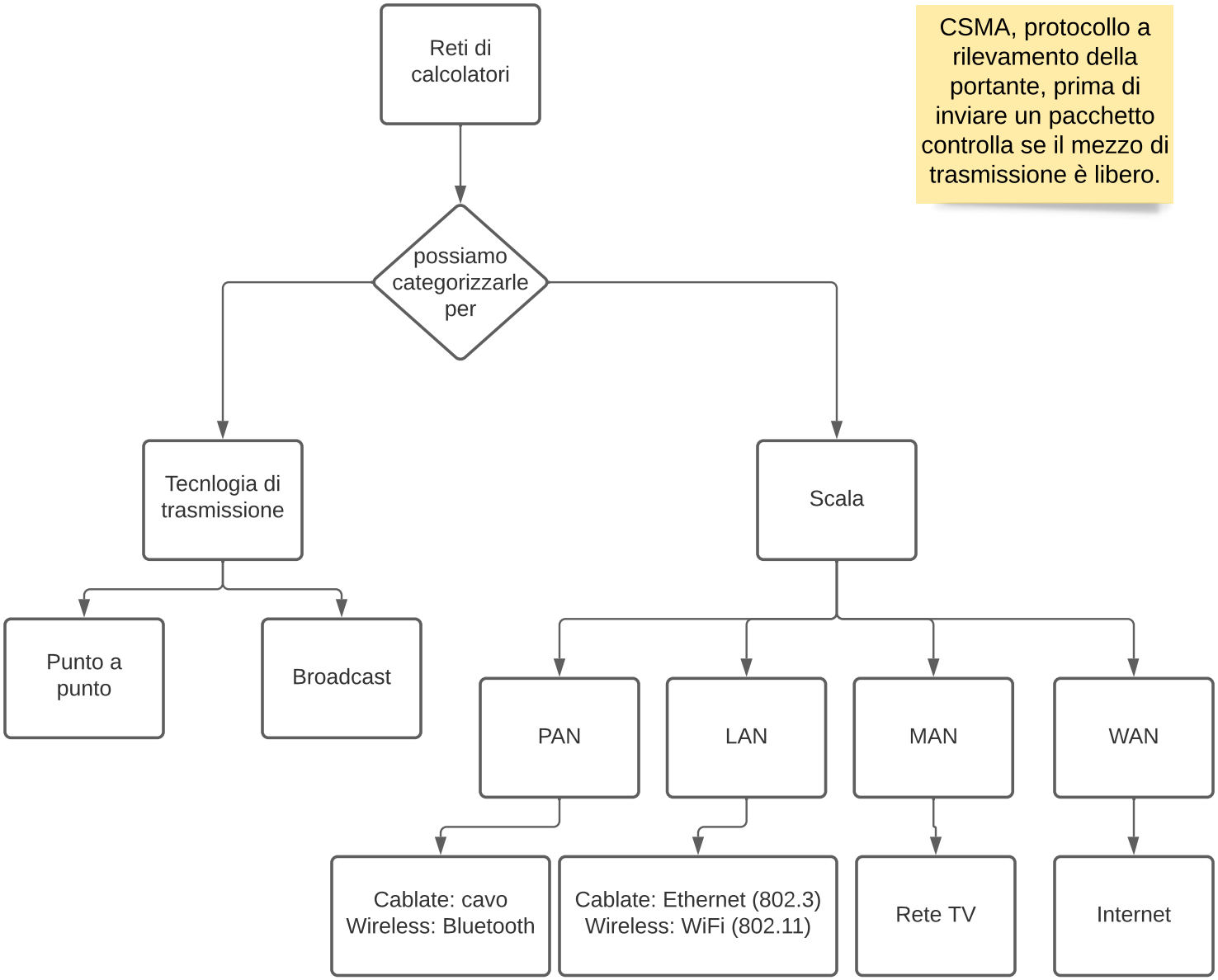


CSMA, protocollo a rilevamento della portante, prima di inviare un pacchetto controlla se il mezzo di trasmissione è libero.

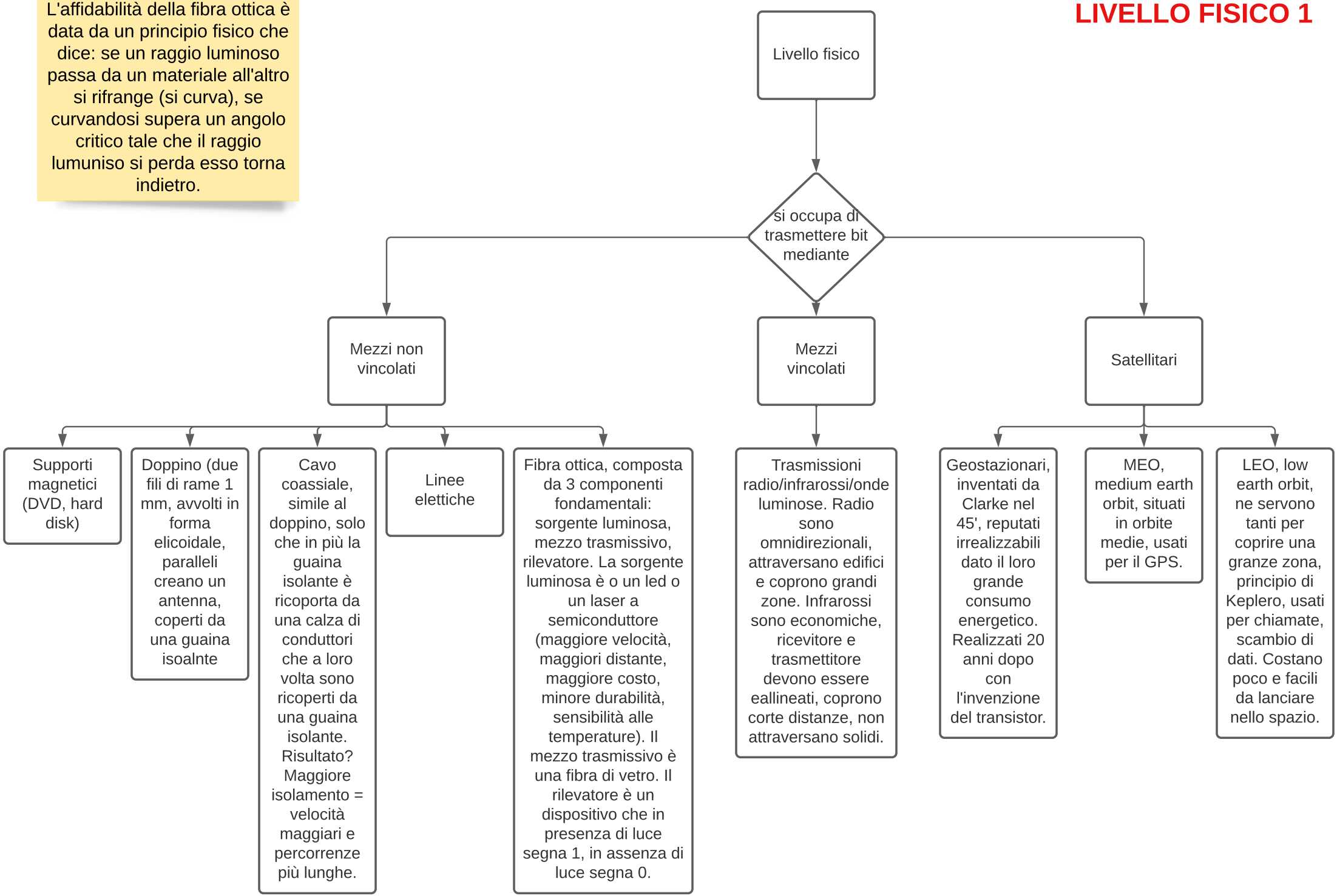
Ethernet nasce da Bob Metcalf, laureato al MIT, ispirandosi al protocollo ALOHA. La prima LAN consisteva nell'uso di un cavo coassale che collegava due PC. Successivamente i PC furono collegati tramite cavi ad un HUB, il quale smistava i pacchetti. Le LAN moderne usano gli switch, migliori perché prevengono le collisioni assegnando ad ogni PC una porta, sono dotati inoltre di un buffer interno, qualora due PC vogliono inviare un pacchetto contemporanemente ad PC il buffer memorizza un pacchetto mentre l'altro viene inviato.

WiFi, standard 802.11, usa le frequenze libere 2.4 GHz e 5GHz, la 5 essendo più libera offre prestazioni migliori, lo standard è studiato per usare frequenze da 2 a 11 GHz. Usa il protocollo CSMA con gestione delle collisioni. La sicurezza è data da WPA 2 (il pc si collega ad un database contente utente e passoword e controlla se l'utente ha l'accesso alla rete). La privacy è data da AES.

Bluetooth, ideato dalla SIG, gruppo voluto da Nokia, IBM ed altre big con l'intento di creare uno standard per collegamenti Wireless che sia a basso costo e raggiunga distanze di massimo 10 metri. Esso usa 2.4 GHz. Per comunicare due dispositivi devono effettuare il pairing.

LIVELLO FISICO 1

L'affidabilità della fibra ottica è data da un principio fisico che dice: se un raggio luminoso passa da un materiale all'altro si rifrange (si curva), se curvandosi supera un angolo critico tale che il raggio lumuniso si perda esso torna indietro.



LIVELLO FISICO 2

Il sistema telefonico mobile si basa su una tecnologia chiamata GSM. La trasmissione delle informazioni avviene mediante onde radio ed il territorio viene diviso in celle dalla grandezza di 10-20 km. Ogni cella usa un insieme di frequenze, diversa dalle celle adiacenti, ma uguale a quelle delle celle non adiacenti. La comunicazione dell'utente avviene mediante un terminale dotato di una scheda SIM che contiene i dati necessari per far identificare l'utente nella rete.

La conversione da bit a segnali analogici si chiama modulazione digitale

esistono due tipologie di trasmissione

Trasmissione in banda base, fa uso della tensione continua, quando c'è tensione vale 1, in assenza di tensione vale 0. In presenza dell'invio di una serie di 0 per distinguerli si usa una tecnica chiamata clock recory, essa usa un temporizzatore dividendo il segnale in tempi.

Trasmissione in banda passante, più comunicazioni usano lo stesso canale usando una tecnica che si chiama multiplexing.

Multiplexing a divisione di frequenza, ogni utente ha un propria frequenza e trasmette solo su quella, evitando così interferenze.

Multiplexing a divisione di tempo, ad ogni utente viene assegnato una fascia temporale entro la quale può trasmettere e ricevere.

Multiplexing a divisione di codice, sarà un algoritmo a decidere quando un utente avrà accesso al mezzo trasmissivo.

Rete telefonica

costituira da tre componenti

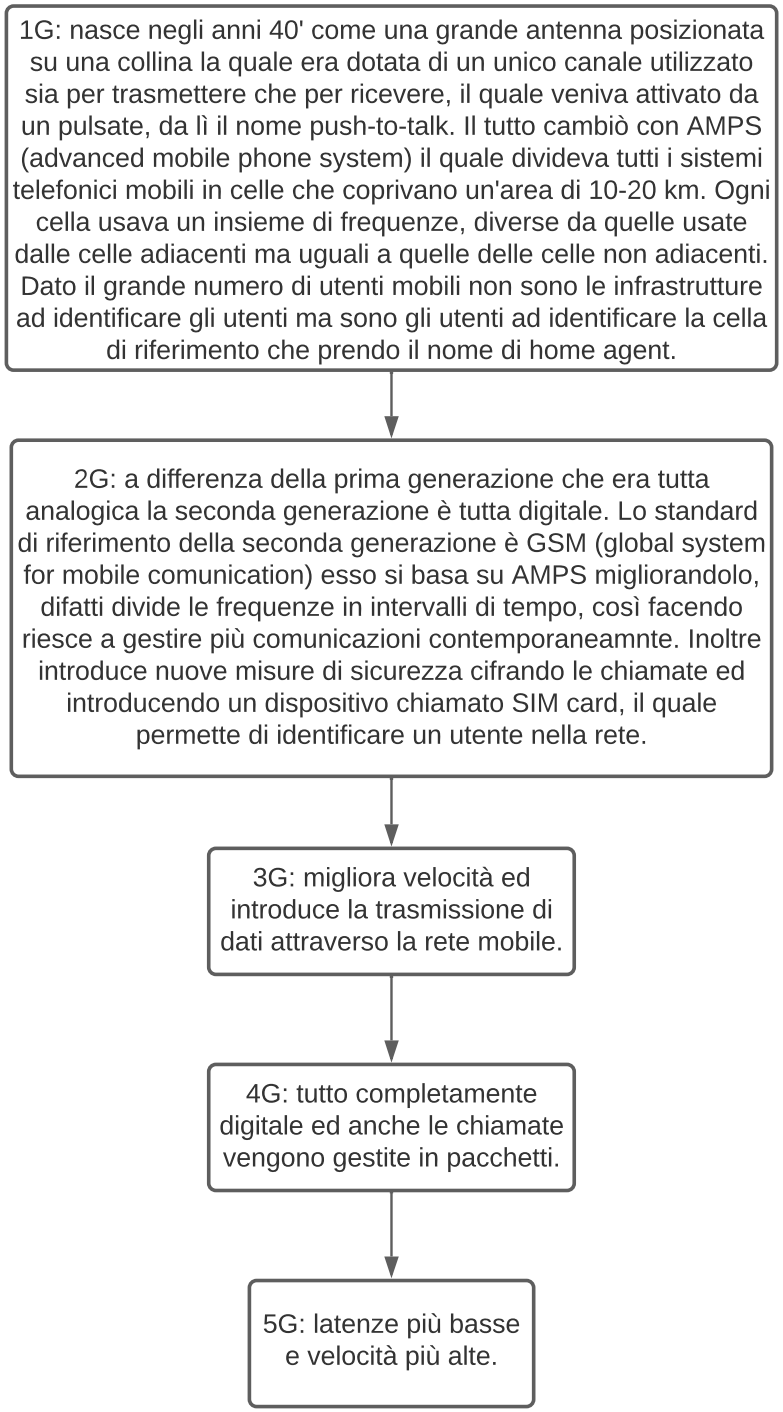
Ultimo miglio, rappresenta la parte che va dalla cabina al modem dell'utente.

Trunk, indica il mezzo di trasmissione che va dalla centrale di commutazione alle varie cabine. Tali mezzi ssono in grado di trasmettere mgliaia di informazioni usando il multiplexing FDM e TDM.

Centrali di commutazione, esse gestiscono la creazione del circuito attraverso cui passano i pacchetti usando due tecniche.

Commutazione di circuito, tenica che si basa sul sistema telefonico tradizionale. Essa concettualmente crea un circuito tra i due interlucutori cercando di creare un vero e proprio percorso fisico. Spreca banda, si guasta uno switch salta la chiamata.

Commutazione di pacchetto, tecnica che stabilisce la comunicazione tra i due interlucutori mediante l'invio di pacchetti. Ottimizza la banda, ottima gestione dei guasti.


1G: nasce negli anni 40' come una grande antenna posizionata su una collina la quale era dotata di un unico canale utilizzato sia per trasmettere che per ricevere, il quale veniva attivato da un pulsate, da lì il nome push-to-talk. Il tutto cambiò con AMPS (advanced mobile phone system) il quale divideva tutti i sistemi telefonici mobili in celle che coprivano un'area di 10-20 km. Ogni cella usava un insieme di frequenze, diverse da quelle usate dalle celle adiacenti ma uguali a quelle delle celle non adiacenti. Dato il grande numero di utenti mobili non sono le infrastrutture ad identificare gli utenti ma sono gli utenti ad identificare la cella di riferimento che prendo il nome di home agent.
2G: a differenza della prima generazione che era tutta analogica la seconda generazione è tutta digitale. Lo standard di riferimento della seconda generazione è GSM (global system for mobile comunication) esso si basa su AMPS migliorandolo, difatti divide le frequenze in intervalli di tempo, così facendo riesce a gestire più comunicazioni contemporaneamnte. Inoltre introduce nuove misure di sicurezza cifrando le chiamate ed introducendo un dispositivo chiamato SIM card, il quale permette di identificare un utente nella rete.
3G: migliora velocità ed introduce la trasmissione di dati attraverso la rete mobile.
4G: tutto completamente digitale ed anche le chiamate vengono gestite in pacchetti.
5G: latenze più basse e velocità più alte.

LIVELLO DATA-LINK

Protocollo simplex stop and wait: protocollo che gestisce l'invio dei dati da solo uno dei due utenti in comunicazione. Il mittende invia i dati, il destinatario li riceve, li elabora e manda un ack al mittente, il quale ricevuto l'ack invia nuovi dati.

I protocolli full duplex gestiscono connessioni in cui entrambe le parti inviano dati. Così facendo si crerebbe un casino tra frame di dati ed ack, quindi gli ack vengono inviati nell'header del frame successivo (piggybacking). Se uno dei frame si danneggia si usano due tacniche. Go-back-n, il destinatario cestina tutti i frame ricevuti dopo il frame corrotto e chiedi al mittente di inviare tutto da capo. Selective-repeat il destinatario richiede al mittente solo il frame corrotto.

Alcune reti sono sono soggette ad errori di trasmissione.

Per individure tali errori il livello data link usa due tecniche:

Codici a correzzione d'errore: stratgie che permettono al destinatario di individuare l'errore.

Codice di Hamming: dati due frame si effettua lo XOR tra i due, i bit diversi che si ottengono rappresentano la distanza di Hamming, più bassa è migliore è la qualità del frame.

Codice di Reed Solomon: sfrutta il principio del codice di Hamming solo che usa un algoritmo più sofisticato che non lavora sui singoli bit ma su gruppi di bit.

Codici a rilevamento d'errore: strategie che permettono al destinatario di sapere se c'è o meno un errore, senza sapere quale.

Bit di parita: tale tecnica fa si che il numero dei bit del frame sia dispari, qualore fosse pari aggiunge un 1 alla fine.

Checksum: esso calcola il valore del frame, ovvero sommando i dati ed effettuando il complemento ad uno della somma. Tale valore si aggiunge alla fine del frame ed il destinatario una volta ricevuto il frame effettua la somma del frame più il checksum, se il risultato è 0 il frame è intatto.

Il livello data link usa algoritmi per rendere affidabile ed efficiente la trasmissione di informazioni, chiamate frame, tra due macchine. Questo implica che un informazione prima di essere trasmessa viene divisa per frame.

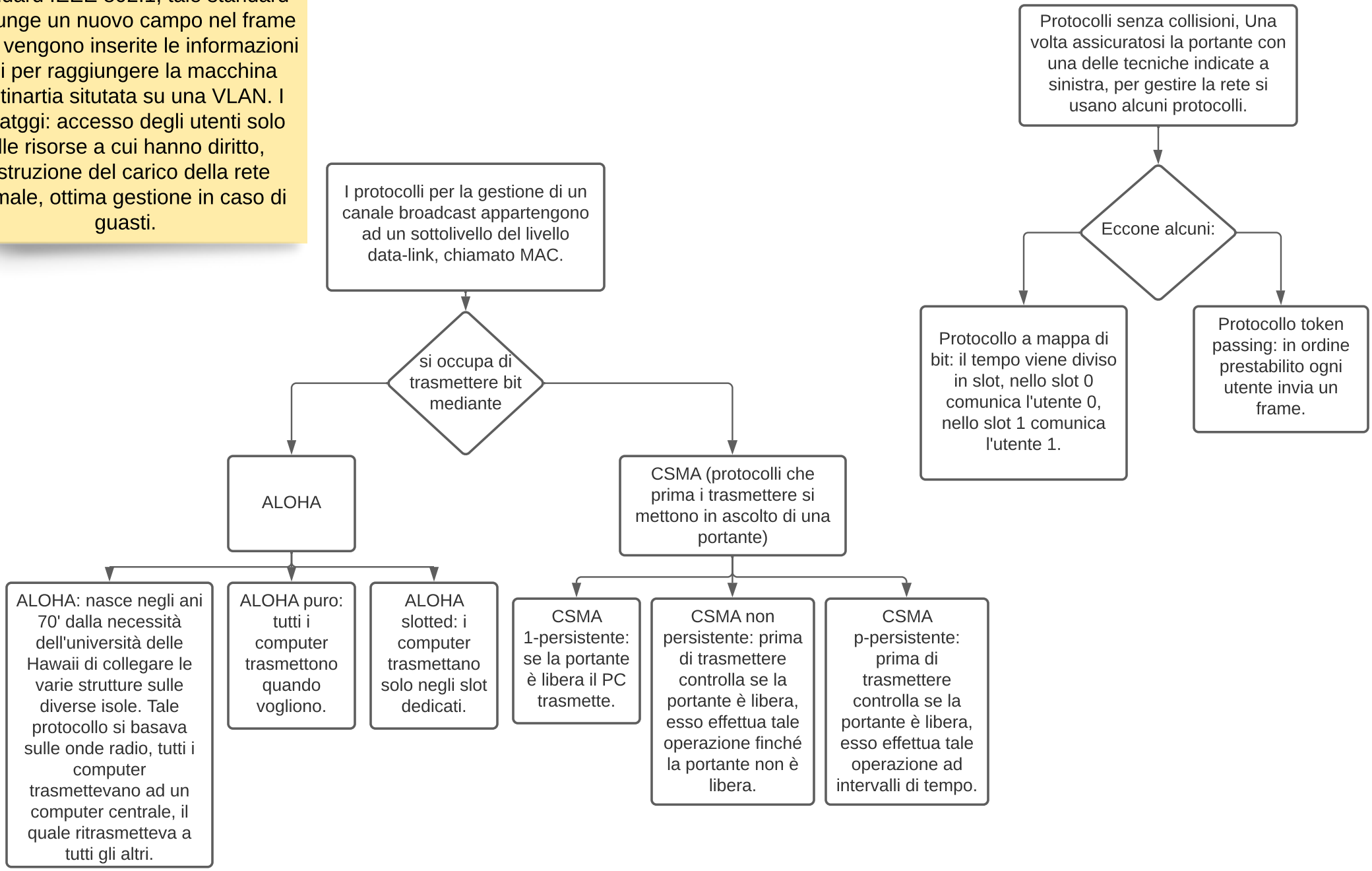
I frame a loro volta vengono divisi, mediante il framing, per individuare i frame appertenenti allo stesso frame si usa:

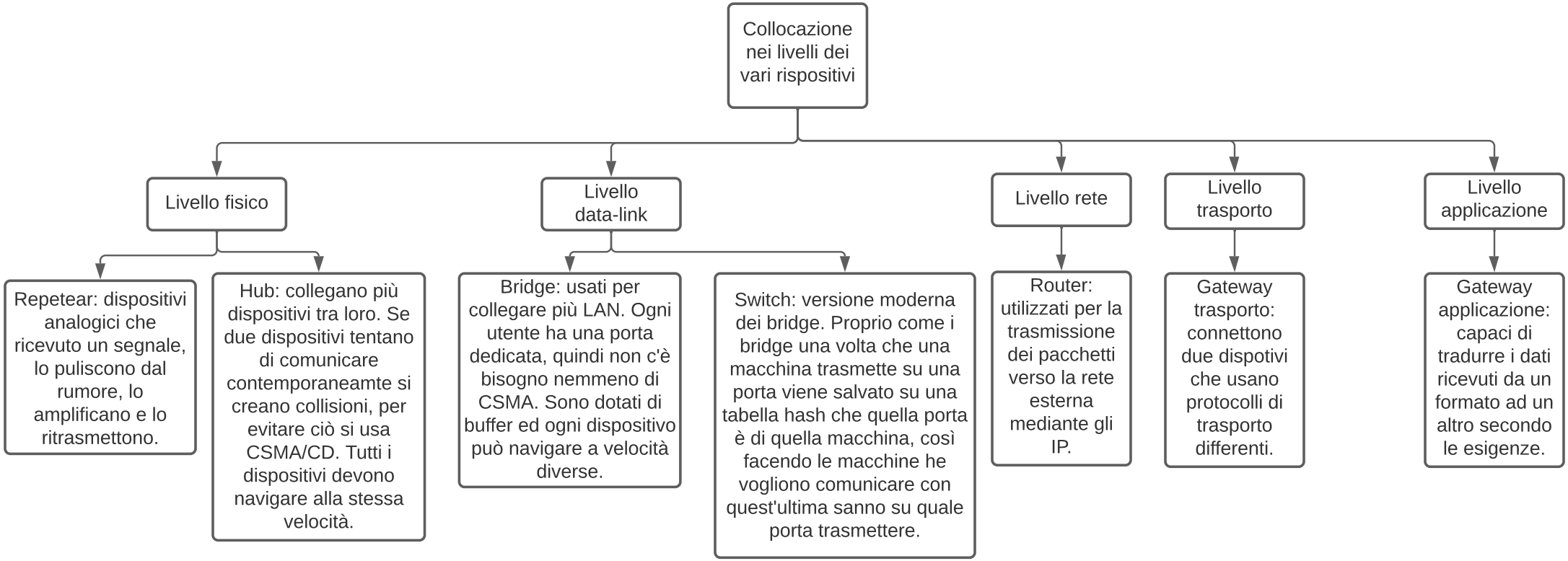
Conteggio dei byte: si inserisce nell'header del frame il numero di byte di cui è composto il frame.

Flag byte con byte stuffing: si inserisce un crattere speciale all'inizio e alla fine del frame, in modo da identificare i diversi frame. Essendo che il carattere speciale può essere contenuto nel frame prime dell'invio del frame stesso si invia un byte stuffing.

LIVELLO DATA-LINK (MAC)

Virtual LAN: esse nascono dall'esigenza di configurare n LAN virtual piuttosto che n LAN fisiche. La loro struttura è identificata nello standard IEEE 802.1, tale standard aggiunge un nuovo campo nel frame dove vengono inserite le informazioni utili per raggiungere la macchina destinartia situtata su una VLAN. I vanatggi: accesso degli utenti solo alle risorse a cui hanno diritto, distruzione del carico della rete ottimale, ottima gestione in caso di guasti.




Collocazione nei livelli dei vari rispositivi
Livello fisico
Repetear: dispositivi analogici che ricevuto un segnale, lo puliscono dal rumore, lo amplificano e lo ritrasmettono.
Hub: collegano più dispositivi tra loro. Se due dispositivi tentano di comunicare contemporaneamte si creano collisioni, per evitare ciò si usa CSMA/CD. Tutti i dispositivi devono navigare alla stessa velocità.
Livello data-link
Bridge: usati per collegare più LAN. Ogni utente ha una porta dedicata, quindi non c'è bisogno nemmeno di CSMA. Sono dotati di buffer ed ogni dispositivo può navigare a velocità diverse.
Switch: versione moderna dei bridge. Proprio come i bridge una volta che una macchina trasmette su una porta viene salvato su una tabella hash che quella porta è di quella macchina, così facendo le macchine he vogliono comunicare con quest'ultima sanno su quale porta trasmettere.
Livello rete
Router: utilizzati per la trasmissione dei pacchetti verso la rete esterna mediante gli IP.
Livello trasporto
Gateway trasporto: connettono due dispotivi che usano protocolli di trasporto differenti.
Livello applicazione
Gateway applicazione: capaci di tradurre i dati ricevuti da un formato ad un altro secondo le esigenze.

LIVELLO RETE 1

Livello rete si occupa del trasporto dei pacchetti. Il suo scopo è: data la topologia di rete trovare il percorso migliore.

Per fare ciò usa diversi algoritmi:

- Algoritmo di cammino minimo: definisce come percorso migliore il percorso che prevede meno salti, quindi l'attraversamento di meno host. Non sempre è il migliore poiché un percorso seppure prevede meno salti gli host possono trovarsi a distanze maggiori l'uno dall'altro.
- Flooding: tale algoritmo effettua scelte in base alle conoscenze locale. Per ottenere tali conoscenze ogni router della rete invia un frame su tutte le linee di uscita. Tale tecnica genera però una grande quantità di traffico, per evitare ciò usa due strategie: nel'header di ogni frame c'è un counter, ad ogni salto diminuisce, arrivato a 0 o ha raggiunto la destinazione o viene cestinato, la seconda consiste nell'inserire nell'header tutti i router che il pacchetto ha attraversato, per evitare doppi passaggi.
  - Algoritmo di routing basato sul vettore delle distanze: ogni router conserva una tabella contenente il percorso migliore per raggiunger ogni router.
  - Algoritmo di routing basato sullo stato dei collegamenti: ogni router invia un frame ai router adiacenti per cercare informazioni, comunica tali informazioni ai router adiacenti, così facendo si creano tabelle mediante la condivisione delle informazioni.
- Algoritmo gerarchico: in caso di reti di grandi dimensioni, quest'ultime vengono divise in regioni, all'interno di ogni regione tutti i router conoscono le informazioni degli altri router della regione, ma solo un router sa come raggiungere i router delle altre regioni.

Unicast: trasmette ad un solo host
Broadcast: trasmetti a tutti gli host
Multicast: trasmette ad un gruppo
Anycast: trasmette all'host più vicino

La congestione avviene quando ci sono troppi pacchetti nella rete o quando il ricevitore non riesce ad elaborare la quantità di dati inviata dal trasmettitore. Quando essa si verifica si può intervenire facendo: distribuendo in maniera omogenea il traffico sulla rete, quando la rete è vicina alla congestione non si accettano nuovi collegamenti, quando si sta per verificare una congestione si avvisano gli utenti. Qualora le tecniche precedenti non bastano la rete elimina direttamente il carico, scartando alcuni pacchetti.

LIVELLO RETE 2

La connessione tra reti diverse (LAN, PAN, WAN) si chiama internet. Essa è possibile mediante un protocollo chiamato IP.

Tale connessione si divide per:

- Connessioni che usano lo stesso protocollo: quando due reti usano lo stesso protocollo (IPv4) ma sono collegate da reti che usano un protocollo diverso (IPv6) tale problema viene risolto mediante il tunnelling.
- Connessioni che usano protocolli diversi: diversa è la soluzione se non ci conosce nulla delle deu reti e magari usano algoritmi di routing diversi e magari hanno ISP diversi. In questo caso il tutto si risolve mediante l'introduzioni dell'algoritmo di routing a due livelli:
  - Protocollo di routing intradominio: trova il percorso migliore all'interno della rete. Ogni rete può usare l'algoritmo che vuole. Un esempio è l'algoritmo OSPF, ha caratteristiche come essere di dominio pubblico, capace di calcolare distanze fisic, ritardo dei pacchetti, capace di adattarsi al traffico e supporta supporti gerachici, come internet che è in continua evoluzione.
  - Protocollo di routing interdominio: comunemente chiamato BGP, trova il percorso migliore per collegare le due reti. Esso è standard e garantisce diverse convenzioni come: mai porre l'Iraq su un percorso che inizia dal Pentagono, mai dirottare il traffico di Apple su server di Google e molte altre.

IPv4, usa indirizzi di rete da 32 bit. Il suo header è composto da 20 byte e da 13 campi, più campi opzionali. I campi contengono informazioni riguardo il tipo la versione (IPv4), il tipo di protocollo usato (TCP, UDP), quanto è grande l'header, quando è grande l'intero indirizzo, checksum, indirizzo mittente e indirizzo destinatario. Esso è in formato big endian.

IPv6, usa indirizzi di rete da 128 bit. Il suo header è composto da 8 byte e da 7 campi, più campi opzionali che in IPv4 erano obbligatori.

128.208.96.0/19 indica che 19 bit dei 32 sono dedicati alla rete e 13 agli host. Quindi tale indirizzo può ospitare 2 alla 13 host (8192).

Per sopperire alla mancanza di IP si possono usare 3 soluzioni: usare IPv6, usare IP dinamici quindi quando una macchina smette di usarlo viene assegnato ad un'altra, usare il NAT, esso prevede l'uso di IP privati, quindi n computer usano un solo indirizzo pubblico (IP) per comunciare con la rete. Per sapere a quale indirizzo privato va ciascun informazione si usano le porte.

LIVELLO TRASPORTO

Il livello di trasporto si occupa di creare protocolli capaci di trasportare dati indipendentemente dalla tipologia di rete su cui opera.

Per fare ciò usa due tipi di protocolli:

UDP (user datagram protocol), protocollo non orientato alle connessioni, difatti invia dati tra due pc senza effettuare una connessione tra di loro, ciò implica di non sapere se il dato è arrivato o meno. L'header dei datagrammi è formato da 8 byte e contiene: porta sorgente, porta destinatario, lunghezza del datagramma ed eventualmente il checksum.

Remote Procedure Call, gestisce l'invio e l'attesa di una risposta in una rete proprio come la chiamata a procedura, dove richiamata una procedura si aspetta il risultato. L'esempio più noto dell'applicazione di questa tecnica è il DNS.

TRP (Real Time Transport Protocol) prevede l'impiego di UDP in ambiti di trasporto real-time dei dati, come le chiamate, videochiamate o streaming video. Esso si basa su due fasi: la prima riguarda l'invio di datagrammi UDP, la seconda la sincronizzazione di quest'ultimi dato che UDP non lo prevede.

TCP (tranfer control protocol), protocollo orientato alle connessioni, difatti prima di trasferire dati tra due PC deve prima stabilire una connessione. L'header è composto da 20 byte e contiene:porta sorgente, porta destinatario, numero di sequenza (nel caso stia inviando un informazione formata da più frame), ack, checksum e molti altri campi.

La connessione avviene mediante il metodo tree-way-handashake.

Dispone di numerosi timer, come l'RTO (retrasmission timeout) allo scadere di questo timer se l'ack non è arrivato il mittente ritrasmette.

TCP gestisce la congestione usando una tecnica chiamata finestra di congestione, la cui dimensione è data dal numero di pacchetti che la rete può gestire contemporaneamente. Un algortimo per la gestione è Slow Start, il quale unisce la tecnica di ack lock alla tecnica secondo cui la finestra di congestione è inizialmente impostata a 1, se riceve correttamente l'ack inviarà due pacchetti, se riceve corettamente gli ack invierà quattro pacchetti e così via in maniera esponenziale.

Ack lock: se il trasmittente è su una linea veloce ed il ricevitore su una linea lenta il tutto si risolve mediante un temporizzatore. Tale strumento misurerà il tempo che il ricevitore impiega per ricevere ed elaborare i dati e farà inviare al miettente i dati a quella velocità.

LIVELLO APPLICAZIONE

DNS (domain name system): tale sistema nasce come rimpiazzo al file host.txt, il quale ai tempi di arpanet veniva aggiormato ogni notte e conteneva per ogni host il relativo IP. DNS nasce nell'83 ed il suo funzionamento si base su l'invocazione di una procedura chiamata resolver, la quale ricevuto come parametro il nome dell'host lo invia mediante un pacchetto UDP al server DNS locale, il trovato l'IP assocciato lo restuisce al resolver.

La risoluzione da parte del DNS avviene mediante una serie di interrogazioni ricorsive, diafatti spesso accade che prima di trovare la risoluzione finale vengano interrogati più server DNS, alla fine ognuno dei server interrogati salverà nella sua cache la sua parte di risoluzione per future interrogazioni.

I domini vengono assegnati da ICANN, un ente no profit.

All'interno dei server DNS i domini sono rappresentati da record, che contengono:

- Nome del dominio
- Il tempo in cui quest'informazione resta valida, per enti sicuri, come quelli governativi durano 24 ore.
- Il tipo, se è IPv4, IPv6
- Il valore, se è IPv4 indica che è composto da 32 bit

I protocolli e-mail in origine erano semplici file di testo con la differenza che la prima riga conteneva l'indizzo del destinatario.

Oggi l'archietettura del sistema mail è cambiata, ma resta comunque semplice. A monte ci sono due user agent rappresentati generalmente da app che consentono all'utente di scrivere e leggere le mail. Gli user agent inviano le mail ad i server chiamati message transfer agent i quali usando il protocollo SMTP (simple mail transfer protocol) comunicano tra di loro.

L'invio finale avviene mediante il protocollo IMAP (internet message access protocol) il quale mette un server in ascolto sulla porta 143 generando una connessione sicura mediante il login sul server.

SERVER

SOCKET: la creazione del socket avviene mediante la creazione della funzione socket, essa crea un descrittore. Tale operazione serve per allocra opportune strutture nel kernel. Essa ha 3 parametri: famiglia (in cui vengono specificate la famiglia di indirizzi che verranno usati-AF_INET), il tipo (SOCK_STREAM o SOCK_DGRAN) ed il terzo è il protocollo usato per implementazioni future.

BIND: Il sistema operativo assegna IP e porta al server. Tale operazione non si effettua nella socket automaticamente poiché alcuni servizi preferiscono decidere autonomamente IP e porta.

LISTEN: pone il socket in ascolto, quindi in attesa di connessioni.

ACCEPT: Una volta completato il tree way hadshake la funzioe accept gestisce la nuova connessione, spostandola dal socket principale che resta in ascolto ad un altro che gestirà la connessione.

READ

WRITE

CLOSE

un descrittore di file è un numero intero non negativo che rappresenta un socket aperto da un processore sul quale il processo può effettuare operazioni di input/output

UDP nel client non c'è la CONNECT e nel server non ci sono la BIND, la LISTEN e la ACCEPT poiché è un protocollo non orientato alle connessione e non le effettua. invece di READ e WRITE usa SENDTO e RECVFROM, entrambe hanno i primi 3 parametri uguali alla READ e alla WRITE ma hanno ulteriori 3 parametri, uno a 0 e gli altri due voglio la sockaddr e la sua dimensione.

SOCKET

CONNECT: funzione che stabilisce la connessione con il server. Essa avvia il tree way handshake.

WRITE

READ

CLOSE

N.B. Tutte le funzioni in caso di esito positivo restituiscono un numero positivo altrimenti negativo.