# Ripasso Reti di calcolatori

*Ogni risposta deve contenere: spiegazione (cos'è e dove viene usata), pregi, difetti.*

Nelle risposte, si cerchi di essere il più possibile completi, ma in maniera attinente alla domanda. Le sue valutazioni, comunque, sono abbastanza altalenanti e dipende da come gli gira. Si scrivano cose sensate solo nel contesto d'uso.

Con ⊙ sono indicati gli argomenti visti superficialmente nel A.A. 2025-26, con ⊠ le domande non presenti in esami precedenti.

Nota bene personale: latenza di trasmissione è un termine abbastanza generico, RTT (Round Trip Time) o RTD (Round Trip Delay) è un termine più rigoroso per definire il tempo che un pacchetto percorre nell'etere / mezzo di trasmissione prima di arrivare al ricevente.

# *Livello 1: strato fisico*

## Codifica Manchester

Si tratta di una codifica dei bit dove un simbolo è rappresentato da un cambio di voltaggio da alto a basso o da basso a alto (che rappresentano rispettivamente 0 e 1). Un segnale si codifica eseguendo uno XOR tra il flusso dati e un clock con frequenza doppia. Un suo pregio è che il segnale può essere decodificato senza previa sincronizzazione. Ha un data rate però relativamente basso: la metà del baud-rate massimo e non si può spingere a frequenze molto alte senza incorrere in problemi non triviali.[1] Viene usato nel DSL e nello standard Ethernet poiché molto economico visto che non necessita di precisi e costosi circuiti di clock.

## ⊙ Modulazione di fase

- https://en.wikipedia.org/wiki/Phase_modulation
- https://it.wikiversity.org/wiki/Modulazioni_analogiche#Modulazione_di_fase
- + en pg 130

È una modulazione che codifica un simbolo come variazioni nella fase di una o più frequenze. Permette un maggiore bit rate a parità di baud-rate ed è la base per modulazioni più complesse e performanti come il QAM, che usa contemporaneamente la modulazione di fase e di ampiezza per aumentare il numero di baud trasmissibili in una certa banda.

## CDMA

Il Code Division Multiple Access è un metodo di multiplexing che permette a più dispositivi di trasmettere sulla stessa frequenza senza causare collisioni. Ad ogni dispositivo viene assegnata una *chip sequence* formata da una serie di 0 e 1 che rappresenta il simbolo 1 associato a quel specifico mittente. Grazie al metodo di Walsh ogni sequenza, rappresentabile come vettore, è ortogonale ad ogni altra sequenza.

Grazie a questa proprietà eseguendo la somma normalizzata tra il segnale ricevuto, ovvero la somma delle chip sequence di ogni dispositivo che ha trasmesso, e la chip sequence di un particolare mittente è possibile ottenere la word originale inviata dal mittente.

Questo metodo ha una efficienza spettrale molto alta, e per questo viene utilizzato negli standard Wi-Fi, nel 2G e in certe varianti del 3G, ma richiede che ogni dispositivo invii il proprio messaggio alla stessa potenza per poter effettuare il demultiplexing. Questo prerequisito richiede che ogni antenna trasmetta ad una potenza nota al mittente, in modo che possa regolare la potenza di trasmissione conseguentemente.

## ⊙ QPSK

La Quadrature Phase Shift Keying è una tecnica di trasmissione dati basata sulla modulazione di fase di due frequenza in 4 punti equidistanti a coppie. Rispetto alla modulazione di fase di una singola frequenza ha un baudrate doppio. Per renderlo più resiliente alla distorsione e al rumore l'encoding viene effettuato con il codice di Gray[2] (ovvero ogni simbolo consecutivo differisce di un solo bit da quello precedente[3]). A differenza del QAM usa solo la modulazione di fase e non anche quella di ampiezza.

---

[1] https://en.wikipedia.org/wiki/Manchester_code
[2] https://en.wikipedia.org/wiki/Phase-shift_keying
[3] https://en.wikipedia.org/wiki/Gray_code

## QAM

Info utili su quora e techdifferences.

La Quadrature Amplitude Modulation è una tecnica di trasmissione che usa contemporaneamente la modulazione di fase e di frequenza su due frequenze dette portanti, solitamente rappresentate dalle lettere Q e I. Aumentando il numero di modulazioni possibili posso aumentare il data-rate mantenendo costante il baudrate. L'alfabeto dei simboli può essere rappresentato in un grafo a costellazione, ovvero un grafo cartesiano dove i due assi rappresentano le due onde Q e I e la loro ampiezza. Ogni punto sul grafo rappresenta l'intersezione tra due ampiezze di Q e I, ovvero un possibile simbolo.

Per la sua alta efficienza spettrale viene usato nella comunicazione satellitare e in vari standard Wi-Fi definiti nel IEEE 802.11.

4-QAM e QPSK sono due metodi leggermente diversi che ottengono lo stesso risultato, usano la stessa decodifica ma una codifica leggermente diversa[4] (i simboli sono spaziati diversamente sul grafo della costellazione).

## I satelliti

Un satellite per telecomunicazioni è un satellite artificiale orbitante attorno alla terra usato per le comunicazioni terrestri. In base alla loro altitudine si suddividono in geostazionari, MEO e LEO.

I satelliti geostazionari orbitano a 35800m dalla terra, distanza che gli permette di avere la stessa velocità della terra ed essere quindi essere stazionari. Per minimizzare le collisioni e le interferenze radio si è limitato il numero di satelliti GEO a 180. Per la loro altitudine sono i satelliti con la maggiore latenza di trasmissione, attorno ai 270ms, e quelli con la maggiore copertura terrestre: con 3 satelliti è possibile coprire l'intero pianeta Terra. Sono utilizzati per il broadcasting televisivo (per esempio Sky Television).

A differenza dei satelliti MEO e LEO la qualità del segnale degrada molto all'avvicinarsi dei poli terrestri. Sono i satelliti più longevi ma allo stesso tempo i più costosi da lanciare per il loro peso e la necessità di attraversare entrambe le fasce di Van Hallen. Per la loro distanza la comunicazione con essi richiede ricevitori molto voluminosi e potenti, poco adatti alla mobilità.

I satelliti MEO sono invece posizionati tra le due fasce di Van Hallen e sono principalmente usati per la navigazione terrestre, come il GPS americano o il sistema Galileo europeo. Poiché non sono stazionari è necessario che il ricevente segua il transponder del satellite in cielo. Richiedono dei transponder più piccoli ed efficienti grazie alla loro altitudine minore, inoltre il lancio di un satellite MEO è più accessibile data la minore distanza e la necessità di attraversare solo una delle due fasce di Van Hallen. Questa orbita è la più popolata e quindi la più pericolosa per la presenza di altri satelliti e di detriti spaziali.

I satelliti LEO (Low-Earth Orbit) sono i satelliti più vicini alla terra, con una latenza massima di soli 7ms. Sono inoltre i satelliti che offrono maggiore banda tra i tre tipi. Questa vicinanza comporta un minimo di 50 satelliti per avere una copertura globale, contro i 3 minimi di un sistema geostazionario o i 30 satelliti richiesti da una costellazione MEO.

[4] mathworks.com

Richiedono le antenne più piccole ed efficienti tra i tre tipi, motivo per cui certi smartphone odierni supportano la comunicazione con costellazioni LEO. Sono inoltre i più economici da lanciare ma anche i meno duraturi dei tre. Alcune reti LEO commerciali sono Iridium e Starlink, che effettuano lo switching tra satelliti e Globalstar, che invece usa i satelliti in modalità bent-pipe ed effettua lo switching a terra.

Rispetto alla fibra la rete satellitare non è usata da molti privati, ma è estremamente efficiente per ogni tipo di broadcasting (basti pensare che un singolo satellite esegue il broadcasting di Sky per gran parte dell'Europa), è immune ad ogni tipo di catastrofe naturale o artificiale (e quindi molto gettonato nelle emergenze o nelle guerre) e ha prezzi molto più accessibili della fibra in aree poco densamente popolate.

ITU = International Telecommunication Union, gestisce gli "slot" orbitali[5]

## ADSL

La Asymmetric Digital Subscriber Line è uno standard per la trasmissione dati digitale e analogica, nata come evoluzione necessaria del DSL per portare velocità maggiore ai privati, sempre più propensi a navigare in Internet. È retrocompatibile con lo standard DSL. Utilizza frequenze fino ai 2.2 MHz suddivise in canali da 4kHz ciascuno tramite una variante del FDM, il Discrete MultiTone. Ogni canale è trattato come una connessione indipendente, che può essere rallentata o velocizzata in base alla qualità del segnale. Il maggiore limite di questo standard è il suo medium, ovvero il cavo UTP3 che percorre l'ultimo miglio: la sua lunghezza è l'unico vero fattore che influisce sulla banda raggiungibile. È tecnicamente stato superato dal VDSL che utilizza frequenze fino ai 12 MHz, utilizzabili però soltanto se lo stesso cavo in che percorre l'ultimo miglio non è troppo lungo o degradato per il tempo, altrimenti il proprio datarate degrada fino a raggiungere le performance della ADSL. Ci furono più evoluzioni di ADSL, la più performante è ADSL2+ Annex M che offre fino a 27 Mbps in download e 3.3 Mbs in upload.

## Modulazione Delta / compressione delta

Si tratta di un metodo di compressione lossy per rappresentare dei dati analogici digitalmente. Fu usata nel 2G sia per il GSM europeo che il D-AMPS americano per poter gestire più chiamate su un singolo canale 1G tramite TDM (Time Division Multiplexing). Ogni sample della voce viene rappresentato come differenza approssimata dal sample precedente.[6] Permette quindi una maggiore efficienza spettrale a costo di una qualità audio percettibilmente inferiore.

N.B. da non confondersi con il delta encoding, che è un'altra cosa ancora (principio simile ai backup differenziali).

## ⊙ Handoff

Nella telefonia ci sono due tipi di handoff:

- hard handoff: che veniva usato nel 1G, dove ogni antenna interrompeva la connessione con ogni dispositivi che riceveva al di sotto di una certa potenza;

[5] www.itu.int

[6] https://en.wikipedia.org/wiki/Delta_modulation

- MAHO (Mobile Assisted HandOff): ogni telefono misura la potenza del segnale dell'antenna a cui è collegato durante le pause attive del TDM e decide automaticamente quando e come passare ad un'altra cella. Viene usato dal 2G in poi.

# *Livello 2: data-link*

## Bit e Byte stuffing

Sono due metodi per rappresentare l'inizio e la fine di un frame nel data link tramite un byte speciale detto flag byte. Nel caso il payload del pacchetto contenga lo stesso byte i due metodi usano soluzioni diverse: il byte stuffing aggiunge uno o più byte speciali detti *di escaping* che segnalano al destinatario di interpretare come parte del payload il byte successivo, mentre nel bit stuffing viene aggiunto un bit ogni volta che viene rilevata una sequenza di bit simile a quella del flag byte. Il bit stuffing è occupa molto meno spazio ma è più lento da eseguire del byte stuffing poiché i moderni calcolatori sono ottimizzati per operare una word alla volta, invece che eseguire operazioni bit per bit. Nessuno dei due metodi ha controlli di integrità. [Pg 199 en]

## ⍟ I protocolli sliding window

Si tratta di una famiglia di protocolli dove mittente e destinatario permettono di ricevere solo una specifica parte di una sequenza di pacchetti detta finestra. Ogni pacchetto al di fuori di questa finestra viene scartato. La finestra viene fatta "avanzare" di uno quando riceve il pacchetto con il numero di sequenza corrispondente al limite inferiore della finestra, permettendo al mittente di inviare una parte successiva del messaggio e così via. Poiché i pacchetti possono arrivare disordinati il destinatario ha un buffer delle stesse dimensioni della finestra. Alcuni esempi di protocollo sono il *go-back-n* e le *sliding windows*. Viene utilizzato nel protocollo TCP e in vari protocolli a livello data-link.

## Go-back-N

La go-back-n è una tecnica di gestione degli errori usata nei protocolli sliding windows quando è presente una banda e una latenza di trasmissione molto alta. Quando viene rilevato un errore in un pacchetto della sequenza il ricevente scarta in automatico tutti i pacchetti successivi e invia in cumulative acknowledgment per tutti i pacchetti precedenti. Il mittente dovrà quindi rinviare tutti i pacchetti scartati, processo molto costoso nel caso il canale sia molto disturbato. Per rimediare a questo difetto è stato creato il protocollo selective repeat, che permette di rinviare meno pacchetti a costo di un uso di memoria maggiore.

## Selective repeat

Il selective repeat è una tecnica di gestione degli errori usata nei protocolli sliding windows quando è presente un canale molto disturbato e quindi la tecnica del go-back-n risulterebbe inefficiente. Nel caso venga rilevato un errore in uno dei pacchetti questo è l'unico per cui non viene mandato un ACK al mittente, che dopo un timeout ritrasmetterà il pacchetto corrotto. Per questioni di efficienza gli ACK sono cumulativi: ovvero il mittente invia un acknowledgment se e solo se tutti i pacchetti precedenti sono stati ricevuti. Una versione leggermente più efficiente invia al mittente dei NAK (Negative ACK) per ridurre il tempo prima che questo ritrasmetta il pacchetto corrotto. È però efficiente solo se la latenza di trasmissione è bassa.

# *Suddivisione di un canale*

## Aloha 🏝️

È un protocollo a contesa limitata, ovvero dove ogni stazione compete per un canale condiviso dove possono esserci collisioni. Ogni stazione tenta di inviare il proprio pacchetto ad una stazione centrale, che periodicamente fa il broadcast di tutti i pacchetti ricevuti. In questo periodo ogni stazione ascolta e rinvia il pacchetto dopo un periodo di attesa casuale. Non è molto efficiente in quanto la banda netta è solamente il 18% della banda totale, ma fu il primo protocollo ad essere infinitamente scalabile per ogni numero di stazioni. Viene utilizzato in contesti con molti utenti non sincronizzati con un traffico dati scarso e dove la latenza non è problematica.

Una sua evoluzione, lo slotted Aloha, suddivide in intervalli lunghi un frame il canale per ridurre le collisioni e quindi aumentare l'efficienza, portandola al 37%. Per la sincronizzazione l'antenna centrale invia un segnale di clock per segnare gli intervalli. Un difetto dei metodi Aloha è che il numero di collisioni aumenta esponenzialmente alla frequenza di tentativi di invio di un pacchetto. Per correggere questo difetto sono nati protocolli più moderni a contesa limitata, dove si limita il quanti utenti e quanti tentativi di invio possono essere fatti in un certo periodo di tempo.

## CSMA

Il CSMA (Carrier Sense Multiple Access) è una evoluzione di Aloha in cui si introduce il Carrier Sense: il trasmittente è quindi capace di rilevare se il canale è già occupato e aspetta fino alla fine della trasmissione per trasmettere. In caso di normale collisione si comporta come Aloha puro. Con questa miglioria si ottiene una efficienza del 50% ma non si è esenti da problemi: se le stazioni sono distanti e il tempo di propagazione tra una stazione ed altra è alto è possibile che più stazioni inizino a trasmettere nella frazione di tempo in cui il canale è libero e la trasmissione dell'altra stazione non li ha ancora raggiunti. Per evitare il primo di dei due problemi è nato il p-Persistent CSMA, che si comporta come il CSMA ma ha una probabilità $p$ di trasmettere un pacchetto quando il canale si libera. Funziona molto bene nella teoria con $p$ estremamente bassi, che però comportano una enorme latenza in una rete poco trafficata.

## CSMA non persistent

È una variante del CSMA dove invece di aspettare la liberazione del canale il trasmittente aspetta un periodo casuale prima di riprovare a trasmettere. Rispetto al p-Persistent CSMA, che trasmette con una probabilità appena il canale si libera, ha una efficienza del 90% e gestisce meglio delle altre varianti del CSMA trasmissioni con diverse quantità di traffico.

## Walking tree protocol

Si tratta di un protocollo a contesa limitata dove si minimizzano le possibili collisioni limitando il numero di stazioni che possono trasmettere. In caso di collisione si usa una ricerca binaria, dove ogni stazione è rappresentata come una foglia in un albero binario, mentre tutti gli altri nodi rappresentano i gruppi di appartenenza di una certa foglia. In caso di collisione si limita il numero di stazioni che possono trasmettere scendendo l'albero binario finché non ci sono collisioni. A differenza di altri metodi come Aloha, CSMA e le

loro varianti e Basic Bitmap ha delle ottime performance indipendentemente da quanto sia congestionata la rete.

Per questo motivo e il fatto che sia un protocollo per reti locali e non globali (ovvero non viene usato per gestire una serie di antenne, e le loro connessioni, ma solo quella di una singola antenna) viene utilizzata nella telefonia mobile, dove la topologia e la congestione della rete cambiano molto e velocemente.

## Problema della stazione nascosta

È un problema presente nella comunicazione wireless: quando due stazioni che sono troppo distanti per essere a conoscenza dell'altro ma abbastanza vicine da avere un ricevitore in comune possono causare collisioni cercando di trasmettere alla stazione comune. Una delle prime soluzioni fu il protocollo MACA (Multiple Access Collision Avoidance), che permette a un mittente di coordinare con il ricevitore l'invio di un pacchetto tramite due primitive: un pacchetto RTS (Request-To-Send) dove il mittente chiede il permesso di trasmettere, mentre con il pacchetto CTS (Clear-To-Send) il ricevitore conferma che è pronto a ricevere la trasmissione. Non è però un protocollo perfetto: ci possono comunque essere collisioni sulle richieste RTS, in tal caso i mittenti attendono un periodo casuale prima di ritentare la trasmissione.

# *Livello 3: la rete*

## Flooding

È un protocollo di routing che si basa sul semplicemente inviare ogni pacchetto ricevuto in broadcasting. È molto semplice ma crea molto traffico inutile se gran parte del traffico non è broadcast. In compenso è un protocollo molto veloce: poiché prova tutte le strade possibili per una destinazione di sicuro prenderà anche quella più veloce. È inoltre il metodo più robusto contro qualunque tipo di cambiamento di rete, motivo per il quale trova largo uso in applicazioni militari e parzialmente nel Link State Routing, il protocollo usato oggigiorno per la gestione del routing.

## Distance Vector Routing

È un protocollo di routing pensato come sostituto del flooding. Ogni router ha una routing table che contiene i costi necessari per arrivare ad ogni stazione che conosce. Per creare questa tabella ogni router chiede ai propri vicini di inviare la propria. In base alle tabelle ricevute e il tempo voluto a riceverle il router crea la propria tabella, che viene periodicamente ricalcolata per gestire eventuali cambiamenti nella rete. Questi aggiornamenti però non sono molto efficaci nel caso il costo di un router aumenti di colpo: poiché nelle tabelle ricevute non è possibile sapere se nel costo è incluso un hop in se stesso il costo di un router congestionato salirà molto lentamente ad ogni ricalcolo, non rappresentando fedelmente lo stato della rete. Questo problema è detto count to infinity.

## Link State Routing

È il successore del Distance Vector Routing ed è il protocollo usato oggigiorno per il routing. Ogni router esegue i seguenti passaggi:

- rileva i router vicini tramite pacchetti HELLO e la loro distanza tramite la latenza alla risposta di pacchetti ECHO;
- sulla base di queste informazioni crea un pacchetto speciale contenente la lista di router a cui il mittente è collegato detto LSP (Link State Packet) di cui esegue il flooding;
- ogni router grazie a queste informazioni può aggiornare la propria routing table, il proprio LSP e la propria mappa della rete. Quest'ultima parte non era possibile con il DVR, che scambiava solo informazioni locali riguardo ai costi per raggiungere un router.

Ogni router quindi riceve informazioni globali e trasmette informazioni locali sullo stato della rete, rendendo il LSR più robusto del DVR in caso di cambiamenti negativi nella rete. Poiché questo flooding è periodico viene usata più banda rispetto al DVR, ma non è presente il problema del count to infinity. Poiché ogni router ha una mappa più completa della rete, si possono utilizzare algoritmi migliori per il calcolo dei percorsi, che richiedono però un hardware più potente.

## Quality of Service

Sono una serie di parametri che definiscono la qualità del servizio internet offerto. I 4 parametri principali sono (1) affidabilità, (2) banda, (3) latenza e (4) jitter, ovvero la deviazione standard della latenza in un periodo breve di tempo. Diversi servizi hanno soglie di accettabile diverse per questi 4 parametri: per il gaming jitter e latenza sono fondamentali, mentre il trasferimento di file priorizza banda e affidabilità. Il fattore non fisico che impatta di più questi parametri è la congestione della rete, motivo per il quale esistono diversi

algoritmi per regolare il traffico di dati, come il choke packet o metodi più avanzati come i leaky buckets o i token buckets.

## Choke packet

È il metodo più semplice per gestire la congestione: quando un destinatario sta per essere saturato invia un pacchetto speciale al mittente, il choke packet, che alla sua ricezione dimezza la banda. Per evitare che una serie di choke packets rallentino troppo un mittente questo alla prima ricezione avvia un timer, detto di fading, per il quale ignora i choke packets fino al suo esaurimento. Poiché questo metodo è lento nel caso il mittente sia un nodo molto distante è stata creata una sua variante, detta hop-by-hop choke, dove ogni nodo per il quale passa il pacchetto dimezza la sua banda.

## Leaky bucket

Il traffico di rete viene normalizzato tramite un buffer (il *bucket*) che limita il numero di pacchetti che possono passare per un host. Nel caso questo limite venga superato il buffer ha una riserva limitata e quando viene riempita i nuovi pacchetti vengono scartati. Questo metodo permette di ridurre il rischio di congestione causato dai burst, ovvero picchi improvvisi di traffico. Viene implementato lato mittente, permettendo quindi di non congestionare parti intermedie della rete, costringendole a scartare pacchetti. I leaky buckets normalizzano efficientemente ed efficacemente il traffico dati, risultano però inadatti a gestire traffico variabile con burst di dimensioni superiori al limite di banda, causando un rallentamento per lo scarto di pacchetti.

La scelta della capacità del secchio e del tasso di uscita richiede una buona comprensione delle caratteristiche della rete e delle applicazioni, complicando la configurazione ottimale.

## Token bucket

È un protocollo per la gestione della congestione nato come evoluzione del leaky buckets. L'interfaccia di rete del mittente genera regolarmente una serie di token, che permettono l'attraversamento di un pacchetto se consumanti. Se dopo un intervallo dei token sono avanzati, vengono accumulati per la successiva serie di pacchetti fino ad un certo limite massimo. A differenza del leaky bucket gestisce meglio i burst nel breve periodo, che vengono smistati più rapidamente grazie ai token accumulati durante il minor traffico precedente, senza però cambiare il traffico medio nel lungo periodo. Una configurazione ottimale è però più difficile da gestire rispetto ad un leaky bucket e i burst molto lunghi causano comunque un rallentamento della trasmissione, visto che i pacchetti devono aspettare la generazione di nuovi token e possono venire scartati nel mentre, causando rallentamenti come i leaky buckets. Poiché l'assegnazione dei token è arbitraria è possibile eseguire del QoS implementando specifici metodi di assegnazione.

## CIDR

Il CIDR (Classless InterDomain Routing) fu introdotto per usare in maniera più efficiente il numero limitato di range di IPv4 creato con il classful routing, rendendo possibile la creazione di reti con subnet mask di dimensioni arbitrare, non solo /8, /12 o /16 come precedentemente dettato dalle classi A/B/C. Nacque per necessità: nonostante il classful routing abbia messo a disposizione il numero giusti di classi per ogni tipo, gran parte dei clienti alla fine comprarono un indirizzo di classe B (un blocco di circa 65mila indirizzi IP), anche se successivi studi mostrarono che gran per gran parte di essi sarebbe stato più che sufficiente un indirizzo di classe C (un blocco di 255 indirizzi IP). Questo proto-

collo aumentò la dimensione delle tabelle di routing, in quanto ogni indirizzo non era più separabile in classi statiche. Per comprimere la dimensione di queste tabelle furono introdotte le *aggregate entries*: due record nella tabella se hanno lo stesso suffisso possono essere compresse in una se entrambi sono instradati sulla stessa linea. Il match non sarà più fatto sull'intero indirizzo IP, ma il suo suffisso. Poiché un indirizzo IP può comparire in più suffissi si cerca il suffisso uguale di lunghezza maggiore per instradare il pacchetto. È un sistema più lento e complicato del classful routing, ma fu necessario per adattare un protocollo pensato per interconnettere università o basi militari ad una rete globale. Viene usato in pressoché ogni rete Internet moderna.

## NAT

Il NAT (Network Address Translation) permette di effettuare il multiplexing di più indirizzi IP privati con un solo indirizzo pubblico. Internamente il router sostituisce l'indirizzo e la porta sorgente con i propri quando invia un pacchetto verso l'esterno e sostituisce porta e indirizzo IP del destinatario quando deve instradare un pacchetto dall'esterno verso la rete privata. La rete interna usa degli indirizzi riservati per questo scopo (per esempio 192.168.0.0/16 nelle reti domestiche). Nacque per necessità: con un numero sempre più stretto di indirizzi IPv4 disponibili fu necessario per permettere a un numero sempre maggiore di utenti di collegarsi a Internet[7].

Il NAT ha il difetto di rendere ogni connessione connection-oriented, anche se il protocollo IP è nato come protocollo connectionless, facendo perdere ad Internet parte della sua resilienza. È anche un single point of failure: gestendo l'associazione dei socket internamente, in caso di disservizio del NAT la rete interna ed esterna non hanno più modo di comunicare tra di loro.

Viene usato da ogni ISP, soprattutto per le connessioni di privati che non necessitano di un indirizzo IP statico. Come effetto collaterale nasconde gli indirizzi interni da possibili attaccanti esterni, oscurando l'organizzazione di una rete interna.

## ARP

L'ARP (Address Resolution Protocol) è un protocollo parte del IEEE 802.3 che si occupa della traduzione di indirizzi IP in indirizzi MAC. Quando una macchina connessa alla rete non conosce l'indirizzo MAC del destinatario invia un pacchetto speciale in broadcast a cui risponde solamente la macchina con l'indirizzo MAC specificato. Per rendere il protocollo più efficiente in ogni broadcast il mittente invia in piggyback la propria associazione MAC-IP, e ogni macchina ha una cache su cui memorizza le associazioni di cui è a conoscenza. Alla prima connessione di rete di una macchina questa invia in broadcast una ARP request per se stesso, in modo da far conoscere a tutti la propria associazione MAC-IP e per controllare la presenza di eventuali collisioni di IP, che si scoprono nel caso un host risponda. Viene usato in quasi ogni macchina connessa ad Internet[8], in quanto è un protocollo essenziale del secondo livello TCP/IP. Non avendo nessun tipo di autenticazione (come gran parte dei protocolli in TCP/IP) un utente malevolo può impersonarsi come un'altra macchina con un attacco detto ARP spoofing[9].

---

[7] Non proprio accurato: la causa furono le migliaia di persone che comprarono indirizzi di classe B quando gli bastavano quelli di classe C, ma non so come scrivere in maniera elegante che è colpa della stupidità delle persone.

[8] Computer Networks 5th edition, pag 468.

[9] https://en.wikipedia.org/wiki/ARP_spoofing

## ICMP[v4]

ICMP (Internet Control Message Protocol) è un protocollo di rete di livello 3 progettato per comunicare o richiedere informazioni di stato ad altri dispositivi IP, ad esempio può segnalare ad un mittente che il suo pacchetto è stato scartato dopo che il suo TTL è arrivato a zero tramite il messaggio *Time Exceeded*, oppure controllare se un dispositivo è disponibile tramite un *Echo Request* a cui il destinatario deve rispondere con un *Echo Reply* (ovvero il *ping*). Viene anche usato per il troubleshooting di una rete poiché è alla base di strumenti come *ping* e *traceroute*. La sua utilità è però limitata poiché è un protocollo *best effort*, quindi inaffidabile, ed è un ottimo vettore di attacco con tecniche come il ICMP flooding e il smurf attack[10]. Per questo certi dispositivi di rete scartano in automatico certi pacchetti ICMP, in particolare *Echo Request* ed *Echo Reply*.

## IPv4

IPv4 (Internet Protocol version 4) è il principale protocollo del livello 3 di Internet. Si occupa della segmentazione dei dati in pacchetti e del loro routing attraverso reti diverse. Per essere il più performante possibile non è né affidabile né connection-oriented, non offre error o flow control e ha un controllo di parità estremamente semplice e poco robusto: offre solo un checksum in modulo 2.

Ogni dispositivo e ogni rete sono identificato da 4 cifre da un byte ciascuno, ovvero l'indirizzo IP, e da una subnet mask che permette di calcolare l'inizio e la fine di una rete e il suo indirizzo di broadcast. Un pacchetto IP è formato da un header con 20 byte fissi e una sezione variabile e un payload di dimensione variabile, definita in uno dei fissi del header. Ogni header contiene l'indirizzo IP del mittente e del destinatario, un checksum e vari flag e campi per gestire dati frammentati in più pacchetti.

Inizialmente gli indirizzi IP erano organizzati in 3 classi con tre diverse subnet per rendere più veloce il routing di un pacchetto, ma a seguito dell'esaurimento degli indirizzi IPv4 fu necessario introdurre il NAT e il CIDR. Queste soluzioni hanno i loro difetti: il NAT per esempio è un single point of failure: nel caso il router abbia dei problemi ogni connessione che passava per il NAT andrà persa e il CIDR richiede tabelle di routing più grandi del classful routing, nonostante le aggregate entries diminuiscano gli "effetti collaterali" del CIDR. Per queste e altre ragioni IPv4 è stato parzialmente sostituito da IPv6, che risolve il problema di IPv4 usando indirizzi di 128 bit.

## ⊙ IPv6

Nato nel 1998, IPv6 fu creato con il preciso scopo di sostuire IPv4 i cui indirizzi IP iniziavano già a scarseggiare, nonostante l'uso di NAT e CIDR. Fu scelto tramite un bando con diversi prerequisiti, tra cui:

- risolvere a lungo termine il problema dell'esaurimento di indirizzi IPv4, anche usando una allocazione inefficiente (come è successo con IPv4);
- essere il più performante possibile;
- gestire meglio di IPv4 il QoS;
- gestire privacy e sicurezza meglio di IPv4;
- deve coesistere facilmente con IPv4.

[10] https://solidwp.com/blog/icmp-attacks-everything-you-need-to-know/#h-smurf-attack

A vincere il bando fu il protocollo SIPP (Simple IP Plus), poi rinominato IPv6. Per risolvere il problema dell'esaurimento degli indirizzi IP il protocollo utilizza indirizzi da 128 bit invece che 32, come IPv4. Per aumentare la velocità di elaborazione di un pacchetto

- sono stati ridotti il numero di campi nel header da 13 a 6
- l'header è di dimensione statica, eventualmente espandibile usando dei puntatori a dei header aggiuntivi opzionali;
- fu tolto il checksum del header, in quanto considerato inutilmente ridondante, visto che se ne occupano già altri livelli ed è particolarmente dispendioso da calcolare;
- per ridurre il numero di campi la frammentazione è stata tolta e la negoziazione della dimensione dei pacchetti è stata affidata agli host. Un pacchetto troppo grande viene scartato dal router che segnalerà al mittente la cosa tramite ICMPv6.

Il suo adottamento fu molto lento per permettere a ISP e aziende una transizione indolore. Questa scelta fu però la debolezza di IPv6, che ancora oggi non ha sostituito IPv4, nonostante siano stati esauriti tutti gli indirizzi IPv4 dal 2020[11].

[11] https://www.apnic.net/manage-ip/ipv4-exhaustion/

# *Livello 4: il trasporto*

## TCP

Il TCP (Transport Control Protocol) è il principale protocollo usato in Internet per gestire delle connessioni affidabili tra due host. Come UDP usa l'astrazione delle porte per permettere il multiplexing su un singolo indirizzo IP. Ogni connessione è gestita tramite le *sliding windows*, che vengono avanzate tramite il campo ACK nel header, che conferma la ricezione del i-esimo byte, anche in piggyback. In caso di fallimento di ricezione TCP usa il *go-back-n* di default, ma è possibile abilitare il *selective repeat* e i NAK. La frammentazione viene gestita tramite un numero di sequenza di 32b (come l'ACK) nel header.

A differenza di UDP il protocollo TCP è solamente single-cast e ogni connessione viene aperta e chiusa «dolcemente» con una serie di passaggi e cambiamenti di flag presenti nel header, passaggi che rendono il protocollo più lento di UDP ma affidabile.

## Handshaking TCP

L'iniziazione di una connessione TCP avviene in tre fasi sequenziali:

1. l'host `A` invia a `B` un pacchetto TCP con il flag `SYN` attivo e un valore casuale $x$ sul numero di sequenza;
2. `B` risponde inviando ad `A` un pacchetto con il flag `SYN` attivo, un `ACK` con valore $x + 1$ e ponendo un numero di sequenza casuale $y$ maggiore di $x$;
3. infine `A` risponde inviando un `ACK` con valore $x + 1$ e numero di sequenza $y + 1$.

## ⊙ UDP

Il UDP (User Datagram Protocol) è un protocollo di livello 4 pensato per essere il più performante possibile. Per questo motivo non è affidabile ma solamente best effort. Un header UDP è composto solamente da 4 campi:

1. porta del mittente
2. porta del destinatario
3. checksum opzionale
4. lunghezza totale del datagramma

Per queste sue caratteristiche viene utilizzato da applicazioni che necessitano della minore latenza di trasmissione possibile, come la risoluzione DNS e lo streaming audio e video. A differenza del più lento e *connection-oriented* protocollo TCP permette il multicast.

# ⊙ *Pillole di sicurezza*

## Attachi cyphertext only

È un metodo che cerca di diminuire la quantità di tentativi bruteforce da eseguire analizzando certe caratteristiche di una lingua come la frequenza di certe sillabe o lettere. Viene usato per decifrare messaggi crittografati con metodi semplici come la sostituzione monoalfabetica o il DES. Oggigiorno è usato assieme ad altri metodi più avanzati in quanto gli algoritmi di crittografia moderna non creano gli schemi ripetitivi alla base di questo tipo di attacco.

## Sostituzione monoalfabetica

La sostituzione monoalfabetica è una tecnica crittografica classica che consiste nella sostituzione di ogni lettera del testo in chiaro (plaintext) con un'altra lettera dell'alfabeto, secondo uno schema fisso determinato da una chiave segreta. Tale tecnica mira a rendere il testo non comprensibile a chi non conosce la chiave utilizzata per la cifratura. Oggigiorno non viene praticamente mai utilizzata poiché facilmente decifrabile con metodi come l'analisi di frequenza di certe lettere o sillabi.

## Cifrari a trasposizione

Sono dei cifrari che scambiano la posizione dei caratteri secondo uno schema predeterminato dalla chiave simmetrica di cifratura, senza cambiarne il valore come la sostituzione monoalfabetica. Il messaggio così crittografato è più difficile da decifrare in quanto lascia segni meno evidenti di ripetizioni. Sono semplici da implementare e possono essere molto veloci tramite dei semplici acceleratori hardware. Sono considerati obsoleti grazie alla potenza dei moderni calcolatori e dalla presenza di algoritmi più complessi e sicuri. Al giorno d'oggi vengono usati solo assieme ad altre tecniche di cifratura per aumentare l'entropia del messaggio crittografato (come viene ad esempio fatto dai block cypher).

## One time pad

È un cifrario che codifica il messaggio in chiaro eseguendo lo XOR tra il messaggio e la chiave. La parte della chiave usata sarà poi scartata per rendere impossibile qualunque tipo di crittoanalisi. È un metodo matematicamente perfetto che però richiede dei prerequisiti molto complessi da applicare in larga scala come:

- lo scambio sicuro di chiavi enormi, lunghe almeno quanto il messaggio,
- una chiave veramente casuale enorme, cosa poco scontata e difficile da ottenere.

Viene usato solamente in ambiti critici come lo scambio di messaggi tra governi e varie agenzie di intelligence, in quanto altri metodi di cifratura sono comunque ragionevolmente sicuri e hanno una creazione e scambio delle chiavi molto più semplice, come l'algoritmo AES.

## ⊠ Block cypher

Sono tecniche che trasformano un blocco di simboli/bit alla volta invece che un carattere alla volta usando ogni volta la stessa chiave. Per rendere l'analisi delle ricorrenze più difficili si usano più block cypher sullo stesso messaggio per aumentarne l'entropia. Le implementazioni più semplici che usano poche permutazioni sono considerate insicure, come per esempio l'obsoleto ECB. Alcuni esempi di block cypher sono gli algoritmi RSA,

AES e DES. Vengono usati nella quasi totalità delle comunicazioni cifrate poiché è facile generare casualmente le chiavi richieste da questi algoritmi, a differenza dei one time pad.

## DES e triplo DES

Il DES è un block cypher che permuta blocchi da 128 bit in 16 iterazioni composte da scambi e sostituzioni definite da una chiave anch'essa da 128 bit. Fu creato dalla IBM e poi standardizzato dalla NSA con chiavi ridotte a 56 bit e blocchi da 64 bit. Fu adottato nel 1977 e fu sostituito prima dal triplo-DES e infine dal più moderno e sicuro AES nel 2002[12]. La transizione fu necessaria grazie al continuo miglioramento del hardware consumer, che permise di effettuare attacchi bruteforce efficaci su connessioni DES già nel 1999. Il triple-DES è un sistema che usa tre chiavi del DES, di cui almeno due univoche, per codificare e decodificare i dati. È retrocompatibile con il DES usando tre volte la stessa chiave. Anch'esso fu sostituito poiché facilmente violabile grazie all'aumento della potenza di calcolo dell'elettronica consumer.

## ECB

L'Electronic CodeBook è il block cypher più semplice in assoluto. Ogni blocco è criptato separatamente tramite una chiave simmetrica, come per esempio la frase di un libro, da cui deriva il nome dell'algoritmo. Poiché due blocchi identici sono crittografati allo stesso modo ogni blocco può essere crittografato in parallelo e quindi molto velocemente. Altrettanto velocemente si può però decrittare il messaggio tramite una analisi delle frequenze, poiché non genera casualità nel messaggio finale, motivo per cui oggi è un algoritmo superato.

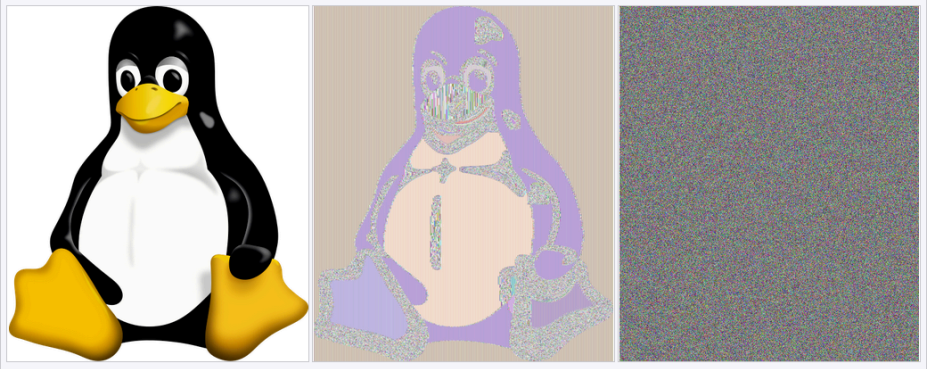


Figura 1: wikipedia.org

## Counter mode cypher

Il counter mode cypher è un block cypher che aumenta l'entropia di un messaggio crittografato aggiungendo alla funzione di codifica un contatore, in modo che due blocchi identici non siano codificati alla stessa maniera. Viene usata nel protocollo CCMP, che a sua volta viene usata in WPA2 per la segretezza delle comunicazioni. Si basa su AES con un cifrario counter mode usato su blocchi e chiave da 128 bit.

[12] https://en.wikipedia.org/wiki/Data_Encryption_Standard#Chronology

## Stream cypher

Sono una famiglia di algoritmi block cypher che operano similmente al one time pad, in cui un blocco del messaggio viene crittografato eseguendo lo XOR con un blocco di eguali dimensione del *keystream*, che viene poi scartato. Il *keystream* viene generato pseudo-casualmente da una chiave simmetrica. È un metodo estremamente veloce, motivo per cui questi algoritmi vengono usati per applicazioni che richiedono la minore latenza possibile, come lo streaming audio e video in tempo reale e le chiamate VoIP. Una sua versione, il RC4, viene usato dal WEP per la crittografia dei dati.

## Hash, HMAC

Una funzione di hash è una funzione che, dato un qualunque input, genera una stringa di lunghezza fissa. Non essendo biunivoca è molto difficile risalire ai dati originali dal hash. HMAC (Hash-based Message Authentication Code) è un metodo di autenticazione e controllo dell'integrità basato sull'uso degli hash: ogni pacchetto contiene un hash della concatenazione di messaggio, chiave segreta ed eventuale padding[13] . Viene usato nei protocolli TLS, HTTPS e IPsec con una funzione di hash specificata dal protocollo rappresentata come HMAC-[metodo hash], per esempio HMAC-SHA256. La robustezza di HMAC dipende dal metodo di hash utilizzato. Si può aumentare la sicurezza del protocollo inviando una parte troncata del hash[13].

## Attacchi DNS

Il DNS (Domain Name System) si occupa della traduzione da nome di dominio a indirizzo IP. Essendo essenziale per la navigazione in Internet sono stati sviluppati diversi metodi per renderlo inacessibile o sostituirsi ad esso, come il *DNS spoofing* che permette ad un utente malevolo di rispondere al posto di un server autorevole ad un utente. Creare dei finti pacchetti UDP di risposta non è difficile: DNS di default opera in chiaro. Per sostituirsi ad un server autorevole si può inibire la capacità del server di gestire richieste tramite un attacco DoS o DDoS (che satura la capacità di risoluzione dei domini) o anche con l'ARP spoofing se l'utente malevolo è connesso alla rete.

## IPsec

IPsec è uno standard di rete che cerca di rendere le connessioni IP sicure tramite l'implementazione di crittografia, autenticazione e controllo dell'integrità. La complessa implementazione di queste funzionalità causa un overhead maggiore nell'elaborazione dei pacchetti rispetto a IP, ma in cambio offre:

- la possibilità di creare e connettersi a reti virtuali tramite la *tunnel mode* (le VPN);
- verifica l'origine del pacchetto (tramite HMAC, che si occupa anche dell'integrità del pacchetto);
- la negoziazione dello scambio delle chiavi crittografiche;
- una protezione base dai *replay attack*.

## ⛒ WEP

Il Wired Equivalent Privacy fu il primo protocollo di sicurezza pensato per le reti wireless specificate nel IEEE 802.11. Per la crittografia dei dati usava RC4, uno stream cypher che esegue lo XOR tra un blocco di dati e parte del *key stream* generato dalla chiave (ovvero la password). Dei difetti di progettazione in WEP resero lo standard particolarmente debole:

[13] https://datatracker.ietf.org/doc/html/rfc2104

parti dello *key stream* erano spesso uguali, rendendo l'analisi delle frequenze un metodo affidabile per ottenere la chiave privata e quindi poter intercettare tutto il traffico di rete della rete[14]. Esistono alcuni strumenti gratuiti che permettono in maniera affidabile di scoprire la chiave di una rete WEP in meno di un minuto già dal 2007[15], solo 8 anni dopo la rettificazione dello standard[16]. Fu sostituito temporaneamente da WPA e infine dal ben più robusto e sicuro WPA2, che è oggigiorno il protocollo più usato in reti domestiche e aziendali. Usa uno CCMP, uno stream cypher in counter mode, rendendo quindi più difficile l'analisi della frequenza.

[14] Pagina 823 Computer Networks 5th edition

[15] https://eprint.iacr.org/2007/120.pdf

[16] https://it.wikipedia.org/wiki/Wired_Equivalent_Privacy