si aspetta un breve intervallo e si procede con il carrier sensing
    - Protocollo CSMA/CD (code detection)
        - Rileva delle collisioni anche durante la trasmissione
        - Nel caso peggiore si rileva la collisione dopo un tempo t=2*tprop
        - Usato in Ethernet
    - Protocollo CSMA/CA (collision avoidance)
        - Usato in standard 802.11
        - Se il mezzo è libero
            - Il terminale attende un periodo di tempo variabile chiamato DIFS e poi inizia a trasmettere
        - Se il mezzo è occupato
            - Si attende un back-off time (a partire da una Contention Windows) e un intervallo DIFS e poi si ritrasmette.
            - Il valore della Contention Window parte da 15 slot e viene raddoppiato ad ogni eventuale collisione successiva (15,31,63 ecc)
            - Il tempo di back-off è definito in maniera casuale a partire dall'intervallo (0, CW)
    - Protocollo polling
        - Un nodo principale (master) sonda gli altri (slaves)
        - Se il nodo principale si guasta l'intero canale resta inattivo
    - Protocollo Token Passing
        - Un messaggio di controllo (token) circola fra i nodi seguendo un ordine prefissato
        - Il flag del token può essere 01111110 (free token), 01111111 (busy token)
        - Ring latency: numero di bit trasmissibili simultaneamente sul ring
        - Diverse possibili operazioni con i token:
            - Multi-token operation (il free token è trasmesso subito dopo l'ultimo bit di una frame). Throughput massimo: 1 / (1 + a/M) ove a = tau/T (tau = tempo

richiesto ad un bit per circolare sul ring, T tempo di trasmissione di una frame)

- Single-token operation (il free token è inserito dopo che l'ultimo bit del busy token è ritornato al nodo di origine). Throughput massimo: 1 / (1 + a(1 + 1/M)
- Single-frame operation (il free token è inserito dopo che il nodo emittente ha ricevuto l'ultimo bit della sua frame) . Throughput massimo: 1 / (a/M + max(1,a))

- **Error recovery**
  - **Stop & Wait ARQ**
    - L'entità A trasmette la frame e poi aspetta il riscontro dell'ACK per un certo intervallo di time-out
    - Si utilizzano due bit per rappresentare la frame corrente ricevuta e la successiva che si aspetta di ricevere
    - Ci sono due stati (Wait, Ready) per il trasmitter e un solo stato (Ready) per il receiver.
    - Rate di trasmissione efficace (nf – no)/to. Numero bit informativi consegnati fratto il tempo necessario per consegnarli
    - Efficienza di trasmissione: Rate trasmissione efficace / bitrate a disposizione
  - **Go-back N ARQ**
    - Utilizza una finestra in trasmissione di ampiezza Ws frame che consente di inviare in sequenza un certo numero di frame
    - Se la finestra si esaurisce, la trasmissione viene interrotta in attesa degli ACK
    - Se non sono ricevuti ACK, allo scadere di un timeout le frame della finestra vengono ritrasmesse. Altrimenti si aggiorna la finestra e si procede con il successivo gruppo di frame.
    - Per garantire una gestione univoca delle frame, la finestra di trasmissione è W = M 1=2^m-1
  - **Selective Repeat ARQ**
    - Selective Repeat ritrasmette s l le frame che s n state perse
    - Si usa l'ACK per convalidare la ricezione e la NAK per richiedere la ritrasmissione di una frame non ricevuta.
    - Le frame successive a quella persa e già ricevute vengono bufferizzate in attesa che la frame persa venga ritrasferita correttamente
    - La finestra di trasmissione può avere valore massimo Ws + Wr = 2m, così che le finestre del receiver e del trasmitter non portino a casi di ambiguità
- **Controllo di flusso**
  - La gestione del flusso consente di evitare i casi di overflow del buffer
  - Si utilizzano segnali XON e XOFF per gestire indicare quando si possono trasmettere frame al receiver e quando no
    - Si deve attivare il segnale di Off in modo da evitare la perdita di pacchetti
    - Lo spazio disponibile nel buffer deve essere almeno uguale a 2* Tprop*R bit per garantire la correttezza delle operazioni
    - Si può vedere la finestra di tramissione come un metodo per definire la quantità massima di frame per evitare overflow. Anche gli ack possono

essere intesi come permessi che concedono per trasmettere o meno le frame.

- **Protocollo PPP**
  - È un protocollo di tipo Point To Point
  - Si occupa di garantire una serie di operazioni:
    - Framing dei pacchetti (il protocollo PPP incapsula un pacchetto a livello di rete all'interno del un pacchetto PPP a livello di link)
    - Trasparenza (non si devono porre limiti sul tipo di dati che sono contenuti nel pacchetto a livello di rete)
    - Rilevazione errori (ma non loro correzione)
  - Il protocollo PPP NON si occupa di:
    - Correzione errori
    - Controllo del flusso
    - Controllo sequenza pacchetti
  - Nel PPP ogni frame inizia con un flag
- **Protocollo HDLC**
  - I frame dati HDLC possono essere trasmessi attraverso collegamenti sincroni o asincroni.
  - Questi collegamenti non possono determinare l'inizio o la fine di un frame, si devono quindi utilizzare i flag
  - I tipi di stazioni sono 3:
    - Terminale primario: è responsabile delle operazioni di controllo sul collegamento. Manda i frame di controllo (comandi).
    - Terminale secondario: lavora sotto il controllo di quello primario. Spedisce solo pacchetti di risposta. Il primario è collegato ai secondari attraverso collegamenti logici multipli.
    - Terminale combinato: ha le caratteristiche di entrambi i terminali sopra. Spedisce sia comandi sia risposte.
  - Questa classificazione contraddistingue tre modalità di funzionamento:
    - ABM (Asynchronous Balanced Mode): in cui interagiscono terminali combinati.
    - NRM (Normal Response Mode): in cui un terminale primario inizia a trasmettere e il secondario risponde se interpellato.
    - ARM (Asynchronous Response Mode): fondamentalmente come l'NRM, con la differenza che un terminale secondario può trasmettere anche senza l'autorizzazione di un terminale primario.
- **Indirizzi MAC**
  - Caratteristiche indirizzi mac
    - Costituito da 48 bit (ipv4 solo 32)
    - È associato al dispositivo e non varia al variare della rete
  - **Tabelle ARP**
    - Ogni nodo IP nella LAN ha una tabella ARP
    - Le tabelle ARP associano a un indirizzo IP il relativo indirizzo MAC del dispositivo ed il TTL (time to live, tipicamente pari a 20 minuti)

        - Quando un host A vuole inviare un messaggio ad un host B il cui indirizzo MAC non è presente nella tabella ARP di A, viene inviata in una frame in broadcast il messaggio di richiesta ARP. B risponde con una semplice frame ad A inviandole il suo indirizzo ARP e il TTL. La tabella ARP di A è aggiornata.
- **Standard Ethernet 802.3**
    - Fa uso di CSMA/CD
        - Se il canale è inattivo la frame Ethernet 802.3 viene inviata
        - Se il canale è occupato si resta in attesa che si liberi
        - Se rileva collisioni, si interrompe il trasferimento e si invia un segnale di disturbo detto jam (di 48 bit) che ha lo scopo di avvisare tutti gli altri host che stanno trasmettendo in rete
        - In presenza di errori si aspetta un tempo pari a K volte 512 bit, con K contenuto nell'intervallo $(0,1,2,\ldots,2^n-1)$, ove n è il numero della ritrasmissione
            - Alla prima ritramissione K appartiene all'intervallo (0,1)
            - Alla seconda ritramissione (0,1,2,3)
            - Dopo dieci ritrasmissioni K appartiene all'intervallo (0,1,2,…,1023)
    - Con un tramission rate di 10Mbit/s si può usare un collegamento Ethernet di lunghezza massima pari a 2500 metri, comprensivo di 4 repeater (ossia 500 metri a tratto)
    - Ogni aumento di 10 volte del bitrate corrisponde ad una diminuzione di 10 volte della massima lunghezza della rete
- **Hub (repeater)**
    - Opera allo strato fisico
    - Rigenera il segnale analogico (re-shaping , re-timing e re-trasmitting) e lo ritrasmette su tutte le interfacce uscenti
    - Rileva eventuali collisioni e avvisa tutti gli host connessi ed isola temporaneamente i tratti di connessione in cui avvengono più di 30 collisioni
        - Questo consente di aumentare le dimensioni di una LAN, superando il limite teorico imposto dal protocollo CSMA/CD
- **Switch (Bridge**)
    - Opera a livello di link
    - Filtra e inoltra le frame Ethernet
    - Esamina l'indirizzo MAC di destinazione e, se possibile, lo invia all'interfaccia corrispondente alla sua destinazione
    - Usa il protocollo CSMA/CD
    - Ogni switch ha una tabella di commutazione (switch table), che comprende
        - L'indirizzo MAC del dispositivo
        - La porta dello Switch a cui è connesso
        - Il TTL (time to live)
    - Le Switch Table non necessitano aggiornamento in reti statiche, mentre devono essere aggiornate qualora i dispositivi possano cambiare nel tempo
    - Gli Switch e i Router sono entrambi dispositivi store-and-forward
        - I router sono a livello di rete e hanno tabelle di routing e implementano gli algoritmi di instradamento

        - Gli switch sono a livello di collegamento, hanno tabelle di switching e implementano algoritmi di filtraggio e autoapprendimento
- **Spanning Tree Protocol (STP)**
    - Serve per rimuovere eventuali loop all'interno della rete
    - Opera in tre fasi
        - Definisce un Root Bridge (la radice dell'albero)
            - Tutti quanti gli switch si credono inizialmente "Root" e allora mandano una trama BPDU (Bridge Protocol Data Unit) contenente come Root ID = Switch ID
            - Alla fine solo lo switch con l'identificativo più piccolo genera Configuration BPDU -> Root Bridge
        - Seleziona la Root Port per ogni switch (ossia la porta usata da ogni switch per raggiungere il root bridge – viene scelta la porta a minor costo per raggiungere il root bridge)
        - Seleziona le Designated Port, cioè la porta utilizzata da ogni LAN per inviare e ricevere trame
- **Wireless LAN**
    - Il Bit Error Rate (BER) è molto più elevato rispetto ad un ambiente "wired"
    - Le operazioni di Collision Detection sono difficili perché una stazione non è in grado di ascoltare le proprie trasmissioni e quindi rivelare eventuali collisioni
    - Possono esserci casi di Hidden Terminal
        - Due host possono inviare ad un dispositivo i dati contemporaneamente perché i due host non si vedono vicendevolmente e non rilevano nulla con il Carrier Sensing
        - Si può risolvere facendo fare il Carrier Sensing al receinver, con il cosiddetto "Virtual Carrier Sensing"
    - Lo standard 802.11 utilizza il protocollo CSMA/CA
        - Non stabilisce valori minimi o massimi per la Contention Window
        - Ogni slot di tempo ha una durata di 9 microsecondi.
        - Sono comunque consigliati un valore minimo di CW di 15 slot (15*9microsecondi) e massimo di 1023 slot (1023*9)
    - Ci può essere un meccanismo opzionale di prenotazione del canale
        - Si usano i pacchetti RTS (Request to send) e CTS (Clear to send)
        - All'interno dei pacchetti RTS e CTS si specifica l'intervallo di tempo in cui il canale sarà occupato.
            - È il cosiddetto Net Allocation Vector (NAV) che indica il tempo minimo da attendere qualora si volesse testare il canale per vedere se è libero.

Strato di rete

- Tipologia delle reti
    - **Reti a circuito virtuale (VC)**
        - Servizio connection oriented

        - Si stabilisce il percorso che i pacchetti devono seguire attraverso comunicazioni tra i singoli switch del percorso (Connect Request – Connect confirm)
        - La connessione che si instaura è identificata da un Virtual Cuircuit Identifiers (VCI) specifico per ogni tratto del percorso
        - La Virtual Circuit Forwarding Table è una tabella contente il VCI di input, quello da inserire in output nell'intestazione del pacchetto in fase di uscita e la porta attraverso cui instradare il pacchetto
    - **Rete a datagramma**
        - È una rete stateless
        - Si utilizzano gli indirizzi per inoltrare i pacchetti nella rete
- **Protocollo IP**
    - Il protocollo IP esegue le seguenti funzioni
        - definisce il formato dei pacchetti
        - lo schema di indirizzamento e le modalità di instradamento
        - frammenta e riassembla, se necessario, i dati nei pacchetti
    - Il pacchetto IP ha sempre almeno 20 byte di intestazione (contenente flag, indirizzi di destinazione e di provenienza, versione protocollo, offset ecc), più eventuali altri 40 byte massimi per informazioni aggiuntive facoltative (totale massimo 60 byte)
    - Alcuni flag gestiscono la frammentazione dei pacchetti
        - DF: Don't Fragment (0: frammentazione permessa; 1: frammentazione vietata)
        - MF: More Fragment (0: ultimo frammento del pacchetto; 1: non è l'ultimo frammento)
- **Protocollo ICMP**
    - Il protocollo ICMP (RFC 792, 950) consente ai router di inviare all'host sorgente informazioni riguardanti anomalie nel processamento di un riguardanti anomalie nel processamento di un pacchetto
    - I messaggi ICMP non sono elaborati dai router intermedi
    - Alcuni errori che possono essere segnalati sono
        - Redirect message (indica al mittente l'indirizzo al quale deve reindirizzare il pacchetto)
        - Destination Unreachable
        - Time Exceeded (quando il TTL – time to live – è scaduto. Il TTL indica il numero massimo di nodi che il pacchetto può attraversare)
- **Classless Inter Domain Routing CIDR**
    - Ideato per rendere più efficiente l'impiego dello spazio di indirizzamento di IP
    - Ad una rete è assegnato un certo numero di blocchi contigui di indirizzi (Supernetting), la rete sarà così caratterizzata da un unico prefisso
- **DHCP – protocollo di autoconfigurazione**
    - Consente ad un host di ottenere dinamicamente il suo indirizzo IP dal server di rete
    - Supporta tre modalità: automatica (assegnazione automatica e permanente di un indirizzo IP), dinamica (assegnazione indirizzo IP per un breve periodo di tempo), manuale (scelta dall'amministratore della rete)

    - Può quindi rendere la gestione dell'assegnazione degli IP dinamica, ma pone dei paletti perché il suo utilizzo è dipendente dall'utilizzo di un apposito server e non è vero "Plug&play" perché i dispositivi connessi devono supportare il protocollo
    - Problemi di sicurezza
- **Network Address Translator NAT**
    - Assegna un indirizzo IP globale ad un dispositivo in maniera dinamica, solo quando gli serve
    - Quando non deve trasmettere fuori dalla rete il dispositivo è identificato da un indirizzo IP locale
    - I dispositivi sono invisibili al di fuori della rete intranet quando non hanno bisogno di essere rilevati dall'esterno
    - È però contestato perché
        - non è del tutto compatibile con le dinamiche del protocollo TCP/IP
        - interferisce con le comunicazioni P2P
        - è incompatibile con il protocollo ICMP
        - Il checksum dei pacchetti che riceve deve essere ricalcolato
- **Sistemi autonomi nella rete IP**
    - Un sistema autonomo (Autonomous System - AS) è un insieme di host e router controllato da una singola autorità amministrativa (es. ISP)
    - un particolare AS è detto "Core AS" e costituisce il backbone di Internet. Gli altri router sono detti Stub router
    - I router connessi al core router sono detti Exterior Gateway
    - Un router interno ad un AS è detto Interior Gateway
    - Ogni AS ha il proprio protoccolo di Instradamento
        - I protocolli di instradamento all'interno di un AS sono detti Interior Gateway Protocols
        - Le informazioni di instradamento che coinvolgono più di un sistema autonomo sono gestite mediante gli Exterior Gateway Protocols
- **Algoritmo di Bellman-Ford**
    - Fanno uso di routing table contenenti
        - La destinazione da raggiungere
        - Il nodo successivo da percorrere
        - La distanza in termini di costo del cammino minimo
    - I router adiacenti si scambiano di Distance Vector (DV) per indicare destinazioni e relativi costi
- **Algoritmo di Dijkstra**
    - Individua il cammino a lunghezza minima tra un nodo s e tutti gli altri nodi di un grafo G procedendo in modo da aumentare progressivamente la distanza.
    - Si sceglie sempre il cammino con minore costo
    - La complessità dell'algoritmo è $o(N^2)$, quindi c'è una maggiore complessità rispeto all'algoritmo di Bellman-Ford
- **Routing Information Protocol RIP**
    - È un protocollo di instradamento intra-AS
    - Si basa sul calcolo della distanza tra i vari router con scambio di messaggi
        - Request (per richiedere ai vicini il distance Vector)

        - Response (per rispondere alla richiesta)
    - Se un router non riceve notizie dal suo vicino per 180 sec, il nodo adiacente viene considerato spento o guasto
- **OSPF (Open Shortest Path First)**
    - Utilizza il flooding di informazioni sullo stato dei link (Link State Advertisement – LSA)
    - Gli LSA sono emessi
        - quando un router contatta un nuovo router vicino
        - quando un link si guasta
        - quando il costo di un link varia periodicamente ogni fissato intervallo di tempo
    - Gli LSA sono trasportati mediante la tecnica del flooding
        - È molto affidabile
        - Esplora tutti i cammini tra origine e destinazione
    - In reti di grandi dimensioni OSPF lavora secondo le disposizioni di tipo gerarchico
- **Border Gateway Protocol (GBP)**
    - Rappresenta l'attuale standard de facto per i protocolli EGP
    - BGP mette a disposizione di ciascun AS un modo per
        - ottenere informazioni sulla raggiungibilità delle sottoreti da parte di AS confinanti
        - propagare le informazioni di raggiungibilità a tutti i router interni di un AS
        - determinare percorsi "buoni" verso le sottoreti sulla base delle informazioni di raggiungibilità e delle politiche dell'AS
- **Protocolli inter Protocolli inter-AS vs. protocolli intra-AS**
    - Politiche
        - Inter-AS: il controllo amministrativo desidera avere il controllo come il traffico viene instradato e su chi instrada attraverso le sue reti.
        - Intra-AS: unico controllo amministrativo, e di conseguenza le questioni di politica hanno un ruolo molto meno importante nello scegliere le rotte interne al sistema
    - Scala
        - L'instradamento gerarchico fa "risparmiare" sulle tabelle d'instradamento, e riduce il traffico dovuto al loro aggiornamento
    - Prestazioni
        - Intra-AS: orientato alle prestazioni
        - Inter-AS: le politiche possono prevalere sulle prestazioni

Strato di trasporto

- **Generalità strato trasporto**
    - Demultiplexing nell'host ricevente
        - Obiettivo di consegnare i pacchetti ricevuti alla socket appropriata

- Multiplexing nell'host mittente
    - Raccogliere i dati, incapsularli con l'intestazione (utilizzata poi per il demultiplexing)
- Una socket UDP è identificata da
    - Indirizzo IP di destinazione
    - Porta di destinazione
- Una socket TCP è invece identificata da quattro parametri:
    - Indirizzo IP origine
    - Porta di origine
    - Indirizzo IP di destinazione
    - Porta di destinazione

- **User Datagram Protocol UDP**
    - Protocollo di trasporto "semplice", senza garanzia di sequenza, senza controlli di congestionamento e con possibile perdita dei pacchetti
- **Transport Control Protocol TCP**
    - E' un protocollo con connessione
        - Three Way Handshake
            - L'host A invia un segmento SYN all'host B
            - L'host B riceve SYN e risponde con un segmento SYN ACK
            - L'host A riceve un segmento SYN ACK e risponde con un segmento ACK, che può contenere dati
    - Interpreta il flusso di dati proveniente dallo strato applicativo come sequenza di ottetti
    - È un protocollo con controllo di sequenza
        - La gestione dei segmenti fuori sequenza non è però gestita dallo standard
    - Prevede un controllo degli errori
        - TCP ha lo scopo di offrire un servizio di trasferimento dati affidabile utilizzando il servizio inaffidabile offerto dallo strato di rete (IP)
        - Si utilizzano solo segmenti ACK
        - Un solo timeout di ritrasmissione
        - Le ritrasmissioni sono avviate da esaurimento del timeout o da ACK duplicati
    - Controllo di flusso
        - Il controllo di flusso ha lo scopo di limitare il ritmo di emissione dei dati da parte di un host per evitare la saturazione della capacità del buffer di ricezione
        - TCP utilizza un controllo di flusso basato su una finestra scorrevole di larghezza variabile
    - Controllo congestione
        - È un controllo applicato alla rete e che verifica che non ci siano troppe sorgenti che trasmettono troppi dati ad un rate che la rete non è in grado di gestire