Networking

I ragni della B1

27 febbraio 2018

Indice

Premessa

Queste dispense rispondono all'esigenza di sistematizzare il materiale didattico dei corsi di Architettura Reti e Protocolli tenuti presso il Dipartimento di Matematica e Informatica dell'Università degli Studi di Perugia, integrando le informazioni che si ricavano dalle dispense dei due corsi e sforzandosi di renderle più facilmente comprensibili. Quanto segue è il risultato di un lavoro di riorganizzazione dei contenuti e progressivo raffinamento delle spiegazioni. Teniamo a sottolineare che non tutti gli argomenti presentano lo stesso livello di approfondimento ed è dunque auspicabile che il materiale venga revisionato, ampliato e aggiornato in accordo agli sviluppi futuri delle tecnologie trattate. Il file LaTeX e le immagini utilizzate sono disponibili nella nostra repository di GitHub[1]. Gli studenti che, nei prossimi anni, volessero collaborare sono invitati a farlo seguendo le istruzioni presenti nel file CONTRIBUTING.md e nel rispetto della licenza allegata.

[1] github.com/Disorganizzazione/Ragnatele

0 Introduzione

La comunicazione, intesa come scambio di informazioni, può avvenire solo se l'emittente e il ricevente concordano sull'interpretazione del messaggio trasmesso. In altre parole, deve esistere una serie di regole comuni che permetta di risalire al significato del messaggio, in quanto la stessa informazione può e deve assumere forme diverse, anche a seconda del canale di comunicazione. Nell'ambito delle telecomunicazioni, questo insieme di regole definito formalmente è detto **protocollo di comunicazione**.
Se i partecipanti sono molteplici, sarà necessario definire un sistema utilizzato da tutti, che indichi quali protocolli utilizzare in quali situazioni. É a questo che servono gli **standard**.

0.1 Gli standard

Si distinguono standard *de iure*, cioè codificati dalle Organizzazioni preposte, e standard *de facto*, affermatisi spontaneamente per la loro adozione massiccia.

0.1.1 IEEE 802

Famiglia di protocolli e servizi standardizzati dall'IEEE 802 *LAN/MAN Standards Committee* (LMSC): situata ai due livelli più bassi del Modello di riferimento ISO/OSI, si dedica alle reti che utilizzano pacchetti di lunghezza variabile. É qui che vengono definiti i sottolivelli MAC e LLC.
Gli standard sono numerati in base al gruppo di lavoro che li ha prodotti.
I gruppi più importanti sono:

- IEEE 802.1 LAN;
- IEEE 802.3 Ethernet;
- IEEE 802.5 TokenRing;
- IEEE 802.11 WLAN;
- IEEE 802.15 WPAN;
- IEEE 802.16 Broadband Wireless Access, conosciuto anche come *WirelessMAN* (WiMAX).

Una lista completa dei gruppi di lavoro e dei loro standard è reperibile sul sito ufficiale dello LMSC: `www.ieee802.org`.

0.1.2 RFC

Request For Comments: tipologia di documento pubblicato dalla IETF, riportante informazioni o specifiche riguardanti innovazioni nell'ambito di Internet. Fonte ufficiale: `www.rfc-editor.org`.

0.1.3 ASN.1

Abstract Syntax Notation One (da non confondere con l'ASN): notazione internazionalmente standardizzata indipendente dall'implementazione, dalla piattaforma e dal linguaggio, volta a specificare strutture dati ad alto livello di astrazione.

0.2 Organizzazioni

0.2.1 IEEE

Institute of Electrical and Electronic Engineers, molto attivo nello sviluppo di standard di comunicazione dati. Al suo interno, riveste un ruolo di particolare importanza nel campo delle telecomunicazioni la **ComSoc** (Communications Society), e più in particolare il comitato IEEE 802 *LAN/MAN Standards Committee* (LMSC), commissione preposta a sviluppare standard per le reti locali e metropolitane.

0.2.2 CCITT

Consultative Committee for International Telephony and Telegraphy: parte della **ITU** (International Telegraph Union), agenzia dell'ONU specializzata in telecomunicazioni, articola i propri lavori in quadrienni, gli *study periods*, al termine dei quali ha luogo un'assemblea plenaria incaricata di emettere le cosiddette *raccomandazioni*.

0.2.3 ISO

International Standards Organization, consulente dell'ONU allo scopo di promuovere a livello globale lo sviluppo di standard, con l'obiettivo di favorire lo scambio internazionale di beni e servizi. Il suo maggior successo nell'ambito delle telecomunicazioni è il concepimento del Modello di riferimento ISO/OSI.

0.2.4 IETF

Internet Engineering Task Force: organismo internazionale composto da tecnici, specialisti e ricercatori interessati all'evoluzione tecnica e tecnologica di Internet. Si occupa di sviluppare e promuovere standard Internet, in stretta cooperazione con il W3C e l'ISO. L'iscrizione è a titolo personale e non come rappresentanti di qualche istituzione pubblica o privata.

0.2.5 IRTF

Internet Research Task Force: organizzazione che coordina i diversi gruppi di ricerca in ambito Internet, controllata dall'**IRSG** (Internet Research Steering Group) e il cui coordinatore è nominato dallo **IAB** (Internet Activities Board).

0.2.6 W3C

World Wide Web Consortium: fondata da CERN e MIT, è un' organizzazione non governativa internazionale che ha come scopo quello di sviluppare tutte le potenzialità del WWW. La principale attività svolta dal W3C consiste nello stabilire standard tecnici inerenti sia i linguaggi di marcatura che i protocolli di comunicazione.

0.2.7 IANA

Internet Assigned Numbers Authority: ente storico incaricato della gestione dello spazio di indirizzamento IP e dei nomi di dominio, degli ASN e dei numeri di protocollo IP. Nel tempo, IANA ha delegato la gestione locale ad una serie di entità regionali:

- **ARIN** per le Americhe;
- **RIPE NCC** per l'Europa;
- **APNIC** per l'Asia e tutta l'area del Pacifico.

Attualmente, la materia è oggetto di completa ristrutturazione sotto la responsabilità dell' ICANN, da cui lo IANA è stato assimilato.

0.2.8 ICANN

Internet Corporation for Assigned Names and Numbers: organizzazione che ha attualmente la responsabilità della gestione dello spazio di indirizzamento IP (vedi IANA).

0.2.9 GIPI

Global Internet Policy Initiative: rete di organizzazioni non governative no-profit che sostiene, nei paesi in via di sviluppo, l'adozione di piattaforme legislative e politiche per la realizzazione di un'accesso ad Internet aperto e democratico.

0.3 Modello di riferimento ISO/OSI

Il modello Open Systems Interconnection è stato progettato dalla ISO come modello di riferimento per standardizzare la comunicazione tra sistemi aperti. Le motivazioni di tale scelta si chiariscono se si pensa all'Internet delle origini: alla fine degli anni '70 i leader del settore delle tecnologie di rete si ritrovarono di fronte a problemi di compatibilità, dovuti alla molteplicità delle diverse architetture proprietarie. Il modello lSO/OSI si prefiggeva dunque di offrire una base teorica per lo sviluppo di standard di comunicazione indipendenti dai fornitori. In base ad esso, il complesso processo della comunicazione di rete si divide in sette livelli, ad ognuno dei quali dovranno essere svolti compiti specifici. Questo può funzionare solo se tutti i sistemi coinvolti nella comunicazione si attengono a regole precise, stabilite dai protocolli, che si applicano ad uno o più livelli (si parla in tal caso di protocolli multilivello). Il modello di riferimento ISO/OSI non è però uno standard di rete concreto: esso descrive in forma astratta quali procedimenti devono essere regolati per far funzionare la comunicazione in una rete.

Vantaggi dell'architettura a livelli La comunicazione tra due computer può apparire banale agli utenti, ma in realtà è proprio la sua complessità che ha portato alla decisione di suddividerla in livelli: ognuno accede tramite un'interfaccia a quello inferiore e mette un servizio a disposizione di quello superiore.
Questo approccio ha due vantaggi decisivi:

- le funzioni di ogni livello sono definite chiaramente, cosicché per ogni livello possono essere sviluppati diversi standard, indipendenti gli uni dagli altri;
- La chiara suddivisione in livelli fa sì che le modifiche ad uno standard non abbiano alcun effetto sui processi che operano ad un altro livello. Anche questo facilita l'introduzione di nuovi standard.

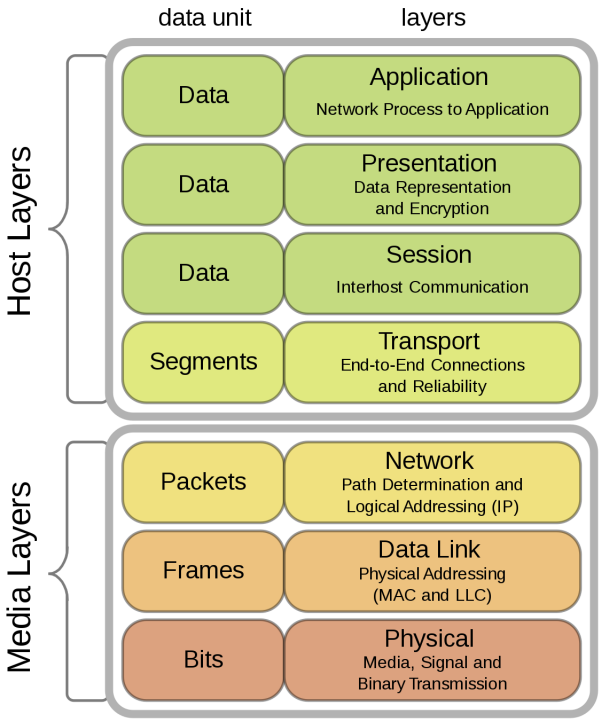


Figura 1: Modello di riferimento ISO/OSI

0.4 Internet

Rete globale di reti che abilita i DTE a comunicare direttamente ed in modo trasparente e a condividere servizi, definita formalmente nel RFC 1122 (originariamente in RFC 760).

Definizione *Internet* si riferisce al sistema di informazione globale che:

- è logicamente interconnesso attraverso uno spazio d'indirizzamento unico e globale, basato sull'IP o sulle sue successive estensioni e sviluppi;

- è in grado di supportare comunicazioni mediante la Internet protocol suite (TCP/IP) o le sue successive estensioni/sviluppi, e/o altri protocolli compatibili con l'IP;
- fornisce, utilizza e rende accessibili, sia pubblicamente che privatamente, servizi di alto livello che poggiano sui differenti strati di comunicazioni e di infrastrutture a esse correlate.

0.4.1 Cronologia

1962:
- Licklider propone il concetto di *galactic network*: un'infrastruttura basata su un insieme di computer globalmente interconnessi al fine di scambiare dati. Internet è il risultato dell'evoluzione di questa idea.
- Licklider avvia il programma di ricerca **ARPA** (Advanced Research Project Agency) che cambierà il proprio nome nel '71 in **DARPA** (Defense ARPA).
- Kleinrock pubblica il primo articolo sulla teoria del *packet switching*.

1965:
- Merrill e Roberts riescono a far comunicare due computer (Uno in Massachussets e l'altro in California), creando la prima WAN della storia.

1969:
- Nasce ARPANET (ARPA NETwork), prima rete globale dalla quale nascerà Internet. Il suo primo stadio è la connessione host-to-host di due nodi.
- Crocker pubblica il primo RFC.

1973:
- A Standford, Cerf e Kahn ideano il TCP/IP: nasce la Posta elettronica.
- Metcalfe inventa l'Ethernet.

1980:
- Il TCP viene adottato come protocollo standard dal DoD (Department of Defense).
- Iniziano le attività di **USENET** (USEr NETwork) e dei relativi primi gruppi di discussione delle NEWS, prime applicazioni client-server su larga scala.

1983:
- Postel sviluppa il DNS.
- ARPANET adotta il TCP/IP, mentre il Modello di riferimento ISO/OSI è sempre meno applicato.
- Vengono introdotte le reti IP di classe A, B e C.
- Vengono introdotti i TLD (vedi DNS) .edu, .com, .net, .org, oltre quelli della codifica ISO.
- La **NSF** (National Science Foundation) costituisce i centri di calcolo per servire la comunità scientifica americana.

1985:
- L'algoritmo di routing originario di Internet viene rimpiazzato dai protocolli IGP ed EGP.
- Nascono le prime multinazionali operanti nel settore delle reti (IBM, Proteon, Synoptis, CISCO...).

1987:
- Diventano sempre più importanti le problematiche di network management, che porteranno allo sviluppo del SNMP.

1989:
- Cerf e Kahn organizzano il primo workshop sul Gigabit.
- Barners-Lee, al CERN, propone il concetto di ipertesto: nasce il WWW.

1991:
- Nasce **PGP** (Pretty Good Privacy).

1992:
- Nasce **ISOC** (Internet SOCiety), fondata da Cerf e Kahn.
- Il WWW esplode. Boom.

1995:
- IL **FNC** (Federal Networking Council) formula la Definizione formale di Internet.

0.4.2 WWW

Word Wide Web: inventato nel 1989 da Tim Berners-Lee, ricercatore al CERN, e comunemente noto come Web, è un modo di accedere alle informazioni tramite internet, basato sul concetto di ipertesto e, in particolare, sul protocollo HTTP.

0.4.3 Intranet

Termine utilizzato per indicare l'uso di Internet all'interno di un'azienda, basato sull'utilizzo di una LAN.

0.4.4 Extranet

Termine che identifica le risorse hardware e software che realizzano la presenza visibile in Internet di un'organizzazione.

0.5 Internet protocol suite (TCP/IP)

Detto anche *Stack TCP/IP*, è la famiglia di protocolli alla base del funzionamento di Internet. I protocolli sono divisi in quattro livelli, ripresi in parte dal Modello di riferimento ISO/OSI, questa suddivisione rappresenta lo standard *de facto* per l'architettura di rete.

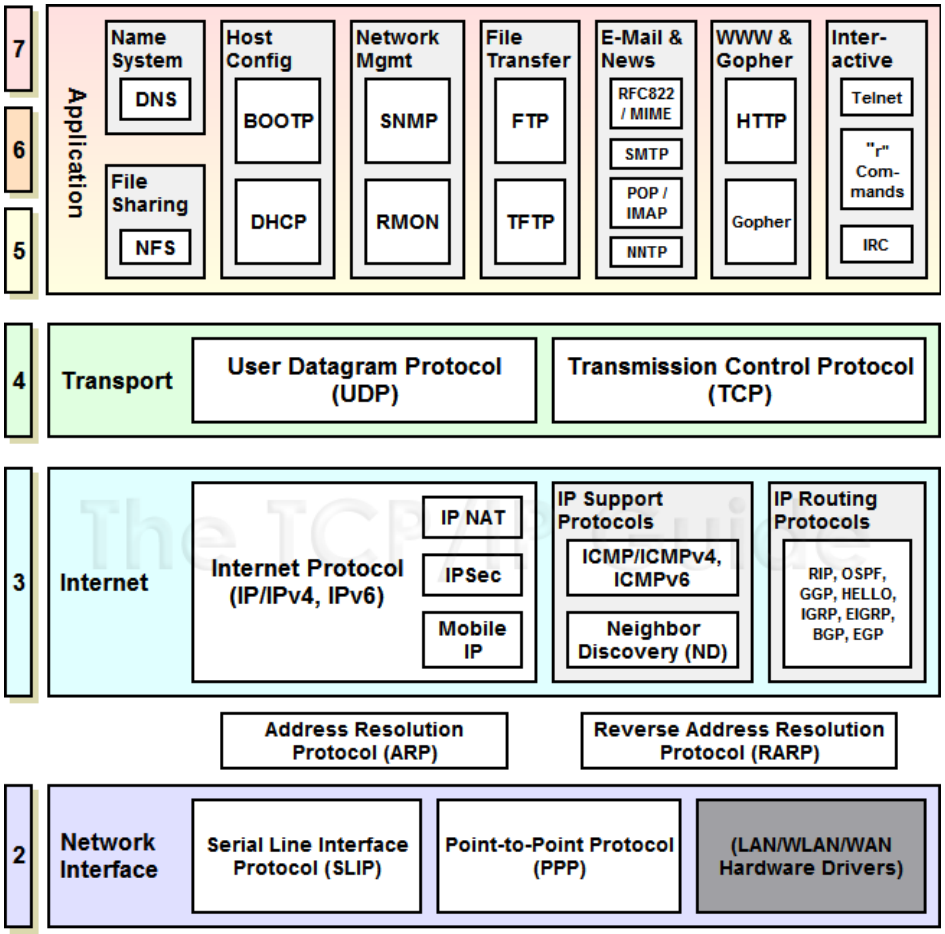


Figura 2: Famiglia dei protocolli TCP/IP

0.6 Protocolli elementari

In questa sezione saranno introdotti alcuni semplici protocolli[2], suddivisi, a seconda della relazione tra i DTE coinvolti, in:

- protocolli in ambito **primario-secondario**: RTS/CTS, XON-XOFF, ARQ;
- protocolli **peer-to-peer**;
- protocolli ibridi;

[2]Nota per i futuri revisori: vi saremmo grati se, una volta individuatoli con certezza, li collocaste ai rispettivi livelli di pertinenza

0.6.1 RTS/CTS

Il protocollo RTS/CTS (*Request To Send/Clear To Send*, basato sull'interfaccia RS-232, è un protocollo in ambito primario-secondario, originariamente utilizzato con modem Half-Duplex. Esso prevede che la stazione secondaria che voglia trasmettere al *master* (cioè alla stazione primaria) attivi il segnale RTS, che le garantisce il permesso di trasmettere, revocabile in qualsiasi momento, attivando il segnale CTS (la rispondenza tra i due segnali è detta *handshake*).

0.6.2 XON-XOFF

Nel caso del protocollo XON-XOFF, la stazione primaria invia dati ad un terminale (stazione secondaria), che li memorizza. Nel momento in cui il terminale si satura, esso invia il carattere ASCII (vedi Codice) XOFF, cui segue l'interruzione delle trasmissioni. Non appena è nuovamente in grado di ricevere, lo segnala tramite il carattere XON.

0.6.3 ARQ

Il protocollo ARQ (*Automatic Repeat reQuest* o *Automatic Repeat Query*) è di tipo Full-Duplex e sfrutta il concetto di *finestra scorrevole* per trasmettere in modo più efficiente: il messaggio è suddiviso in sequenze di frame, inviati a gruppi. Alla ricezione di un certo numero di frame, il mittente riceve un riscontro da parte del destinatario, il quale indica quali frame sia necessario ritrasmettere tramite una sequenza di `0` ed `1`. Per quel che riguarda la ritrasmissione, possono essere adottate due metodologie differenti:

- *Go-back-n*: si ricomincia la trasmissione a partire dall'n-esimo frame, il primo danneggiato;
- approccio selettivo: vengono ritrasmessi i soli frame danneggiati.

1 Livello fisico

Nonostante l'amministratore di rete non abbia la possibilità di influirvi direttamente, è importante descrivere lo strato fisico poiché esso influenza significativamente le prestazioni della rete.

1.1 Terminologia

1.1.1 Informazione

L'informazione è una grandezza misurabile in bit. In particolare,

$$Q = log_2 n$$

dove Q è il numero di bit necessari per rappresentare l'informazione relativa ad n possibili stati.

1.1.2 Codice

Al fine di rappresentare l'informazione in maniera tale da renderne più semplice la gestione, un codice associa sequenze di bit a caratteri. I codici che godono della più ampia diffusione sono:

- ASCII (American Standard Code for Information Interchange, 7 bit estesi a 1 byte);
- BCD (Binary-Coded Decimal);
- AIKEN;
- Gray;
- EBCDIC (Extended Binary Coded Decimal Code) 8 bit, in uso presso le banche.

1.1.3 Segnale

Si dice *segnale* una grandezza fisica variabile nel tempo corrispondente ad un'informazione. Un segnale **analogico** varia in modo continuo nel tempo ed ha infiniti livelli di intensità; un segnale **digitale** varia invece in modo discreto e ha solo due livelli di intensità. Ogni tipo di dato può essere rappresentato in entrambe le maniere ed essere convertito in entrambi i sensi.

Fra i segnali analogici assumono particolare rilevanza i **segnali sinusoidali**, ossia segnali che variano nel tempo secondo una legge del tipo

$$u = U sen(\omega t + \varphi)$$

dove

- u è l'ampiezza istantanea;
- U è l'ampiezza massima;
- ω è la *velocità angolare*, ovvero la variazione dell'angolo nel tempo, espressa in radianti al secondo;
- φ è la *fase*, ossia lo sfasamento rispetto all'origine, espresso in radianti;
- t è il tempo;
- T è il *periodo*, cioè l'intervallo di tempo (in secondi) impiegato dall'onda per effettuare un'oscillazione completa;
- $1/T = f$ si dice *frequenza* e si misura in Hz $(1/s)$.

La curva in figura rappresenta istante per istante il valore del seno dell'angolo descritto da un segmento che ruota con un estremo vincolato all'origine degli assi cartesiani, in senso antiorario, con velocità angolare ω. Di conseguenza, la frequenza f è il numero di volte che il segmento effettua un giro completo in un secondo.

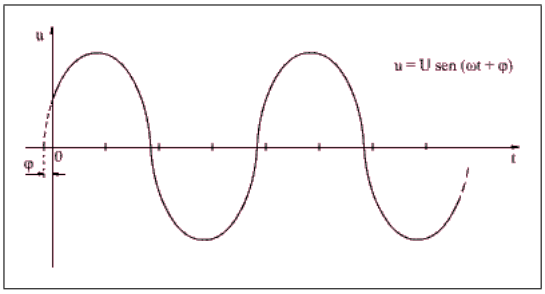


Figura 3: Rappresentazione grafica di un segnale sinusoidale

1.1.4 Lunghezza d'onda

In un segnale sinusoidale, la distanza tra due massimi relativi è detta *lunghezza d'onda* $\lambda = c/f = cT$ (dove c è la velocità di propagazione del segnale).

1.1.5 Spettro

Lo spettro è l'insieme delle frequenze che compongono un segnale. Questa affermazione va considerata alla luce del **teorema di Fourier**, il quale afferma che un segnale può essere rappresentato come somma di sinusoidi (potenzialmente infinite) con caratteristiche differenti.

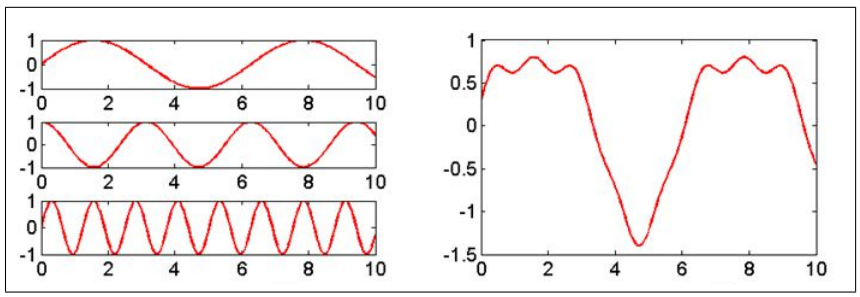


Figura 4: Esempio di funzione composta da tre sinusoidi semplici.

1.1.6 Banda

La banda è costituita dall'insieme di frequenze dello spettro *effettivamente utilizzate* e corrisponde alla massima velocità teorica della rete. Si parla di *banda larga* nel caso in cui l'ampiezza di banda sia sensibilmente superiore a quella utilizzata correntemente in telefonia (3100 Hz).

1.2 Qualità delle trasmissioni

I criteri per valutare la bontà della rete sono molteplici, legati da un lato alle prestazioni, dall'altro ad affidabilità e sicurezza.

1.2.1 Criteri di valutazione in base alle prestazioni

Throughput Quantità di dati spedita nell'unità di tempo; rappresenta l'effettiva velocità della rete.

Latenza Detta anche ritardo, è il tempo necessario perché un messaggio giunga a destinazione; per il suo calcolo si tiene conto di:

- **tempo di propagazione**: tempo di transito sulla rete per arrivare dal mittente al destinatario;
- **tempo di trasmissione**: tempo necessario per immettere i bit sulla rete, ossia $\frac{dim_m}{v}$, dove dim_m è la dimensione del messaggio e v la velocità trasmissiva;
- **tempo di elaborazione (o di inoltro)**: tempo necessario ai nodi per consegnare il messaggio in transito, non legato al traffico ma solo ad hardware e software;
- **tempo di attesa** nelle code di rete, dipendente dal traffico.

1.2.2 Criteri di valutazione in base all'affidabilità

Jitter Variabilità del ritardo con cui i pacchetti vengono consegnati in ricezione.

Packet loss Percentuale dei pacchetti non giunti a destinazione.

1.2.3 Velocità di trasferimento

Un parametro interessante in ambito di comunicazione dati è la velocità di trasferimento o *bitrate*, espressa in *bit/sec*. Preliminarmente, occorre intendersi sul tipo di canale interessato, distinguendo:

- canali *perfetti*, cioè senza alcun tipo di distorsione;
- canali *ideali*, con solo un ritardo costante nella propagazione;
- canali *reali*, con alterazioni in funzione della frequenza dei segnali che li attraversano.

La massima velocità di trasferimento, detta anche *max data rate*, può essere calcolata sia in funzione del numero di livelli, sia in funzione del Rumore.

1.2.4 Condizione di Nyquist

Stabilisce che la massima velocità di trasferimento su un canale di banda B con m livelli è

$$2B \log_2 m$$

1.2.5 Teorema di Shannon-Hartley

Afferma che la massima velocità alla quale è possibile trasmettere senza errore è

$$B \log_2(1 + \mathbf{SNR})$$

dove B è l'ampiezza di Banda e **SNR** è il rapporto segnale-Rumore.

1.2.6 Strumenti software

I criteri sopra descritti possono essere valutati con numerosi strumenti software, tra cui:

- il comando Unix-Linux `ping`, che, mediante l'invio di *echo messages* del protocollo ICMP, verifica se un host remoto possa essere raggiunto e riporta le statistiche relative alla trasmissione, in particolare:
  - Packet loss, in percentuale. Con una buona connessione dovrebbe sempre essere pari a 0;
  - RTT (*round trip time*): statistiche sul tempo di trasmissione;

```
→  ~ ping google.com
PING google.com (172.217.19.46) 56(84) bytes of data.
64 bytes from ham02s11-in-f46.1e100.net (172.217.19.46): icmp_seq=1 ttl=51 time=95.5 ms
64 bytes from ham02s11-in-f46.1e100.net (172.217.19.46): icmp_seq=2 ttl=51 time=83.0 ms
64 bytes from ham02s11-in-f46.1e100.net (172.217.19.46): icmp_seq=3 ttl=51 time=83.4 ms
64 bytes from ham02s11-in-f46.1e100.net (172.217.19.46): icmp_seq=4 ttl=51 time=77.0 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 77.007/84.773/95.521/6.717 ms
```

Figura 5: Esempio di output del comando `ping`.

- il comando Unix `traceroute` o `tracepath`, che indica i dispositivi attraversati per raggiungere una data destinazione;
- applicazioni web quali ad esempio `speedtest.net` e Ne.Me.Sys, quest'ultimo sviluppato da AGCOM, utilizzabile per produrre elementi probatori nel caso in cui l'utente voglia esercitare il diritto di reclamo e recesso rispetto a promesse contrattuali di velocità di accesso ad Internet non mantenute dall'operatore.

1.3 Filtri

Un filtro è un sistema che tratta le varie componenti del segnale in modo diverso a seconda della loro frequenza.
È opportuna innanzitutto una distinzione tra filtri *passivi* ed *attivi*: i primi sono costituiti solamente da resistenze e condensatori, mentre i secondi includono altre componenti, come i transistor e gli amplificatori. Inoltre, a seconda del comportamento, si distinguono quattro tipi di filtri:

- **filtro passa basso**: permette il passaggio delle frequenze al di sotto di una determinata *frequenza di taglio*;
- **filtro passa alto**: complementare al filtro passa basso, permette il passaggio delle frequenze al di sopra della frequenza di taglio;
- **filtro passa banda**: composizione di un filtro passa basso e un filtro passa alto: permette il passaggio delle frequenze comprese tra le frequenze di taglio dei due filtri;
- **filtro elimina banda**: complemento del filtro passa banda, blocca le frequenze comprese tra le due frequenze di taglio.

1.4 Alterazioni del segnale

L'espressione "alterazioni del segnale" racchiude tutti i tipi di deterioramento del suddetto.

1.4.1 Attenuazione

Perdita di energia del segnale, misurata in dB, cioè $10 \log_{10} \frac{P_i}{P_f} = 20 \log_{10} \frac{V_i}{V_f}$, dove P_i rappresenta la potenza iniziale e P_f la potenza finale, mentre V_i e V_f sono rispettivamente il potenziale elettrico iniziale e finale; vi si pone rimedio tramite dispositivi come gli amplificatori.

1.4.2 Distorsione

Cambiamento di forma del segnale, si verifica quando esso è composto da varie frequenze e dipende dal ritardo all'arrivo delle singole componenti.

1.4.3 Rumore

Insieme dei segnali indesiderati, generati da processi sia interni che esterni al sistema, che si sovrappongono a quello utile. Il rapporto segnale-rumore (**SNR**, *Signal to Noise Ratio*) mette in relazione la potenza del segnale utile con quella del rumore.

1.4.4 Interferenza

Sovrapposizione di informazioni non desiderate al segnale utile. Solitamente, per interferenza s'intende in particolare la contaminazione da parte di segnali esterni, i quali, a differenza del rumore, che è totalmente casuale, possono portare a loro volta informazione, benché indesiderata. L'interferenza **ISI** (*Inter Symbol Interference*, interferenza intersimbolica) avviene quando, in seguito alla traduzione, i simboli si sovrappongono sull'asse del tempo; chiaramente questo è legato ai limiti della banda.

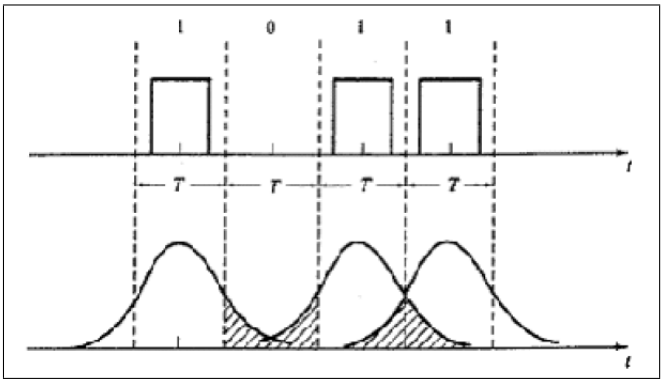


Figura 6: Interferenza intersimbolica

1.5 Multiplazione

La multiplazione è una tecnica che prevede l'impiego di un unico canale per più comunicazioni differenti contemporanee.

1.5.1 FDM

Frequency Division Multiplexing: tuttora impiegata nelle comunicazioni telefoniche, prevede che in fase di trasmissione le comunicazioni subiscano un shift di frequenza e che la frequenza originaria sia ripristinata all'arrivo alla destinazione. Il numero di canali multiplabili dipenderà, in linea di principio, solo dalla capacità del mezzo trasmissivo.

1.5.2 WDM

Wavelength Division Multiplexing: utilizzata per i segnali ottici (vedi Fibra ottica), consiste nel modulare la lunghezza d'onda del raggio luminoso, così da inviare diversi raggi contemporaneamente.

DWDM Dense WDM: capace di modulare 16 lunghezze d'onda alla distanza di 0.8 nm.

CWDM Coarse WDM (WDM grossolana): utilizza maggiori spaziature tra i canali, con risparmio a livello economico. Impiegata per la realizzazione di MAN a basso costo.

1.5.3 TDM

Time Division Multiplexing: nella TDM, i dispositivi ottengono a turno, per un brevissimo lasso di tempo, l'uso esclusivo del canale di comunicazioni e delle risorse ad esso dedicate, ad esempio la banda. La TDM si suddivide in:

- **sincrona**: gli intervalli di tempo sono indipendenti dalla presenza di dati da spedire;
- **statistica**: gli intervalli vengono allocati solo quando ci sono dati da inviare. La velocità complessiva è solitamente minore della somma delle velocità dei canali.

1.6 Modulazione

Sovente capita che l'informazione debba essere convertita in maniera idonea ad essere inviata nel mezzo trasmissivo adottato. Tale processo è detto *modulazione* ed è reversibile: il *segnale portante*, caratteristico del mezzo trasmissivo, viene modificato in uno dei suoi parametri essenziali in accordo al segnale in ingresso, contenente l'informazione da trasmettersi, che è detto *segnale modulante*, tipicamente analogico.

1.6.1 Modulazione ad onda continua

Si parla di modulazione ad onda continua nel momento in cui viene modulata una portante sinusoidale. Ne esistono tre tipologie.

AM (Amplitude Modulation): l'ampiezza del segnale portante viene modulata in proporzione al segnale modulante.

FM (Frequency Modulation): è la frequenza del segnale portante ad essere modulata, infittendosi quando la modulante si innalza e rarefacendosi quando si abbassa. Tipica delle trasmissione radiofoniche in Italia, pur necessitando di circuiti più complessi, è preferibile alla modulazione di ampiezza per motivi di efficienza e maggior tolleranza a disturbi di vario tipo.

PM (Phase Modulation): molto simile alla modulazione di frequenza - come si può notare in figura, consiste nel variare la fase Φ (vedi Segnale) in proporzione all'intensità della modulante. Spesso s'impiega in sistemi in FM per ottenere l'amplificazione del segnale.

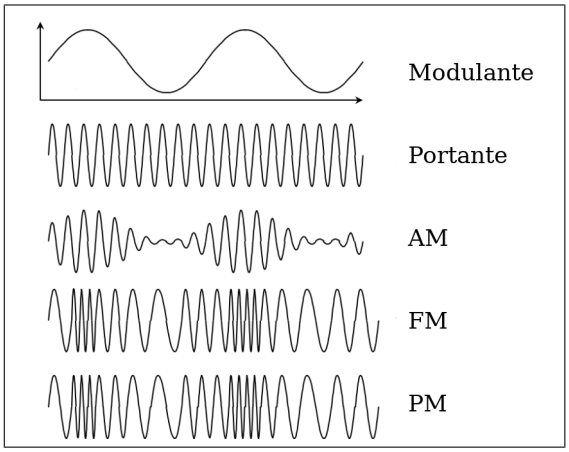


Figura 7: Confronto tra tipologie di modulazione ad onda continua

1.6.2 Modulazione impulsiva

La modulazione impulsiva è un tipo di modulazione in cui la modulante è una sinusoide, mentre la portante è composta da una serie di impulsi.

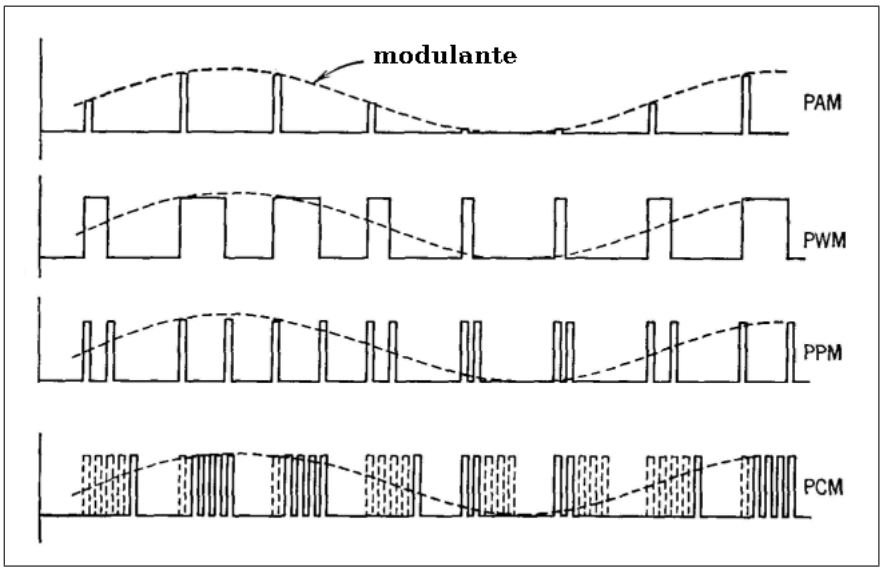


Figura 8: Confronto tra tipologie di modulazione impulsiva

PAM (Pulse Amplitude Modulation), analoga alla AM;

PWM (Pulse Width Modulation), dove la durata dell'impulso cambia in base all'ampiezza della modulante;

PPM (Pulse Position Modulation), analoga alla PM;

PCM (Pulse Code Modulation), nata dall'esigenza, intorno agli anni '40, di aumentare il numero di collegamenti telefonici interurbani. Per evitare l'impianto di grossi fasci di conduttori, ingombranti, costosi e difficili da connettere, si pensò di multiplare più collegamenti su un unico cavo, utilizzando una soluzione preesistente, la FDM, poi abbandonata per la più moderna TDM, inizialmente realizzata per mezzo delle tre tecniche impulsive sopra descritte, poi attraverso appunto la PCM, ad oggi l'unica adottata su larga scala.
La PCM costa di tre fasi distinte:

1. **campionamento**: conversione del segnale continuo in un segnale discreto nel tempo, valutandone l'ampiezza a intervalli regolari. Ciò è possibile, come affermato dal Teorema di Shannon[3], poiché è possibile rappresentare un segnale con frequenza limitata tra f_1 ed f_2, con $f_1 < f_2$

[3]url: it.wikipedia.org/wiki/Teorema_del_campionamento_di_Nyquist-Shannon

mediante una successione di campioni con frequenza minima $2f_2$. La minima frequenza di campionamento (**cadenza di Nyquist**) è pari al doppio della banda; nella PSTN (Public Switched Telephone Network) si assume come frequenza di campionamento $f_c = 8Khz$.
Il campionamento si realizza per mezzo della PAM;

2. **quantizzazione**: discretizzazione dell'ampiezza del segnale campionato. Per ottenere un range di valori discreti, si stabiliscono un valore minimo e un valore massimo e si suddivide l'intervallo così ottenuto. Nella quantizzazione uniforme, l'intervallo è diviso in pari uguali; di norma, tuttavia, la suddivisione segue una scala logaritmica.
Com'è intuibile, la quantizzazione è un processo irreversibile, per cui è necessario tener conto dell'errore commesso - è dimostrato che, utilizzando 256 livelli di quantizzazione, l'orecchio umano non percepisce sostanziali differenze nella riproduzione dei suoni;

3. **codifica**: gli impulsi campionati e quantizzati vengono convertiti in sequenze di bit.
Nel PCM europeo, che utilizza appunto $256 = 2^8$ livelli, occorrono 8 bit per campione. Tra due sequenze di 8 bit destinate ad uno stesso canale telefonico ve ne sono altre trentuno, dirette ognuna ad un altro canale. Vengono dunque trasmessi 32 canali -di cui due di servizio- da 8 bit con 8000 campioni al secondo, per un totale di $32 \cdot 8000 \cdot 8 = 2048Mbit/sec$.

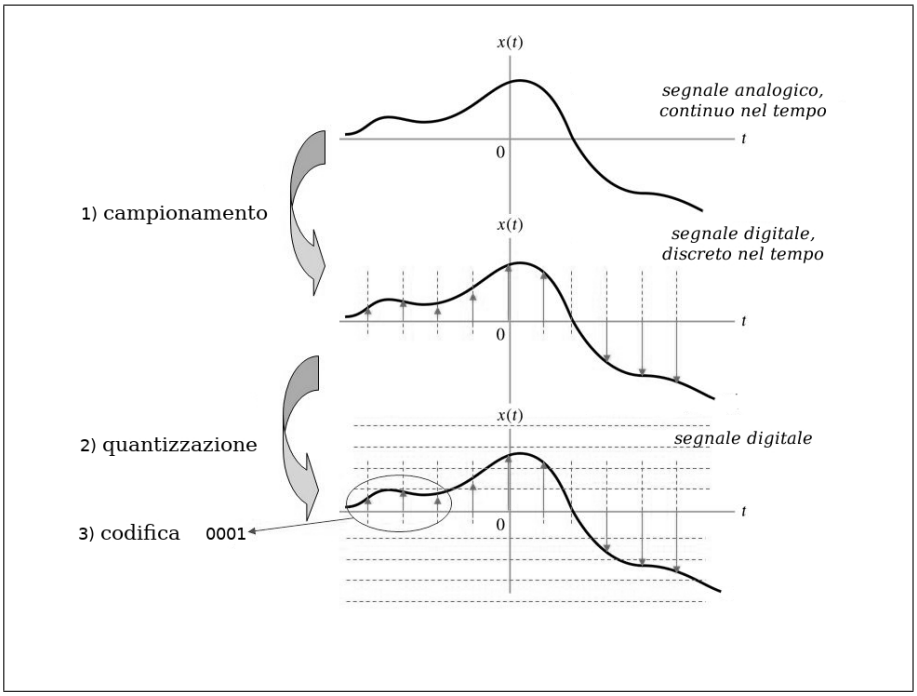


Figura 9: Fasi della PCM

1.6.3 Modulazione digitale

Nel caso in cui la comunicazione avvenga fra DTE (tramite un Modem), il termine modulazione é improprio, poiché il segnale viene convertito da digitale ad analogico (poi viceversa), ma tale conversione è ottenuta facendo corrispondere ad ogni sequenza di bit in input un forma d'onda analogica univoca e limitata nel tempo in uscita, detta *simbolo*. É più corretto dunque parlare di *codifica*, della quale esistono diverse varianti.

ASK (Amplitude-Shift Keying), derivante dalla AM. Di semplice realizzazione ma poco utilizzata, se non per trasmissioni a breve distanza, per la sua forte sensibilità al rumore. Solitamente, si concretizza in una modulazione OOK (On-Off Keying), in cui il segnale modulato ha ampiezza 0 in corrispondenza dello 0 logico e ampiezza pari a quella della portante non modulata in corrispondenza dell'1 logico.

FSK (Frequency-Shift Keying): la frequenza della portante viene alternata fra due frequenze di valore ben definito. Tali frequenze sono note l'una come frequenza d'impulso (1 logico), l'altra come frequenza d'intervallo (0 logico). In merito alla scelta di tali frequenze va notato che:

- occorre limitare il più possibile l'occupazione della banda, ma i valori delle frequenze devono essere sufficientemente distanti per evitare che vengano confuse l'una con l'altra (*Interferenza intersimbolica*);

- i due simboli devono avere periodo inferiore o uguale alla frequenza di bit dell'informazione digitale in ingresso;

- è assolutamente necessario mantenere una continuità di fase nelle variazioni di stato, poiché il circuito di demodulazione, costituito in genere da un rivelatore di passaggio per lo zero, deve essere in grado di individuare il salto di frequenza con la massima precisione.

La FSK è stata utilizzata nei primi modem V.21 e V.23 e la si impiega ancora oggi nei ponti radio e nelle trasmissioni di tipo GSM tra cellulari.

PSK (Phase-Shift Keying), derivante direttamente dalla PM. Può essere applicata in varie maniere, le più diffuse delle quali sono:

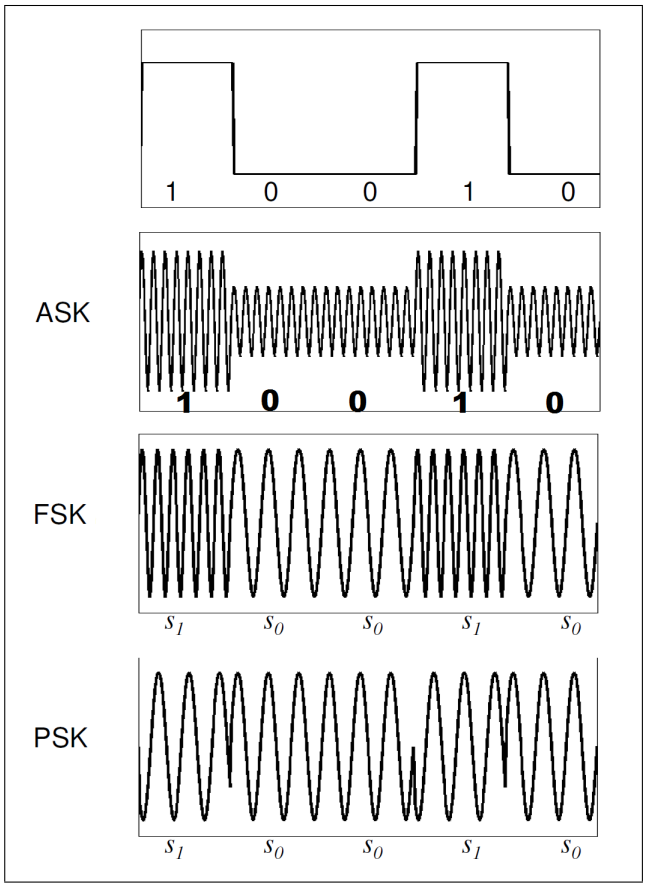


Figura 10: Confronto tra codifiche ASK, FSK, e PSK

- **BPSK** (BiPolar-Shift Keying) o **2-PSK**: quando la modulante cambia stato, il segnale modulato cambia fase. Per garantire la massima protezione dal rumore e dalle interferenze, solitamente vengono scelti i due valori di fase estremi, 0° e 180°;

- **4-PSK** e **4-QPSK**: i bit del segnale in input vengono suddivisi in coppie da un convertitore, che genera così due segnali separati; vi sono inoltre due modulatori e due portanti con frequenza identica, ma in quadratura[4]. I due segnali modulati, detti I (*Infase*) e Q (*Quadratura*), poi sommati, cambiano dunque fase a seconda del valore della coppia di bit in input e il segnale in uscita può avere quattro distinti valori di fase (le due varianti differiscono per la posizione delle quattro fasi utilizzate, che nella 4-PSK sono poste sugli assi cartesiani, mentre nella 4-QPSK sono sfasate di 45°);

[4]L'espressione *in quadratura* indica semplicemente una sfasatura di 90°: i due segnali sono ortogonali, cosicché si evitano le interferenze

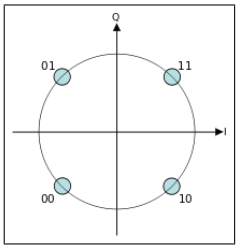


Figura 11: Esempio di distribuzione delle fasi nella modulazione 4-QPSK

- **8-PSK**: analoga alla 4-PSK, comporta l'utilizzo non di coppie ma di terne di bit;
- **DPSK** (Differential Phase-Shift Keying): analoga alla PSK, ma sono i salti di fase, e non i valori assoluti, a codificare i bit. Ne esistono diverse varianti, quali la 2-DPSK, la 4-DPSK e la 8-DPSK.

QAM (Quadrature Amplitude Modulation): combinazione di ASK e PSK, consiste nel modulare in ampiezza portanti in quadratura di uguale frequenza. Varianti della QAM particolarmente rilevanti sono la 16-QAM e la 64-QAM, usata nell' ADSL;

TCM (Trellis Coded Modulation): simile alla QAM, assicura una maggiore immunità al rumore e un minor tasso di errore aumentando la ridondanza della trasmissione. Vi è un cambio di stato sempre e soltanto in presenza di un bit 1. Il nome di questo tipo di modulazione deriva dal fatto che l'andamento temporale del segnale può essere rappresentato mediante un diagramma, visivamente simile ad un traliccio (in inglese, *trellis*).

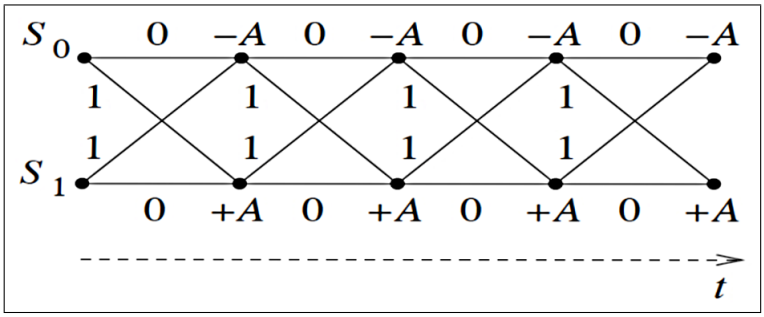


Figura 12: Diagramma a traliccio

Diagramma a costellazione Rappresentazione grafica teorica di un segnale modulato secondo uno degli schemi di modulazione digitale. Il segnale viene mostrato su un piano bidimensionale in cui I e Q sono gli assi cartesiani e i punti in cui un vettore può trovarsi vengono rappresentati con dei punti. Se c'è del rumore, attorno al punto ideale si creano delle aree, utili per la comprensione delle cause del rumore stesso.

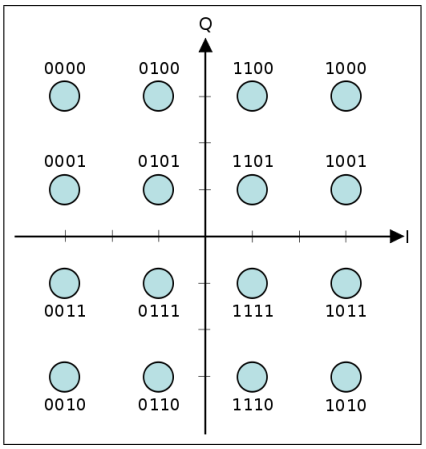


Figura 13: Diagramma a costellazione

Vettore errore Il vettore errore rappresenta la differenza tra il punto teorico in cui si sarebbe dovuto trovare il segnale nel Diagramma a costellazione e la sua posizione reale. Ciò che interessa maggiormente del vettore errore è il suo modulo, utile a valutare la qualità della modulazione, detto anche **EVM** (Error Vector Magnitude). Esso è espresso in percentuale o in dB, come rapporto tra il valore quadratico medio della potenza del vettore errore e il valore quadratico medio[5] della potenza del segnale di riferimento. In questo caso, l'EVM può avere -ed è auspicabile che abbia- valore negativo. Per la misurazione dell'EVM esistono strumenti hardware e software, tutti quanti basati sulla demodulazione del segnale ed il confronto con quello ideale.

Velocità di modulazione La velocità di modulazione, espressa in $baud = \frac{simboli}{sec}$, indica il numero di simboli trasmessi nell'unità di tempo[6]. Più in particolare, in un sistema di comunicazione digitale, si parla di *baud rate*. Velocità di trasferimento e di modulazione sono in relazione

$$v_m = \frac{v_t}{\log_2 m}$$

dove v_m è la velocità di modulazione, v_t la velocità di trasferimento ed m il numero di livelli.

1.7 Modem

Un modem (contrazione di modulatore/demodulatore) è un DCE con funzionalità di Modulazione in trasmissioni analogiche e digitali. Esistono svariati tipi di modem:

- **Modem in banda fonica**;
- **Modem ISDN** (128 kbps);
- **Modem xDSL** (640 kbps-100 Mbps);
- **Modem per PLC** (Power Line Communications), comunicazioni su linea elettrica (640 kbps-200 Mbps);
- **Modem GPRS, UMTS e HSDPA**, spesso integrati nei cellulari o come PC card;
- **Modem in banda base**, utilizzati per scopi industriali su linee private o noleggiate, che mettono in comunicazione diretta due utenti su doppino telefonico.

Ognuno dei modem suddetti può essere inoltre **interno** o **esterno** al DTE. Tra i modem **esterni**, in base al tipo di collegamento al DTE, si distinguono:

- **Modem seriali**, collegati con cavo seriale tramite interfaccia RS-232 o USB;
- **Modem paralleli**, collegati con cavo parallelo alle porte LPT1 o LP2 (vedi Interfacce parallele).

Tra i modem **interni** si distinguono invece:

- **Modem PCI**, che lavorano appunto sul BUS PCI (Peripheral Component Interconnect);
- **Modem PCMCIA, PC card o Express card**, utilizzati esclusivamente nei portatili.

Modem in banda fonica Si utilizza quando si presenta la necessità di trasmettere i segnali digitali sulla linea telefonica e viceversa. Occorre notare che la banda disponibile sulla linea telefonica è solamente di $4kHz$, il che rende inefficiente la trasmissione del segnale digitale su di essa, in particolare per via dell'Attenuazione delle alte frequenze e per la scarsissima velocità di trasferimento. Un modem fonico opera dunque una Modulazione digitale volta a comprimere la banda dei segnali emessi dal DTE. Di seguito alcuni standard delle tecniche d'interfacciamento, stabiliti dalla CCITT:

- FSK V.21: primo modem al mondo, risalente ai primi anni '80;
- QAM V.29;
- QAM V.32, che utilizza in realtà la TCM, ed implementa la soppressione dell'eco.
- Modem V.34: utilizzato per collegamenti in cui entrambe le terminazioni della linea sono analogiche, sfrutta completamente la banda disponibile;

[5] Si noti che il concetto di valore quadratico medio non coincide con quello di scarto quadratico medio: si veda it.wikipedia.org/wiki/Valore_efficace

[6] Non si confonda il baud con i $bps = bit/sec$: un simbolo può essere composto da più bit.

- Modem V.90: modem asimmetrico pensato per migliorare il V.34 dando la priorità alla velocità di ricezione piuttosto che a quella di trasmissione;
- Modem V.92: si tratta dello standard oggi più utilizzato, che ha introdotto nuove funzionalità quali:
  - *quick connect*, che riduce notevolmente il tempo di negoziazione dei parametri per la connessione;
  - MOH *Modem On Hold*, che consente di interrompere temporaneamente la connessione;
  - PCM upstream, che permette di effettuare trasmissioni digitali a più alta velocità (fino a $48kbit/s$) sulle linee telefoniche analogiche.

1.8 Altri dispositivi

1.8.1 Ripetitore

Dispositivo di rete che si limita a ripetere i pacchetti che gli arrivano. Si utilizza quando ci si scontra con i limiti fisici all'estensione della LAN: le reti collegate possono in tal caso essere viste, da un punto di vista logico, come una rete unica.

1.8.2 Hub

Uno hub è un dispositivo di rete che funge da nodo di smistamento dati di una una Rete a dorsale o in una Rete a stella. Poiché non è in grado di reinviare i pacchetti se non in broadcast, è attualmente impiegato in misura molto minore rispetto allo Switch.

1.9 Interfacce hardware

Dal punto di vista fisico, un'interfaccia è caratterizzata da un canale di trasmissione, identificato da un mezzo trasmissivo (ad esempio un cavo), due connettori e due porte o *slot* poste agli estremi della trasmissione; dal punto di vista logico, da una modalità di trasmissione (seriale o parallela).

1.9.1 Interfacce parallele

Le interfacce parallele trasmettono segnali da più pin in contemporanea.

Interfaccia Centronics Ormai obsoleta, sostituita in gran parte dei casi dall'interfaccia USB, originariamente monodirezionale, è stata impiegata soprattutto per collegare i DTE alle stampanti, ma più di recente ne è stato sviluppato uno standard bidirezionale che permette anche il collegamento di dispositivi di input. Tale interfaccia consente di trasferire 8 bit in parallelo nello standard **TTL**[7]. La porta parallela del DTE è un connettore femmina detto "a vaschetta" o DB 25, con 25 pin, mentre sulle periferiche è presente un connettore differente, chiamato appunto Centronics, dal nome del primo costruttore. Alle due porte corrispondono chiaramente due diversi connettori maschio.

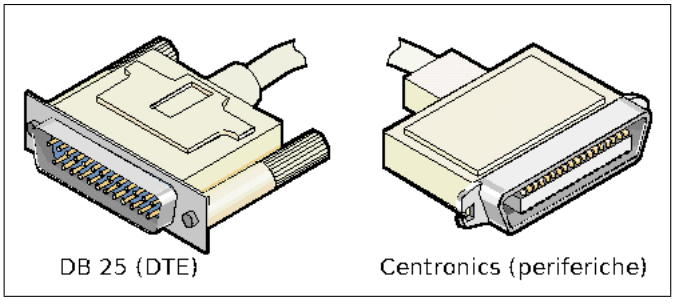


Figura 14: I due diversi connettori maschio dell'interfaccia parallela

Sul DTE si trovavano tipicamente da una a tre porte parallele, dette **LPT** (*Line Printer Terminal*) 1, 2 e 3, a ciascuna delle quali sono assegnati uno specifico interrupt (IRQ 7 per LPT1) e tre indirizzi riservati contigui:

- il **registro dati**, contenente gli 8 bit da trasmettere;

[7] Transistor-Transistor Logic: prima tecnologia di circuiti integrati diffusa su larga scala.

- il **registro di stato**, accessibile in sola lettura e solo per cinque dei suoi bit, volti a descrivere lo stato della stampante;
- il **registro di controllo**, in sola scrittura, che mette a disposizione altri 4 bit.

1.9.2 Interfacce seriali

Le interfacce seriali trasmettono da un solo pin alla volta.

RS-232 L'RS-232 è uno standard che permette la realizzazione di una trasmissione seriale tra un DTE e un DCE, in modalità sia sincrona che asincrona. Dal momento che il numero di linee effettivamente utilizzate varia sensibilmente a seconda del tipo di collegamento e dei modem eventualmente impiegati, per questa interfaccia esistono due diversi tipi di connettore: quello a 25 pin e quello ridotto, a 9 pin, sufficiente per molte applicazioni.

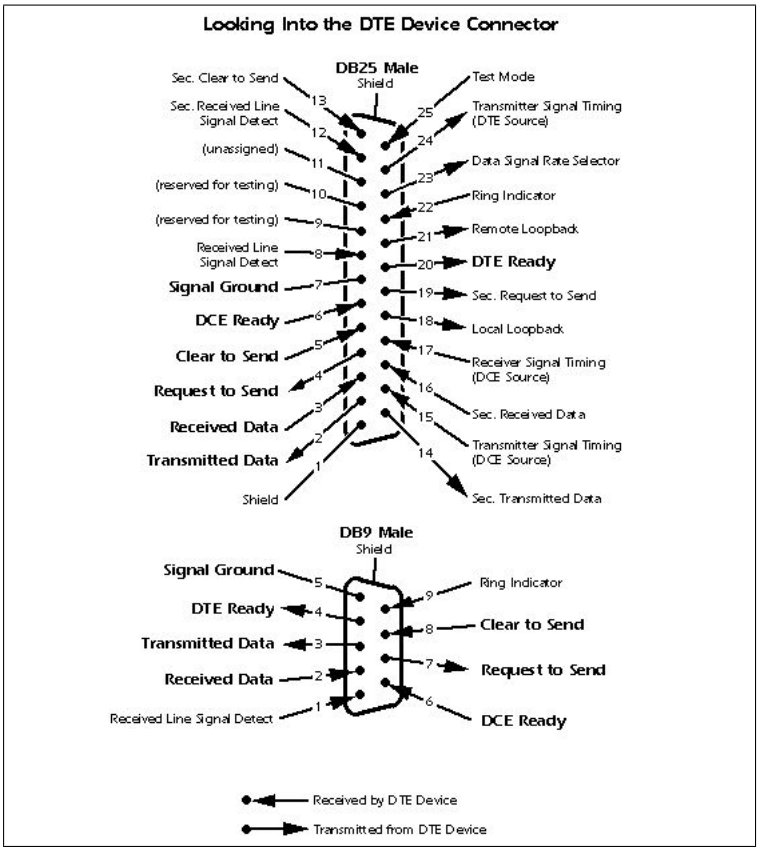


Figura 15: Uso di ogni linea nei due tipi di connettore RS-232

USB Ideata nel 1995 da un consorzio di costruttori tra cui Intel, Compaq, Digital e Microsoft, l'USB (*Universal Serial Bus*) ha soppiantato le interfacce precedentemente descritte. Essa risulta infatti vantaggiosa, oltre che in termini di velocità e versatilità, poiché può fornire direttamente l'alimentazione alle periferiche e consente di creare *collegamenti a caldo*, senza necessità di spegnere le macchine, le quali riconoscono automaticamente le periferiche (interfacce *plug-and-play*). I connettori USB sono molteplici (tipi A, B e C con rispettive varianti miniaturizzate), ma tutti con quattro poli ed uguali funzionalità. Un'estensione dell'USB, chiamata USB-OTG (On-The-Go), consente a una singola porta di fungere sia da dispositivo sia da controllore, semplificando le connessioni USB dei piccoli dispositivi. Il sistema USB è asimmetrico: consiste in un singolo gestore e molte periferiche collegate ad albero, attraverso Hub. Supporta fino a un massimo di 127 periferiche per gestore, ma nel computo vanno inclusi anche gli hub e il gestore stesso. Attualmente, la massima velocità di trasmissione reale raggiunta è 7,2 Gbps (versione USB 3.1).

IEEE 1394 La IEEE 1394, ideata da Apple nel 1968 per essere utilizzata nei PC e nota anche con i nomi commerciali **FireWire** ed **iLink**, attribuitile rispettivamente dalla stessa Apple e da Sony, è un'interfaccia bidirezionale in grado di gestire fino a 63 dispositivi sulla stessa linea ad alta velocità, miscelando dati sincroni ed asincroni. Come la USB, consente di collegare e scollegare i dispositivi a caldo tramite due diversi tipi di connettore, l'uno a quattro pin, senza alimentazione, l'altro a 6,

con alimentazione da 8 a 30 V. Il limite principale di tale interfaccia è la portata, limitata a pochi metri, portati a 100 con lo standard IEEE 1394b.

RS422 Utilizzata principalmente per realizzare collegamenti punto-a-punto tra due apparecchiature -siano esse DTE o DCE- con alta immunità ai disturbi anche a distanze considerevoli (tipicamente fino a 1200 m) e a velocità anche superiori a 10 Mbps, è uno standard molto diffuso specie in ambito industriale. Prevede, per ogni coppia di fili, trasmissione unidirezionale e non reversibile. Pertanto, per realizzare una connessione Full-Duplex, si utilizzano due coppie di fili.

1.10 Mezzi trasmissivi

Le diverse reti utilizzate per l'accesso ad internet sfruttano mezzi trasmissivi differenti.

1.10.1 Cavo coassiale

Cavo originale delle reti Ethernet, costituito da un filo di rame ricoperto da un materiale dielettrico, quindi da una calza in rame e una guaina in polietilene. Sulla base del diametro, se ne distinguono due varianti:

- thick (RG-8), di diametro 0.4 cm;
- thin (RG-58). di diametro 0.25 cm, che usa un connettore a T, tipico delle vecchie LAN (si veda in particolare la sezione Rete a dorsale).

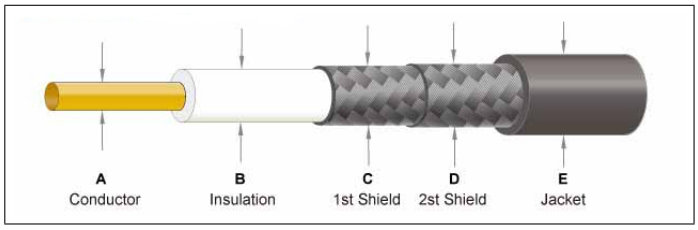


Figura 16: Sezione di un cavo coassiale.

1.10.2 Doppino telefonico

Un *doppino ritorto* (detto anche *coppia bifilare*) è un tipo di cablaggio composto da una coppia di conduttori in rame isolati ritorti, utilizzato nella **rete di accesso**[8] alla **PSTN** (*Public Switched Telephone Network*). I doppini sono utilizzati anche, in un intreccio di quattro coppie, per trasmettere dati in una rete locale, attraverso il protocollo Ethernet.

1.10.3 Cavo UTP

Unshielded twisted pair: evoluzione del doppino telefonico, è costituito da più doppini intrecciati. É soggetto a disturbi elettrici, in particolare se il segmento è molto lungo, poiché agisce come un'antenna, ma è vantaggioso in termini economici.

1.10.4 Cavo STP

Shielded Twisted Pair: risente dei disturbi elettrici in misura minore del cavo UTP, ma è più costoso e difficile da stendere.

1.10.5 Fibra ottica

Le fibre ottiche sono filamenti di materiali vetrosi o polimerici, realizzati in modo da poter condurre al loro interno la luce (propagazione guidata). Ne esistono due tipologie, le *monomodali*, in cui la sorgente è un laser, e le *multimodali*, in cui la sorgente è un LED. Disponibili sotto forma di cavi, presentano numerosi vantaggi: sono flessibili, immuni ai disturbi elettrici ed alle condizioni atmosferiche più estreme e poco sensibili alle variazioni di temperatura. Le architetture di rete che utilizzano la fibra ottica come mezzo trasmissivo sono indicate genericamente con l'acronimo **FTTx** (*Fiber To The x*). In particolare, la sigla FTTH (*Fiber To The Home*) indica un tipo di rete in cui

[8] Termine con cui si indica la parte di rete destinata al collegamento fra la sede dei singoli utenti finali fino alla prima centrale di commutazione, e più in generale al collegamento tra un utente e il suo provider.

il collegamento in fibra ottica raggiunge la singola unità abitativa. È la soluzione più costosa, ma garantisce la massima velocità di trasmissione. Elementi principali di una rete FTTx sono:

- **OLT** (*Optical Line Termination*): gestisce il flusso di dati; si trova presso il provider;
- **ONT** (*Optical Network Termination*) ed **ONU** (*Optical Network Unit*): interfacce di rete presso l'utente finale.

Reti AON Le reti AON (Active Optical Network) sono strutture P2P (point-to-point), nel senso che ogni utente ha un tratto di fibra proprio, che giunge direttamente al suo ONT. Nelle AON si utilizzano componenti attivi, come amplificatori, ripetitori, router o switch. La loro topologia è solitamente a stella (vedi Rete a stella). Garantisce, a costi elevati, la massima velocità di trasmissione.

Reti PON Le reti PON (Passive Optical Network) utilizzano solo componenti passivi e sono caratterizzate da una topologia ad albero (vedi Rete ad albero). In esse, tratti di fibra vengono condivisi tra più utenti, e solo alla fine uno splitter ottico suddivide il segnale in più segnali uguali ma di potenza minore in modo da distribuirlo.

1.11 Protocolli di primo livello

1.11.1 PDH

Plesiochronous Digital Hierarchy: tecnologia utilizzata nelle reti di telecomunicazione per trasportare grandi quantità di dati su apparecchiature di trasporto digitali. Rappresenta il primo metodo di Multiplazione per trasmettere molti (per l'esattezza 30) canali contemporaneamente. Tramite un multiplexer TDM si uniscono i diversi canali. Poiché questi possono funzionare a bitrate differenti, il multiplexer si trova a dover inserire bit aggiuntivi (i cosiddetti *dummy bits*) per compensare la differenza e rendere sincrono il flusso in entrata al demultiplexer ricevente, che li riconosce e li elimina. Il PDH è incapace di monitorare le prestazioni della rete e garantire buone performance per trasferimento contemporaneo di audio, video e dati. Problemi di temporizzazione (il termine *plesiochronous* significa letteralmente "quasi sincronizzato") portano a preferire l'SDH.

1.11.2 SDH

Synchronous Digital Hierarchy: protocollo usato per la trasmissione di fonia e dati su fibra e rete elettrica, anch'esso ha il compito di aggregare flussi di dati con bitrate diversi e spedirli tutti insieme a grandi distanze. A differenza del PDH, prevede che tutti gli elementi della rete siano sincronizzati da uno stesso clock. Consente inoltre di trasferire informazioni essenziali per la corretta gestione della rete, permettendo di raggiungere elevatissimi livelli di qualità del servizio. Non presenta limiti di distanza e ad oggi offre velocità fino a 140Gb/s. L'unico vincolo è dovuto alla multiplazione TDM, che fornisce ad ogni utente una capacità costante nel tempo. Diffuso in tutto il mondo tranne che in Nord America, dove si utilizza un protocollo analogo, il **sonet**

1.11.3 DSL

Il termine DSL (Digital Subscriber Line) indica una famiglia di tecnologie che fornisce trasmissione digitale di dati su Doppino telefonico, comunemente utilizzata nella connessione ad Internet da utenza domestica nella sua specifica più diffusa, l'**ADSL** (Asymmetrical DSL). Il protocollo ADSL sfrutta completamente la banda passante del doppino telefonico, molto più ampia dei 4kHz utilizzati normalmente in fonia, utilizzando due tecniche di modulazione: la CAP (Carrierless Amplitude Phase, variante della QAM) e la DMT (Discrete Multi Tone). Con un filtro DSL, spesso chiamato *splitter*, le bande di frequenza vengono tripartite, consentendo di utilizzare allo stesso tempo un'unica linea telefonica sia per il servizio ADSL che per le chiamate telefoniche. L'ADSL è generalmente installata solo per brevi distanze dalla centrale telefonica (l'ultimo miglio), o comunque meno di 4 km.

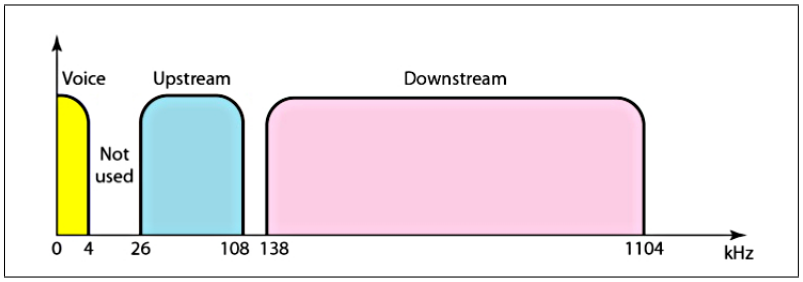


Figura 17: Tripartizione della banda tramite splitter

Le velocità teoriche ottenibili sono dell'ordine degli 8Mbit/s per quel che riguarda il downstream e 800kbit/s per quanto riguarda l'upstream, ma lo stato delle linee e della bassa qualità del doppino le porta a circa 1,5Mbit/s in download e 256kbit/s in upload. Nonostante il fatto che le linee guida siano dettate dallo standard ANSI T1.423 Issue 1, categorie 1 e 2, questa tecnologia non é ancora totalmente standardizzata: ogni produttore di modem per ADSL propone la propria variante.

2 Livello di collegamento

In inglese *Data Link Layer* (DLL), il secondo livello del Modello di riferimento ISO/OSI si occupa di:

- raggruppare in frame i bit da inviare;
- modulare la multiplazione per l'accesso condiviso fra più utenti al canale fisico per evitare conflitti;
- controllare gli errori di trasmissione e gestirli;
- gestire il flusso di dati.

2.1 Sottolivelli

Il DLL, secondo lo standard IEEE 802, in caso di reti LAN brodcast, è diviso in due sottolivelli:

2.1.1 MAC

Il livello MAC (*Media Access Control*) è diverso per ciascun tipo di LAN e disciplina l'accesso contemporaneo di molti nodi ad un solo canale di comunicazione condiviso, evitando e gestendo le collisioni.

Indirizzo MAC A questo livello si pone l'indirizzo MAC, ossia l'indirizzo fisico della macchina, non individuabile dall'esterno, utilizzato per l'instradamento diretto in reti locali, ovvero per raggiungere un host da una stessa sottorete passando per il solo livello 2.
La conversione degli indirizzi di livello 3 (es. IP) in indirizzi MAC di livello 2 è in genere eseguita dal protocollo ARP, mentre la procedura opposta da protocolli come RARP e DHCP.

2.1.2 LLC

Il livello LLC (*Logical Link Control*), posto tra livello MAC e Livello di rete, controlla il flusso di dati e gestisce gli errori, fornendo un'interfaccia unica per tutti i tipi di LAN. I protocolli PPP e HDLC fanno parte di questo sottolivello.

Standard I dati ricevuti dal livello superiore vengono incapsulati sottoforma di *frame LLC* ed inviati a quello inferiore (MAC), che si occuperà di trasmetterli sul mezzo fisico prescelto. I frame LLC sono costituiti dall'indirizzo sorgente, di destinazione, un campo di controllo ed infine i dati.
In base all'implementazione, il LLC prevede 3 diversi servizi fornibili al livello superiore:

- **LLC1**: servizio Connectionless, non è prevista alcuna forma di *conferma*, di *correzione errori* ne di *controllo del flusso*;
- **LLC2**: servizio Connection-oriented unicast (punto-punto) e simmetrica. Prevede meccanismi di *correzione errori* e di *sequenziamento dei dati*. Analogo ad altri protocolli di livello 2 come l'HDLC;
- **LLC3**: servizio alternativo al LLC1 in quanto è Connectionless, ma prevede una *conferma di ricezione* (acknowledge - ACK) per i frame inviati e garantisce la *consegna ordinata* dei dati.

2.2 Ethernet

É una delle tecnologie per il collegamento LAN più utilizzate al mondo, posta a metà fra il primo e il secondo livello (più in particolare nel sottolivello MAC) del Modello di riferimento ISO/OSI.
L'interfaccia Ethernet ha funzione di:

- Incapsulamento e decapsulamento dei dati;
- Codifica e decodifica Manchester dei bit per trasmettere il clock insieme ai dati. Questa codifica garantisce la transizione del segnale elettrico in ogni bit trasmesso, il che permette al ricevitore di agganciare il clock del trasmettitore nella fase di preambolo e ricevere il messaggio nel modo giusto.

2.2.1 IEEE 802.3

Le reti locali appartenenti a questo standard adottano uno accesso al bus di tipo CSMA/CD. Lo standard 802.3 prevede diverse varianti del livello MAC:

- **10base5**: prima versione del MAC, prevede l' uso di Cavo coassiale thick RG-8 da 50 Ohm. La velocità è di 10 Mbps e la lunghezza massima di un singolo cavo è 500 m: distanze superiori richiedono l'utilizzo di Bridge locali o remoti che operano su trame generate al livello MAC. La connessione delle stazioni impiega i cosiddetti *connettori a vampiro*;
- **10base2**: creato per evitare i problemi relativi alla difficile manipolazione dei cavi thick, sfrutta cavi coassiali sottili tipo RG-58, molto più flessibili. La lunghezza massima di un segmento è 185 m, con 30 stazioni collegabili ad un singolo segmento. I limiti di questo metodo sono la difficoltà nel localizzare danni nei cavi e interferenze dovute a cavi eccessivamente ripiegati su loro stessi;
- **10baseT**: creato per semplificare la realizzazione delle reti tramite sistemi di cablaggio strutturato, utilizza cavi UTP ed ha una struttura topologica a stella con hub connessi in parallelo. La lunghezza massima di un tratto è di 100 m;
- **10baseFOIRL**: impiega la fibra ottica al posto del Cavo coassiale thick.
- **10baseF** insieme degli standard di ricezione per la fibra ottica. Comprende **10baseFP** (velocità: 10mb/s, topologia a stella, passiva) **10baseFB** (con dorsale fra i ripetitori) e **10baseFL** (topologia point-to-point o stellare).

2.2.2 Switched Lan

Sono LAN Ethernet caratterizzate dall'impiego di Switch, che risolve i problemi del metodo di accesso CSMA/CD minimizzando le collisioni. É una tecnologia con bassi costi di installazione e manutenzione e la migrazione da LAN a switched LAN necessita della sola sostituzione degli apparati attivi, cioè mantiene il cablaggio inalterato.

2.2.3 Ethernet framing

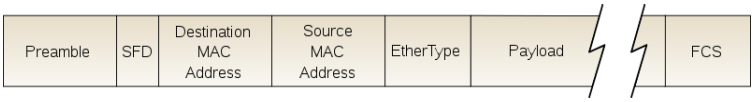


Figura 18: Frame ethernet di tipo 2 (fra i più comuni).

Nonostante esistano diversi tipi di Ethernet, tutte le varianti condividono la struttura del frame, strutturato come segue:

- *Preamble* (preambolo): sette byte ognuno dei quali ha valore `10101010`, servono a svegliare il ricevente ed a sincronizzarlo con l'emittente, non fa quindi parte del vero frame ma avvisa che a breve ne arriverà uno;
- *Start Frame Delimiter* (SFD): ulteriore byte non appartenente al frame, ha valore `10101011` se il messaggio in arrivo è importante, altrimenti ha lo stesso valore dei byte del preambolo. É protetto da codifica Manchester;
- *Destination MAC Address* (indirizzo destinazione): di 6 byte, contiene l'indirizzo fisico del ricevente; se esso non corrisponde il frame viene scartato al Livello fisico.
- *Source MAC Address* (indirizzo sorgente): di 6 byte, contiene l'indirizzo fisico del mittente.
- *Ether Type* (tipo): di 2 byte, indica il tipo di protocollo di rete in uso o, nello standard IEEE 802.3, la lunghezza del campo dati.
- *PayLoad* (campo dati): da 46 a 1500 byte, contiene i dati reali, i dati troppo grandi vengono divisi in più frame mentre ai dati troppo piccoli viene aggiunto un riempitivo (padding) della lunghezza necessaria.
- *Frame Check Sequence* (controllo a ridondanza ciclica): di 4 byte, verifica la presenza di errori, il ricevente calcola il FCS tramite un algoritmo per poi confrontarlo con quello presente nel frame.

2.3 Tipi di trasmissione

Una trasmissione può essere asincrona o sincrona, quest'ultima orientata al bit o al carattere. Inoltre, a seconda del ruolo delle due stazioni, si può suddividere il flusso trasmissivo in simplex, half duplex e full duplex.

2.3.1 Asincrona

In una comunicazione asincrona il ricevente sta a riposo finché non riceve un segnale di start, che precede il messaggio. Alla fine del messaggio viene inviato un segnale di stop che, se non seguito da altri messaggi, rimanda a riposo il ricevente. L'asincronia è dovuta al fatto che l'intervallo di tempo tra l'invio di due caratteri non è precisabile. Questo metodo è vantaggioso in caso di comunicazioni irregolari senza la precisione di una comunicazione sincrona, ma il segnale di start e quello di stop rappresentano circa il 30% dei bit trasmessi.

2.3.2 Sincrona

Con il termine *sincrona* si indica una comunicazione scandita da un clock, che sincronizza trasmettitore e ricevitore; i dati vengono raggruppati in blocchi e trasmessi secondo il tempo dato dal clock. Il ricevitore ha sia il sincronismo a bit, cioè è in grado di estrarre singoli bit dal flusso di dati in ricezione, sia il sincronismo di carattere, può cioè estrarre interi caratteri dal flusso di bit, cosa che, generalmente, viene assicurata da alcuni caratteri inviati all'inizio della trasmissione.
Vi sono vari metodi per assicurare la sincronizzazione, ad esempio il PLL (Phase Lock Loop, molto utilizzato) o l'AMI.

Orientata al carattere La trasmissione orientata al carattere, utilizzata per le informazioni testuali, come i file in ASCII, prevede la lettura dei bit a gruppi di otto.
La sincronizzazione è ottenuta tramite una serie di caratteri di controllo SYN, il primo dei quali viene ricercato spostandosi di un bit alla volta. Una volta raggiunta la sincronia si ricerca il carattere di controllo STX che sancisce l'inizio della trasmissione, terminata dal carattere ETX.
Per evitare che i dati della trasmissione vengano scambiati per caratteri di controllo si fa precedere ai caratteri STX e ETX, un altro carattere di controllo chiamato DLE (tutti 1 o tutti 0 a seconda del sistema) e in invio viene eseguito il *byte stuffing* dei dati: eventuali occorrenze del carattere DLE nei dati vengono duplicate in modo da renderle riconoscibili.

Orientata al bit Questa tecnica è preferibile sia quando i dati non sono organizzati in caratteri, sia, in generale, quando si preferisce non dipendere da caratteri di controllo. La sincronizzazione si basa su degli *idle bytes* (`011111111`), inviati nei periodi di inattività, e dei *flag bytes* (`01111110`) che indicano l'inizio e fine della trasmissione, il rischio di simulare il flag nella trasmissione è scongiurato dall'utilizzo del *bit stuffing*: durante l'invio dei dati, ogni volta che si incontrano 5 bit uguali a 1 viene aggiunto uno 0 che verrà poi rimosso dal ricevente.

2.3.3 Simplex

Flusso monodirezionale. Le trasmissioni radiofoniche ne sono un tipico esempio.

2.3.4 Half-Duplex

Flusso bidirezionale in cui la trasmissione può avvenire in un solo senso alla volta. Le ricetrasmittenti lavorano in questa maniera.

2.3.5 Full-Duplex

Flusso bidirezionale in cui la trasmissione può avvenire in ambo i sensi contemporaneamente, come nella rete telefonica.

2.4 Encoding

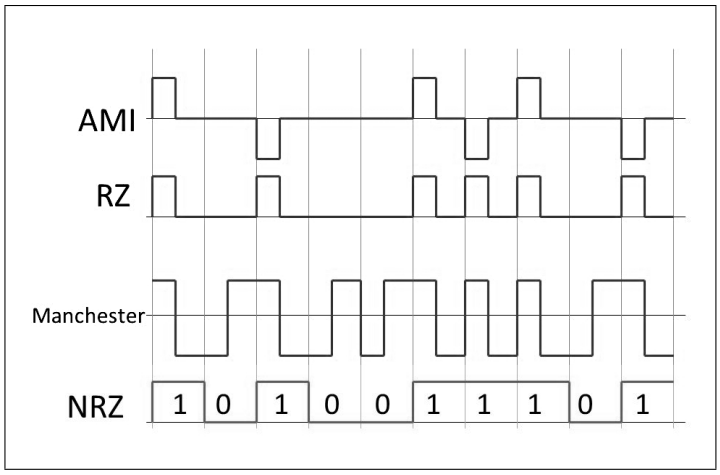


Figura 19: Principali codifiche a confronto.

2.4.1 NRZ

Not Reduced Zero: codifica molto semplice dove lo stato digitale 1 viene rappresentato da un segnale alto mentre un lo stato 0 viene rappresentato da un segnale basso. Richiede circuiti semplici ed ha una buona resistenza agli errori, il problema è che su lunghe trasmissioni si perde la sincronia nella trasmissione di lunghe serie di bit di uguale valore.

2.4.2 RZ

Return to Zero: questa codifica è del tutto analoga all'NRZ, con la differenza però che a metà di ogni impulso il segnale torna sempre a zero; il clock ha quindi frequenza doppia per dimezzare la durata di un impulso, questo metodo non causa desincronizzazione ma ha un più alto rischio di errore. Può essere anche a tre livelli (*RZ bipolare*), ed in tal caso il livello inferiore (-V) rappresenta lo 0 logico, il livello superiore (+V) l'1 logico e a metà di ogni impulso si ritorna al livello intermedio (0), che non rappresenta di per sé alcun valore logico.

2.4.3 Manchester

Come nella RZ, la frequenza del clock è raddoppiata. Allo 0 logico corrisponde una transizione dal basso verso l'alto, mentre all'1 logico una transizione dall'alto verso il basso. In tutti e due i casi la transizione avviene a metà dell'impulso.

2.4.4 AMI

Alternate Mark Inversion: come la RZ bipolare, utilizza tre stati, con la differenza che lo 0 logico corrisponde allo stato 0 mentre l'1 logico si alterna fra +V e -V. Questa codifica è usata nella PCM.

2.4.5 Scrambling

Lo scrambling è un metodo che consente di risolvere alcuni problemi nelle trasmissioni di lunga distanza, consiste nel mescolare in modo "intelligente" i bit per mantenere attiva la linea, è utilizzata nella codifica 2B1Q (two Binary, one Quaternary).

2.5 Controllo degli errori

Esistono 3 tipi di errore:

- single-bit (un solo bit cambia di valore);
- multiple-bit (più bit non consecutivi cambiano di valore);
- burst (più bit consecutivi cambiano di valore).

Per rilevare gli errori esistono diversi metodi, che consistono principalmente nell'aggiunta di bit ridondanti che, in fase di ricezione, dopo la verifica l'integrità del messaggio, vengono cancellati. I principali algoritmi di controllo sono illustrati di seguito.

2.5.1 VRC

Il VRC (Controllo di Ridondanza Verticale) consiste nell'aggiungere un solo bit di valore 1 al messaggio, in modo tale da rendere pari (o dispari) il numero di bit con tale valore per verificare se il messaggio è alterato. Questo metodo é semplice e pratico ma gestisce pochi errori poiché se gli errori sono tali da non cambiare la parità non funziona.

2.5.2 LRC

L'LRC (Controllo di Ridondanza Longitudinale) è un VRC bidimensionale. Assicura una migliore gestione di errori di tipo multiple-bit e burst ma non è sufficiente robusto per le transazioni di bit.

2.5.3 CRC

Il CRC (Controllo di Ridondanza Ciclica) consiste nel creare, a partire dal file che verrà trasmesso con il messaggio, secondo un dato polinomio generatore, un numero in binario. Questo permette di avere un ottimo controllo degli errori, di qualsiasi tipo essi siano.

2.6 Protocolli di secondo livello

2.6.1 BSC

Introdotto dalla IBM, il *Binary Synchronous Communication* è un protocollo sincrono orientato al carattere. Il flusso trasmissivo è di tipo Half-Duplex con velocità tra 1200 e 19200 bps.
Il frame è composto da circa cento byte, divisi tra messaggio da trasmettere e caratteri di controllo. La codifica binaria utilizzata può essere ASCII, EBCDIC (Extended Binary Coded Decimal Interchange Code) oppure SBT (Six Bit Transcode).
In base alla rete su cui opera, il BSC si suddivide in:

- BSC1: rete dedicata punto-punto;
- BSC2: rete commutata punto-punto;
- BSC3: rete multipunto.

Nei due casi di rete punto-punto, il trasmettitore invia caratteri di sincronismo (PAD o SYN) seguiti da ENQ; dato che i DTE sono sia trasmettitori che riceventi, possono entrare in contesa qualora entrambi cerchino di trasmettere nello stesso momento: uno dei due diventerà una stazione primaria che ripete l'invio, mentre l'altro sarà una stazione secondaria e dovrà rinunciare. Il ricevente risponderà con ACK se è pronto, oppure NAK se non può acquisire i dati. Il collegamento viene terminato con il messaggio EOT.
Nel caso di rete multi-punto l'elaborazione centrale effettua un'interrogazione ciclica (*pollic*) per individuare il terminale a cui collegarsi (il protocollo deve conoscere gli indirizzi del destinatario).

Tipo carattere	Carattere	Commento
Sincronismo	PAD	Sinc. di carattere
	SYN	Sinc. di bit
Interrogazione	ENQ (enquiry)	Richiesta trasmissione
Controllo	DLE	Il carattere successivo va interpretato come char di controllo
Risposta	ACK0 ACK1	Inviati alternativamente dal ricevitore, preceduti da DLE0 per ACK0 e così via
	NAK	Risposta negativa ricevitore
	WAK	Ricevitore non pronto a ricevere (DLE+3B)
	RVI (Rev. interrupt)	Il ricevitore informa che ha un messaggio ad alta priorità da trasmettere
Testo	STX	Inizio testo messaggio
	SOH	Inizio intestazione (heading)
	ETB	Fine blocco (End Transmission Block)
	ITB	Fine blocco intermedio (Intermediate Transmission Block)
	ETX	Fine del testo (End of Text)
	EOT	Fine trasmissione
Controllo errori	BCC	Block Character Check (ad es. CRC-16)

Figura 20: caratteri di controllo nel BSC

L'efficienza del protocollo BSC non è molto elevata. Ciò è dovuto sia al tipo di trasmissione half-duplex, sia alla presenza di un gran numero di caratteri di controllo, che sottraggono capacità di rappresentazione ai caratteri del messaggio vero e proprio.

2.6.2 HDLC

Il protocollo High Level Data Link Control costituisce lo standard ISO per trasmissioni sincrone Full-Duplex; è orientato ai bit e utilizzato su reti di grandi dimensioni.
Prevede 3 tipi di terminali:

- Stazione primaria: detta anche *master*, ha il compito di controllare il collegamento inviando i comandi di controllo;
- Stazione secondaria: agisce in base ai comandi della stazione primaria e può spedire soltanto pacchetti di risposta;
- Stazione combinata: ha le caratteristiche di entrambi i terminali sopra: può inviare sia comandi sia risposte.

La connessione fra mittente e destinatario è detta **bilanciata** se sono entrambi stazioni combinate; al contrario, se vi è una stazione primaria che comunica con una o più stazioni secondarie si parla di connessione **sbilanciata**: in questo caso il protocollo lavora in modalità Half-Duplex ed i messaggi inviati dal master prendono il nome di *command*, mentre quelli delle stazioni secondarie sono detti *response*.
Nello specifico, HDLC può lavorare in 3 diverse modalità:

- **NRM** (Normal Response Mode): connessione half-duplex sbilanciata.
  Le stazioni secondarie possono trasmettere anche senza autorizzazione esplicita del master;
- **ABM** (Asynchronous Balanced Mode): bilanciata full-duplex tra due stazioni paritetiche;

- **ARM** (Asynchronous Response Mode): come NRM ma limitata a due stazioni.

Il protocollo HDLC prevede che, a seconda delle necessità, le stazioni possano scambiarsi *frame* di 3 tipologie:

- **I-frame**: il tipo ***I****nformation* è usato per trasportare i dati dal Livello di rete. Può contenere, in aggiunta, comandi per il controllo del flusso e degli errori;
- **S-frame**: il tipo ***S****upervisory* è usato esclusivamente per controllare il flusso e gli errori;
- **U-frame**: il tipo ***U****nnumbered* fornisce funzioni di controllo aggiuntive, come informazioni per iniziare/terminare la connessione, ma è usato anche per l'invio di dati in modalità *connectionless*.

I frame sono divisi nei seguenti sottocampi:

- **flag**: due sequenze di 8 bit `01111110` utilizzate come inizio e fine della trasmissione. La stessa sequenza viene trasmessa continuamente dalle stazioni in *idle* al fine di garantire la sincronizzazione. La forma del flag rende necessario ricorrere alla tecnica del *bit stuffing* (vedi trasmissione Orientata al bit);
- **indirizzo**: campo di 8 bit che può essere anche esteso previo accordo tra le stazioni: identifica la stazione che ha trasmesso o che deve ricevere il frame;
- **controllo**: 8 o 16 bit contenenti informazioni di controllo o definizione del pacchetto. La struttura di questo campo varia in base al tipo di frame (N.B: il bit a sinistra è il meno significativo):
  - *Information*: la forma è `0SSSPRRR`, dove `SSS` conta i frame trasmessi, `RRR` conta quelli ricevuti.
    `P` è detto bit P/F (*Poll/Final*) e, nelle connessioni sbilanciate, è posto a `1` nel frame in cui il master invita la stazione secondaria a trasmettere (*poll*), la quale utilizzerà `P=1` solo nell'ultimo frame che invia (*final*). Nelle connessioni bilanciate il bit P/F posto a `1` equivale alla richiesta (o alla relativa risposta) di *acknowledgment* del frame;
  - *Supervisory*: la forma è `10TTPRRR`, in cui i primi due bit sono fissi ed identificano il tipo S-frame; `P` ha lo scopo visto in precedenza.
    I due bit `TT` comunicano che:
    00 = *Received Ready*: sono stati ricevuti tutti i frame, la stazione è pronta a ricevere;
    01 = *Reject*: c'è stato un problema di acquisizione, è necessario ritrasmettere tutti i frame a partire da `RRR`;
    10 = *Receive Not Ready*: la stazione non può ricevere;
    11 = *Selective Reject*: invito a rinviare il frame numero `RRR`.
  - *Unnumbered*: la forma è `11MMPMMM`. I possibili messaggi per avviare e controllare la connessione sono mostrati in figura:

Code	*Command*	*Response*	*Meaning*
00 001	SNRM		Set normal response mode
11 011	SNRME		Set normal response mode, extended
11 100	SABM	DM	Set asynchronous balanced mode or disconnect mode
11110	SABME		Set asynchronous balanced mode, extended
00 000	UI	UI	Unnumbered information
00 110		UA	Unnumbered acknowledgment
00 010	DISC	RD	Disconnect or request disconnect
10 000	SIM	RIM	Set initialization mode or request information mode
00 100	UP		Unnumbered poll
11 001	RSET		Reset
11 101	XID	XID	Exchange ID
10 001	FRMR	FRMR	Frame reject

Figura 21: Comandi di controllo più comuni negli U-frame

- **campo informativo**: contiene i dati significativi da trasmettere. La lunghezza è arbitraria in quanto sarà poi il flag di chiusura ad identificare la fine del pacchetto.
  N.B: questo campo è assente nei S-frame;

- **campo FCS** (Frame Check Sequence): 16 o 32 bit utilizzati per rilevare evenutuali errori di trasmissione.

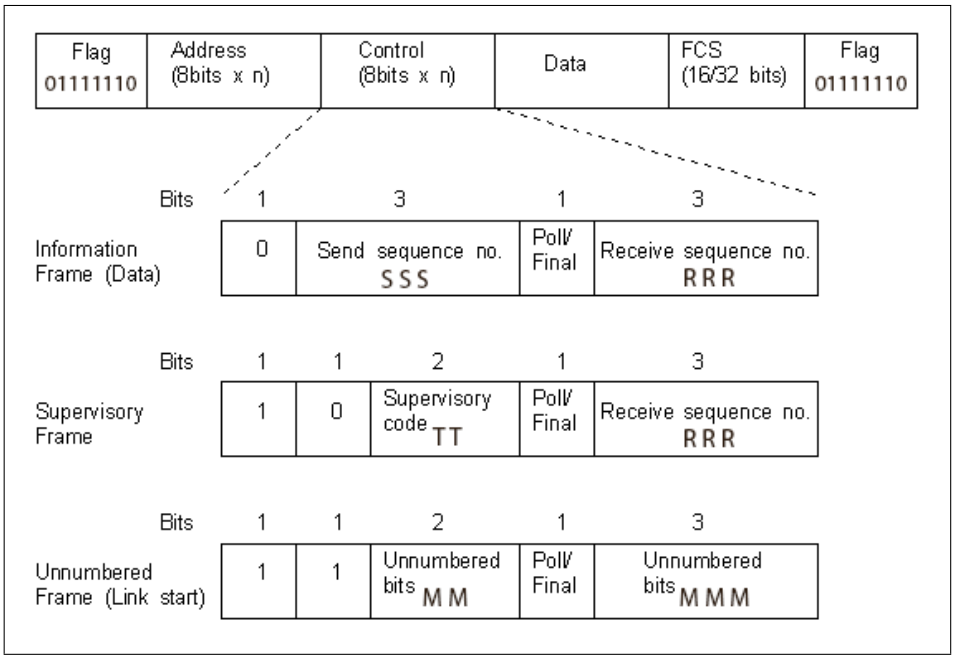


Figura 22: Struttura dei frame in HDLC con differenze nel campo di controllo nei casi I, S ed U

2.6.3 SDLC

HDLC deriva da SDLC (Synchronous Data Link Control), un protocollo definito da IBM negli anni '70. Rispetto ad HDLC, il protocollo SDLC:

- ha il campo FCS di 8 bit;
- supporta configurazioni a loop, come il token ring;
- può lavorare solo in NRM;

2.6.4 PPP

Il Point-to-Point Protocol è, come intuibile, un protocollo usato nelle connessioni punto-punto e trova la sua più ampia diffusione in ambito WAN.
Si può definire un'estensione del protocollo HDLC in quanto il funzionamento è analogo (RFC 1662). Utilizza solo **U-frame**, la cui struttura differisce da quelli in HDLC nei seguenti campi:

- **indirizzo**: i suoi 8 bit sono sempre `11111111` dal momento che le trasmissioni avvengono esclusivamente in *broadcast*;
- **controllo**: solo 8 bit che, mentre in HDLC hanno struttura `11MMPMMM`, in PPP sono del valore fisso `11000000` e rappresentano il comando UI (*unnambered information*), ovvero un messaggio che contiene dati;
- **campo informativo**: contiene i dati da scambiare. La lunghezza massima è 1500 byte e, in caso di messaggi più corti, si colma la differenza facendo uso del **padding**.

Inoltre, il PPP prevede un campo che non compare in HDLC:

- **protocol**: fatto di 1 o 2 *byte*, serve ad identificare il protocollo incapsulato nel frame.

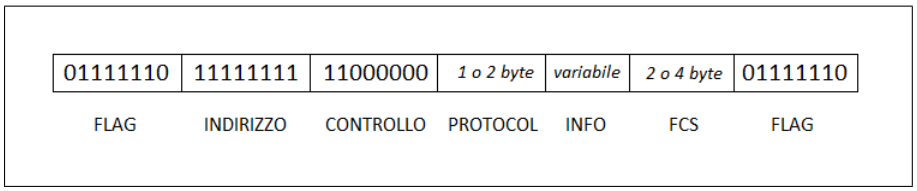


Figura 23: Struttura dei frame nel PPP

Per le operazioni del Livello di collegamento il PPP si avvale del protocollo LCP (Link Control Protocol), mentre per le negoziazioni con il Livello di rete impiega protocolli del tipo NCP (Network Control Protocol).
Di seguito sono specificate le fasi di una connessione in PPP:

1. **Definizione della connessione**: avviene il tentativo di connessione tramite LCP (Link Control Protocol), che provvederà a gestire i pacchetti di configurazione scambiati tra gli host interessati;

2. **Autenticazione** (opzionale): permette alle parti di autenticarsi prima di stabilire la connessione, se lo prevedono;

3. **Configurazione protocollo di rete**: ogni protocollo viene configurato separatamente tramite il proprio NCP (Network Control Protocol). Avviene inoltre la chiusura dei protocolli del Livello di rete;

4. **Terminazione**: la connessione viene interrotta. Può accadere a seguito del fallimento della fase 2, oppure se la connessione cade improvvisamente o se l'utente decide volontariamente di interromperla.

2.6.5 FR

Frame Relay: tecnologia di comunicazione Connection-oriented ad alte prestazioni utilizzata per connettere più reti, costituisce un'evoluzione del protocollo X.25[9], da cui differisce principalmente per la strategia di correzione degli errori, che garantisce maggiore velocità (fino a 2Mbps), ed è il risultato ottenuto nel 1990 da un consorzio appositamente creato (il Frame Relay Forum), cui appartengono, tra gli altri, Cisco, Digital, Northern Telecom e Stratacom. In sintesi, FR va inteso come un modo per inviare informazioni attraverso una WAN, suddividendole in *frames*. Utilizza una forma di Packet switching che ben si presta ad essere usata nelle LAN e in Internet. In una rete FR, gli endpoint sono connessi da un *logical path*, denominato *virtual circuit*.

2.6.6 ATM

Asynchronous Transfer Mode è un protocollo nato negli anni '90 allo scopo di unificare varie tipologie di traffico all'interno di un solo sistema integrato. Per adempiere a tale compito, infatti, è in grado di trasportare contemporaneamente segnali diversi e, di conseguenza, supportare molteplici velocità e tipologie di traffico. Ciò rende ATM ottimale sia nelle connessioni LAN-LAN che in quelle LAN-WAN.
Il consorzio *ATM Forum* ha condotto il processo di standardizzazione del protocollo con il fine di realizzare una rete BISDN (*Broadband-ISDN*), ovvero una rete a banda larga che trasporti sia voce, sia dati. Questo modello prevede, tra le altre cose, la presenza di interfacce **UNI** (*user-network interface*) e **NNI** (*network-network interface*).
Nello specifico, le UNI possono essere pubbliche o private a seconda se l'utente è connesso, rispettivamente, allo Switch ATM di un fornitore pubblico o a quello di una rete privata. La differenza riguarda il mezzo trasmissivo (e quindi il protocollo al Livello fisico) in base alla distanza che separa lo *user* dal *network*: nel caso di UNI pubblica il segnale può viaggiare anche per molti km, mentre nelle UNI private le distanze da coprire sono, di norma, al disotto dei 100 metri.

A differenza delle reti LAN, dove i messaggi viaggiano in *broadcast* con conseguenti problemi di sicurezza ed efficienza, nelle reti ATM i dati vengono inviati *point-to-point*. Inoltre queste ultime non soffrono dei problemi relativi alla condivisione della banda; al contrario, maggiori sono le stazioni a comunicare, maggiore è la capacità della rete.
Un altro vantaggio delle reti ATM è l'indipendenza da un particolare mezzo trasmissivo, un fattore che le rende facilmente adattabili a nuove tecnologie.

Celle ATM L'unità di trasmissione dei dati è un particolare pacchetto detto *cella*; questa ha una lunghezza fissa di 53 byte, di cui:

- 5 byte di ***header***, il quale contiene i seguenti campi:
  - GFC (Generic Flow Control): presente solo nelle celle UNI, è costituito da 4 bit che avrebbero lo scopo di negoziare il controllo del flusso tra le celle di varie connessioni

[9] nota per il futuro revisore: l'X.25 è l'unico argomento che, per carenza di informazioni, abbiamo totalmente tralasciato in questo lavoro: ti invitiamo a scriverne qualcosa

ATM. Tuttavia non esiste uno standard dei valori che dovrebbe assumere e per questo viene posto sempre a `0000`,

  - VPI (Virtual Path Identifier): identifica il percorso virtuale che dovrà percorrere la cella per giungere a destinazione. Questo campo è più lungo nelle celle NNI data l'assenza del GFC,
  - VCI (Virtual Channel Identifier): utilizzato insieme al VPI, identifica il canale virtuale che dovrà percorrere la cella per giungere a destinazione;
  - PT (Payload Type): indica il tipo di messaggio trasportato dalla cella (dati utente o informazioni di servizio),
  - CLP (Cell Loss Priority): indica la priorità del messaggio e viene consultato in caso di congestione nella rete,
  - HEC (Header Error Control): usato per il controllo a ridondanza ciclica (CRC) dello header, ovvero la verifica dell'integrità;

- 48 byte di ***payload***, ovvero il corpo di dati utili.

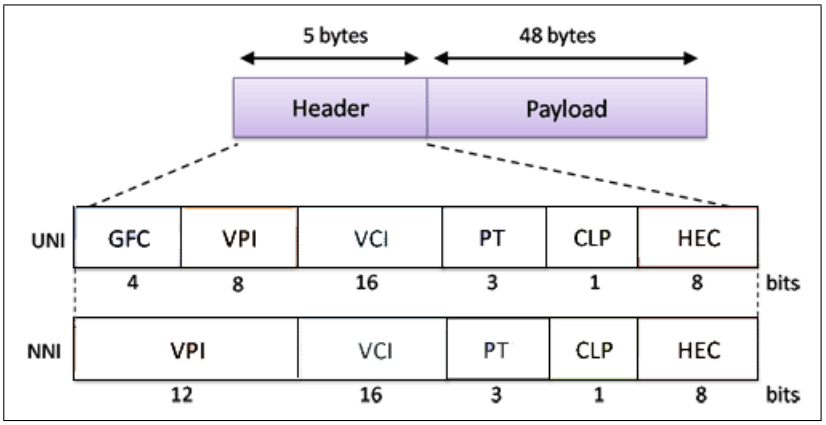


Figura 24: Struttura delle celle in ATM

Il *routing* viene effettuato a monte dello scambio di dati: per prima cosa viene inviato un pacchetto di *handshake* che, passando per i vari switch ATM, calcola progressivamente l'instradamento andando a creare quelli che poi saranno i campi VPI e VCI nello header della cella.
Il resto della trasmissione viaggerà dunque sul percorso così creato ottenendo un Throughput più alto e riducendo *overhead*[10] e Latenza.

ATM utilizza un **PRM** (Protocol Reference Model) raccomandato da CCITT, il quale prevede che il protocollo operi su tre livelli:

- **Physical Layer**: l'equivalente del Livello fisico nella gerarchia ISO/OSI;
- **ATM Layer**: paragonabile ad una parte del Livello di collegamento ISO/OSI, si occupa del routing;
- **AAL** (ATM Adaptation Layer): necessario alla connessione ed alla corretta comunicazione tra la rete ATM e reti non ATM. Qui si effettuano le operazioni di segmentazione/riassemblaggio dei dati.

L'architettura di ATM segue il principio del *Core & Edge*: nei nodi interni (*core*) avvengono soltanto la commutazione e la multiplazione, ovvero operazioni sui due livelli più bassi, mentre i terminali utente (*edge*) operano su tutti i livelli. Questa organizzazione permette di velocizzare notevolmente il trasporto dei dati nei nodi interni della rete, relegando ai nodi esterni alcune funzioni più costose in termini computazionali (ad esempio il controllo degli errori).

[10] Nell'ambito delle reti di telecomunicazioni, col termine *overhead* s' intende quella parte di banda utilizzata per spedire messaggi non contenenti dati utente.

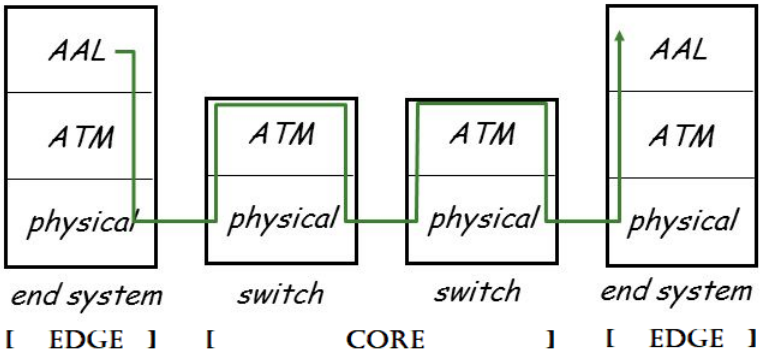


Figura 25: Visualizzazione di come viaggia l'informazione nei nodi di una rete ATM attraverso i tre livelli più bassi.

ATM Adaptation Layer AAL è un livello di adattamento creato per far comunicare i livelli superiori ISO/OSI con i livelli più bassi di ATM e deve per questo supportare i protocolli di trasporto non basati su ATM. Ad esempio, servizi come Gigabit Ethernet, IP e Frame Relay richiedono di essere intermediati.
Le principali attività svolte da questo livello sono:

- *Segmentation and Reassembly* (SAR): i pacchetti di livello superiore vengono presi in carico da AAL il quale decide come segmentarli e riassemblarli in Celle ATM. Questo compito è svolto da un sottolivello di AAL denominato, appunto, **SAR**;
- Gestione degli errori di trasmissione e delle celle mancanti o compromesse. Questo compito è svolto dal sottolivello **CS** (Convergence Sublayer);
- *Timing*, ovvero sincronizzazione tra sorgente e destinazione, e *flow control*, cioè il controllo nel flusso delle celle.

Il livello AAL deve comportarsi in modo diverso in base alle reti con cui ATM si interfaccia. Per rispondere a questa esigenza si è deciso di suddividerle in quattro **classi di servizio** - A, B, C e D - secondo 3 parametri:

- *Timing* necessario o non necessario;
- *Bit rate* costante o variabile (CBR o VBR);
- Connessione di tipo Connection-oriented o Connectionless.

Class A	Class B	Class C	Class D
Circuit emulation	Compressed video	Bursty data	Datagram service
constant Bit Rate	Variable Bit Rate	VBR	VBR
Timing Required	Timing Required	Timing Not Required	Timing Not Required
Connection Oriented	Connection Oriented	Connection Oriented	Connection less
AAL 1	AAL 2	AAL 3/4	AAL --3/4 & AAL 5

Figura 26: Classi di servizio e versioni di AAL corrispondenti.

Ad ognuna di queste classi è stato fatto corrispondere uno specifico tipo di ATM Adaptation Layer:

- **AAL 1**: utilizzato per le applicazioni che richiedono emulazioni di circuito (telefonia), dove il bit rate è costante e la connessione è di tipo *connection-oriented* (**Classe A**).
  Su ogni cella viene effettuato l'incapsulamento SAR che prevede di riservare dal payload un byte in cui inserire i seguenti campi:
  - SN (Sequence Number), costituito da:
    * CSI (Convergence Sublayer Indicator): di 1 bit, individua i limiti dei blocchi di correzione nel Convergence Sublayer,

    - SC (Sequence Counter): di 3 bit, indica il numero della cella;
  - SNP (Sequence Number Protection), costituito da:
    - CRC: di 3 bit, è usato per il controllo ridondanza ciclica,
    - 1 bit di parità;

- **AAL 2**: utilizzato per quelle applicazione che richiedono una classe di servizio VBR-rt (real time VBR, cioè bit rate variabile e timing necessario) come il trasporto di audio-video compresso (**Classe B**).
  Nelle celle AAL 2 il payload non ha dimensione fissa; per ogni cella, la sua lunghezza è dichiarata in un campo apposito di 6 bit detto LI (Length Indicator);

- **AAL 3/4**: si rivolge ad applicazioni che richiedono una classe di servizio VBR-nrt (non real time VBR, cioè bit rate variabile e timing non necessario). Dal punto di vista della connessione, può supportare sia la tipologia *connection-oriented* (**Classe C**), sia quelle di tipo *connectionless* (**Classe D**), sebbene per queste ultime sia ormai stato soppiantato da AAL 5.
  Applicazioni di queste classi prediligono l'integrità dei dati piuttosto che la costanza nel *cell delay*. I controlli di correttezza sul payload e Serial Number vanno quindi a sostituire quei campi che nei casi precedenti erano dedicati a controlli sul timing. I messaggi ricevuti vengono prima incapsulati tra appositi header e trailer, e solo dopo sono segmentati in celle.
  Nelle celle di ALL 3/4 la parte di header deve fornire informazioni sul segmento, numero di sequenza e campo per il multiplexing; il trailer deve contenere l'indicatore di lunghezza ed il campo CRC. Il payload è quindi ridotto a 44 byte;

- **AAL 5**: è stato introdotto, data la complessità di AAL 3/4, per:

  - ridurre l'overhead di elaborazione del protocollo,
  - ridurre il sovraccarico nella trasmissione,
  - garantire l'adattabilità ai protocolli di trasporto esistenti.

  Di contro, AAL 5 diventa più insicuro, assumendo un comportamento simile a quello del sottolivello MAC dell'Ethernet: se il pacchetto consegnato non è valido, non si corregge ma viene automaticamente scartato.

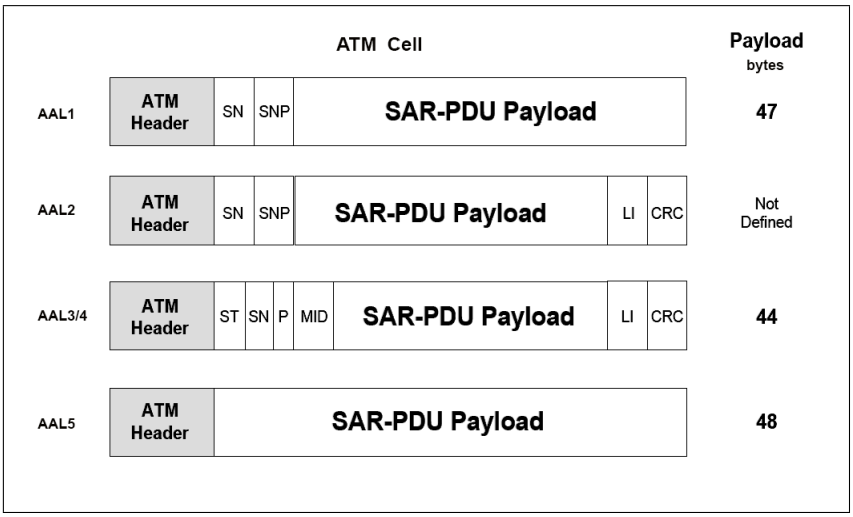


Figura 27: Celle ATM nei diversi tipi di AAL

Il modello di riferimento di ATM prevede anche 3 piani trasversali che, andando ad intersecarsi con i livelli visti in precedenza, costituiscono il cosiddetto modello 3D. Questi piani sono:

- **Control Plane**: piano responsabile della generazione e gestione delle richieste di segnalazione;
- **User Plane**: piano responsabile della gestione del trasferimento dei dati utente;
- **Management Plane**: piano che non si interseca con i tre livelli ATM, ma si compone di due unità:

– *layer management*: gestisce alcune funzioni come il rilevamento di guasti e problemi di protocollo;
– *plane management*: gestisce e coordina le funzioni relative alla comunicazione tra i piani.

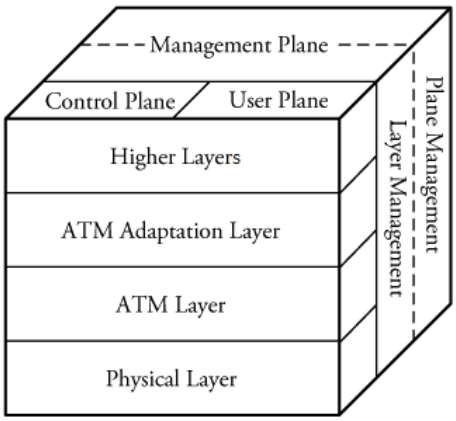


Figura 28: ATM 3D Reference Model

2.7 Dispositivi

Nel secondo livello OSI troviamo dispositivi di rete plug-and-play ed "intelligenti", che non si limitano alla sola replicazione del segnale ma sono in grado di riconoscere, nei segnali elettrici che ricevono dal mezzo trasmissivo, i dati organizzati in frame. Agiscono quindi sui frame ricevuti, gestendoli ed instradandoli, il tutto in modo trasparente all'utente.

2.7.1 Bridge

Un *bridge* (ponte) è un dispositivo di rete munito di porte con cui è collegato a diversi ***segmenti di rete*** (generalmente due o più LAN) da cui riceve dati che instrada selettivamente verso la porta di destinazione. Alla ricezione di un pacchetto, il bridge ne riconosce il tipo di frame, ne estrae gli indirizzi sorgente e destinazione e in base ad essi cerca di capire se il destinatario si trova nello stesso segmento del mittente o meno (***filtering***). Nel secondo caso, cioè se mittente e destinatario non condividono lo stesso bus, inoltra il frame verso il segmento del destinatario (***forwarding***). Se non riesce ad identificare la posizione del destinatario, invece, il bridge inoltrerà il frame su tutte le porte (***Flooding***).
Per instradare i frames, il bridge mantiene una *tabella di forwarding* di indirizzi MAC raggruppati per porta, in modo tale da essere in grado di capire verso quale segmento inoltrare il frame.

Tipologie In base alle tipologie delle due reti si distinguono:

- **Transparent Bridge**: collega due LAN Ethernet o IEEE 802.3;
- **Source Routing Bridge**: collega due LAN Token Ring;
- **Translational Bridge**: collega due LAN di tipo diverso, adattandosi alle caratteristiche specifiche di ognuna.

2.7.2 Switch

Uno *switch* (commutatore) è un dispositivo molto simile al bridge, ma a differenza di quest'ultimo è collegato direttamente agli host ed ha un numero di porte nettamente superiore. La funzione di instradamento è implementata mantenendo in un buffer locale tutti gli indirizzi MAC degli host connessi alla rete, raggruppati per porta dello switch.
L'instradamento è analogo a quello del bridge, ma nel caso in cui lo switch invii il pacchetto a tutte le porte (flooding), il nodo destinatario, ricevuto il pacchetto, risponderà facendo sapere allo switch la sua porta ed il suo MAC address.
Infine, usando lo switch, si riescono ad evitare le collisioni ed è possibile usare la modalità Full-Duplex.

3 Livello di rete

3.1 Terminologia

3.1.1 Rete

Insieme di dispositivi connessi da canali di comunicazione.

3.1.2 DTE

Data Terminal Equipment: qualunque dispositivo che è la sorgente o la destinazione di una comunicazione di dati. Un esempio è il Personal Computer (PC).

3.1.3 DCE

Data Circuit-terminating Equipment o Data Communication Equipment: dispositivo intermedio tra uno o più DTE e il resto della rete; esegue conversioni di segnale, correzione di errori e gestisce il clock dei dispositivi connessi. Può anche essere interno al DTE. Tipicamente è un Modem.

3.1.4 CPE

Customer Premises Equipment: dispositivo terminale connesso direttamente ad una WAN. Rientrano in questa categoria telefoni, Router e Switch di rete.

3.1.5 IS

Intermediate System: dispositivo di rete con funzionalià fino al terzo livello del Modello di riferimento ISO/OSI, come un Router o un Gateway.

3.1.6 Packet switching

Il packet switching, in italiano *commutazione di pacchetto*, fu concepito negli anni '60, nel contesto della guerra fredda, come soluzione al problema di garantire la sopravvivenza di una rete di telecomunicazioni in seguito ad un attacco nucleare. L'idea di base consiste nel suddividere l'informazione in entità elementari, i *pacchetti*, che vengono poi trasmesse ed instradate indipendentemente l'una dall'altra per essere poi riassemblate nel punto di destinazione.

3.1.7 ISP

Internet Service Provider: Organizzazione che fornisce accesso ad Internet.

3.1.8 AS

Autonomuos System: dominio di Routing gestito dallo stesso ISP nel quale vengono applicate le stesse *policy*, può essere di più tipi:

- **Stub** se connesso solo ad un altro AS;
- **Multihomed** se connesso a più AS ma senza permettere il *pass-trough*, ovvero il passaggio di traffico diretto ad un altro AS;
- **Transit** se permette il *pass-trough*.

Strutturare Internet in AS, suddividendo i router in gruppi, si è rivelato necessario innanzitutto perché se Internet fosse una singola rete, il numero dei suoi router sarebbe tanto grande da rendere insostenibile il traffico, difatti il **ritardo** (vedi Qualità delle trasmissioni - Criteri di valutazione in base alle prestazioni) e l'**overhead di gestione** dipendono dal numero di router coinvolti. Inoltre è opportuno che le diverse organizzazioni commerciali siano il più possibile autonome nella gestione delle proprie reti. L'utilizzo degli AS è definito nell'RFC 1930.

ASN Ogni AS è identificato da un ASN (Autonomous System Number) assegnato dall'ICANN ai RIR (Regional Internet Registers), che a loro volta li assegnano alle organizzazioni. Fino al 2007 gli ASN erano costituiti da numeri interi a 16 bit (0-65535), denominati *asplain*, poi sostituiti da numeri a 32 bit detti *asdot* (RFC 4893), nella forma $x.y$, con x e y numeri interi a 16 bit, dove i numeri $0.y$ coincidono con gli asplain.
Gli ASN 0, 23456 e 65535 sono riservati e non possono essere usati dagli operatori. Gli ASN 64512-65534 sono definiti come privati dall'RFC 6996.

3.1.9 Router

Nodo provvisto di procedure specifiche volte ad effettuare le scelte di Routing. Collega più reti o sottoreti dello stesso tipo. Può essere:

- **Interior** se opera all'interno di un AS, utilizza protocolli IGP;
- **Exterior** se opera tra AS differenti, utilizza protocolli EGP.

3.1.10 Gateway

Router che connette due reti o sottoreti di tipo diverso.

3.2 Tipologie di rete cablata

3.2.1 PAN

Personal Area Network: Rete personale che non si estende per più di 10-20 metri. Il termine si riferisce propriamente a reti con connessioni via cavo, ma poiché la gran parte delle reti di dimensioni così piccole è wireless, è spesso utilizzato come sinonimo di WPAN.

3.2.2 LAN

Local Area Network: Rete con un raggio limitato ad una abitazione o un edificio. La prima rete LAN è stata ARKNET nel 1977.

3.2.3 WAN

Wide Area Network: Rete che copre ampie aree geografiche connettendo tra loro più sottoreti locali.

3.2.4 MAN

Metropolitan Area Network: Rete metropolitana caratterizzata da una velocità di trasmissione molto elevata (tipicamente fibra ottica).

3.2.5 GAN

Global Area Network: Internet.

3.3 Tipologie di rete wireless

3.3.1 NFC

Near-Field Communication: Lo scambio di informazioni avviene tramite tag elettromagnetici. Portata: 20cm.

3.3.2 BAN

Body Area Network: Rete che collega dispositivi indossabili, raggio di azione inferiore al metro.

3.3.3 WPAN

Wireless Personal Area Network: Rete di dispositivi personali in un raggio inferiore ai 20 metri, ad esempio stampanti Bluetooth.

3.3.4 WLAN

Wireless Local Area Network: LAN ottenuta tramite tecnologie wireless, ad esempio reti WiFi.

3.3.5 Dispositivi

NIC Network Interface Card: scheda di rete. Svolge tutte le elaborazioni o funzioni necessarie a consentire la connessione dell'apparato informatico ad una rete.

AP Access Point: dispositivo elettronico di telecomunicazioni che, collegato ad una rete cablata, o anche, per esempio, ad un router, permette all'utente di accedervi in modalità wireless direttamente tramite il suo terminale, se dotato di NIC wireless.

3.4 Topologia delle reti

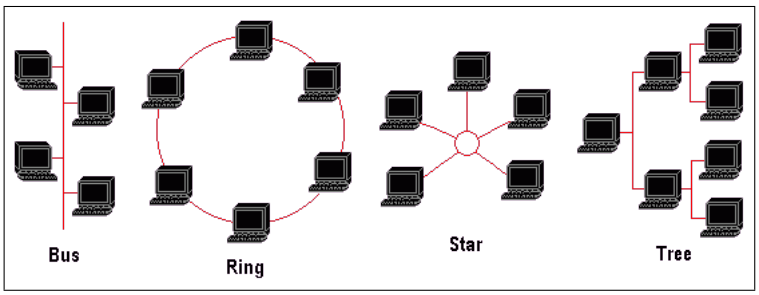


Figura 29: Possibili topologie.

3.4.1 Rete a dorsale

I dispositivi sono connessi tutti ad una via di trasmissione principale detta appunto dorsale. Un'interruzione in qualunque punto della dorsale compromette tutta la rete.

3.4.2 Rete ad albero

La trasmissione avviene in modo gerarchico tra i nodi padre e figlio, fino ad arrivare alla *root* dalla quale dipende tutto il funzionamento della rete.

3.4.3 Rete a stella

Tutti i dispositivi sono connessi ad un *hub* (router o swith di rete), più economico da sostituire in caso di rottura. Inoltre, in caso di danni ad un cavo, viene disconnesso solo un terminale. Questa topologia è tipicamente utilizzata per la realizzazione di reti LAN.

3.4.4 Rete ad anello

Le informazioni vengono passate da un dispositivo all'altro in modo ciclico, la trasmissione è unidirezionale anche se questo si può ovviare con un secondo anello in direzione opposta. Questa topologia era tipica delle LAN TokenRing, ora viene utilizzata principalmente nelle MAN in fibra ottica.

3.4.5 Rete a maglia

In inglese *mesh*, è una rete in cui ogni dispositivo può essere connesso ad ogni altro dispositivo ottenendo un grafo fortemente connesso. É la topologia di rete meno vulnerabile, ma è poco utilizzata nelle reti cablate a causa dei costi. É diffusa invece nelle WLAN, spesso nella versione *ad hoc*, dove i collegamenti nascono e muoiono dinamicamente. In questa topologia il Routing viene effettuato da ogni nodo.

3.5 Grid

Rete di computer incentrata sulla condivisione dinamica delle risorse, nel contesto di calcolo distribuito e HTC (*High Troughput Computing*).
Rispetto ad un vero e proprio cluster di computer, la grid ha una composizione più eterogenea. La condivisione della capacità di calcolo non si limita al software, ma coinvolge anche l'hardware, grazie a librerie *middleware* (*software glue*) che si collocano tra il sistema operativo e lo strato fisico della macchina. La più importante grid europea è EGEE del CERN, bastata sul middleware gLite.

3.6 IP

Internet Protocol: fornisce le funzioni necessarie per l'invio di pacchetti di bit detti *Internet datagram* da un host all'altro con un approccio Connectionless, per cui l'affidabilità delle trasmissioni è garantita da servizi di più alto livello, deputati al reinvio degli eventuali pacchetti persi e al ristabilire la loro giusta sequenza (**consegna best-effort**). Il protocollo IP definisce inoltre l'esatto formato dei dati e svolge funzioni di routing.
Nel contesto del protocollo IP, l'unità fondamentale di trasferimento è detta **datagram** IP, suddiviso in *header* e blocco di dati.

Header L'header del datagram IPv4 contiene i seguenti campi:

- **Version**: versione IP del datagram;
- **HL** (Header Length): lunghezza dell'header in parole da 32 bit;
- **TOS** (Type Of Service) o *differentiated services*: indicazioni sulla corretta gestione del datagram, volte a trattare in modo differente i diversi servizi, quasi del tutto inutilizzate;
- **Total lenght**: lunghezza totale del datagram;
- campi che controllano la frammentazione e il riassemblaggio dei datagram:

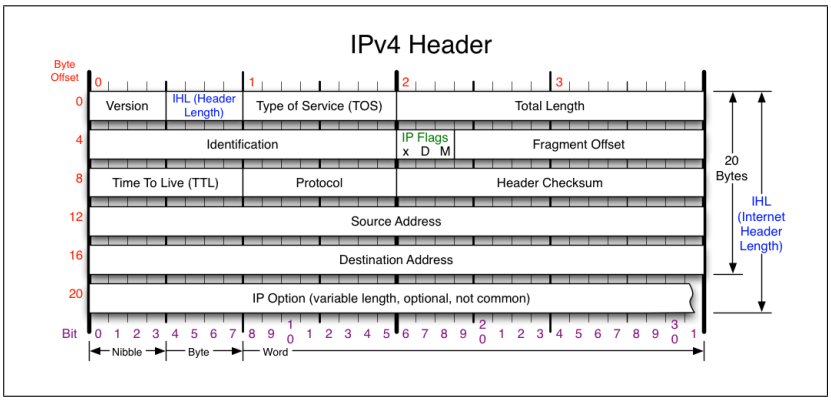


Figura 30: Formato header IPv4

  - **Identification**: indicazione del pacchetto cui appartiene il datagram,
  - **IP flags**,
  - **Offset del frammento**.

- **TTL** (Time To Leave): durata per cui il datagram permane in transito, espressa in secondi. Evita che pacchetti inutili rimangano in rete a tempo indeterminato;
- **Protocol**: indicazione di quale protocollo di più alto livello ha generato il blocco dei dati;
- **Header checksum**: sequenza di bit che utilizzata per verificare l'integrità dei dati contenuti nell'header;
- **Source address**: Indirizzo IP di provenienza;
- **Destination address**: Indirizzo IP di destinazione;
- **Opzioni** (campo opzionale, utilizzato per test e debugging).

3.6.1 Indirizzo IP

Ogni dispositivo connesso ad una rete IP è identificato da un indirizzo IP, univoco in quella rete. Più propriamente l'indirizzo IP viene associato alle interfacce del dispositivo. Un dispositivo con più schede di rete -per esempio un router- può connettersi direttamente a più reti e per ognuna avrà un indirizzo IP.

Indirizzo IPv4 Composto da 4 byte, è in forma $x.y.z.q$ e suddiviso in due parti, *rete* ed *host*. Gli indirizzi IP si suddividono in classi a seconda del numero di byte dedicato alla rete:

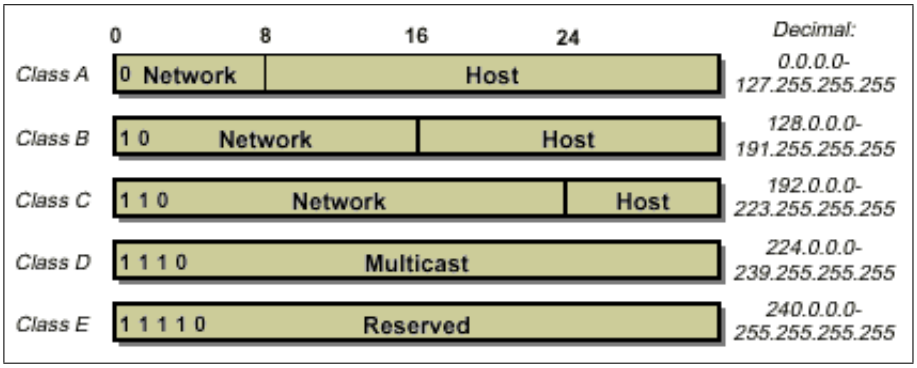


Figura 31: Suddivisione in classi degli indirizzi IPv4

- classe A: la parte rete ha valore < 128;
- classe B: la parte rete ha valori compresi tra 128 e 191;
- classe C: la parte rete ha valori compresi tra 191 e 223;
- classe D: la parte rete ha valori compresi tra 224 e 239 e viene utilizzata per l'IP multicasting;
- classe E: la parte rete ha valore > 239. Gli indirizzi di questa classe sono riservati.

Netmask Quando si fa riferimento ad una rete è necessario associare all'indirizzo IP una maschera di rete. La maschera indica il numero esatto di bit riservati alla rete. Quando la netmask differisce da quella predefinita per la classe dell'indirizzo, si stanno creando sottoreti (*subnetting*) o, viceversa, si sta incrementando il numero di possibili host a scapito del numero di possibili reti (*supernetting*). Oltre che, appunto, come numero decimale, si suole rappresentare la netmask come un indirizzo IP in cui tutti e soli i bit riservati alla rete hanno valore 1.

Esempio:
110.127.234.18 è un indirizzo di classe A, la sua rete di default si può indicare come 110.0.0.0/8 e la sua netmask espressa come indirizzo è 255.0.0.0. Se la netmask fosse invece 110.0.0.0/10 si starebbe facendo subnetting.

Nell'ambito degli indirizzi IPv4 sussistono alcune convenzioni:

- se la parte host di un indirizzo è 0, si sta indicando non un host in particolare, bensì la rete stessa;
- se la parte host di un indirizzo ha valore 1 su tutti i bit, si sta specificando un *indirizzo broadcast*, utilizzato per inviare pacchetti a tutti gli host della rete;
- l'indirizzo 0.0.0.0 specifica la *default route*, indicante il gateway di default al fine di instradare pacchetti la cui destinazione non è nella tabella di routing. Si tratta di una scelta poco felice, poiché costituisce uno spreco di spazio d'indirizzamento di classe A;
- l'indirizzo 127.0.0.1 è il cosiddetto *loopback address* (`localhost`), associato all'Interfaccia di rete virtuale di loopback;
- gli indirizzi di rete 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 e 169.254.0.0/16 sono riservati, ossia identificano reti private gestite dai server Packet filtering.

Differenze tra IPv4 e IPv6 L'IP versione 4 fornisce anche i servizi di frammentazione e riassemblaggio di datagram, quando la trasmissione avviene attraverso reti con capacità di trasporto di pacchetti più piccola del pacchetto originale (dovuto alle diverse tecnologie di rete del passato). IP versione 6 abolisce questo comportamento, non più necessario.

3.6.2 Interfaccia di rete

Ad ogni scheda di rete (hardware) di un dispositivo corrisponde un'interfaccia di rete (software) sulla quale operano protocolli di rete come Ethernet. Esistono anche interfacce virtuali, come quella di loopback locale, presente in ogni computer (`lo` su Unix). Quando un'interfaccia di rete viene configurata ad essa viene assegnato un indirizzo IP. Ciò avviene manualmente, o automaticamente (attraverso il protocollo DHCP).
Nei sistemi Unix-Linux, il comando per la configurazione manuale dell'IP è `ifconfig` (dove "if" sta per "interface"). La sintassi è la seguente:

```
$ ifconfig <nome interfaccia> <indirizzo IP> netmask <netmask
x.y.z.q> broadcast <indirizzo broadcast>
```

Il comando `ifconfig` senza argomenti mostra lo stato delle interfacce.

```
→  ~ ifconfig
enp3s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether c8:0a:a9:56:1a:76  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 453  bytes 152891 (149.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 453  bytes 152891 (149.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::45ac:80c7:ada3:59c0  prefixlen 64  scopeid 0x20<link>
        inet6 fe80::4c94:3ab9:1f95:b393  prefixlen 64  scopeid 0x20<link>
        inet6 fe80::eeac:5590:37e9:6e40  prefixlen 64  scopeid 0x20<link>
        ether f0:7b:cb:71:4e:66  txqueuelen 1000  (Ethernet)
        RX packets 41958  bytes 41254742 (39.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32386  bytes 4469440 (4.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 32: Output del comando ifconfig su una macchina Linux

Più di recente, `ifconfig`, `route` (vedi Routing) ed `arp` sono stati rimpiazzati dal comando `ip`, preinstallato su gran parte delle distribuzioni arch-based. Per i dettagli su tale comando, si visiti questa pagina[11].

3.7 IP multicasting

Si parla di IP multicasting quando un datagram è trasmesso ad un gruppo di host identificato da un unico Indirizzo IP. Gli appartenenti al gruppo possono cambiare dinamicamente -un gruppo può essere dunque permanente o transitorio- e si può definire una chiave di accesso che renda selettivo l'ingresso. La gestione delle informazioni relative alla composizione dei gruppi e l'invio in internet dei datagram sono responsabilità dei *multicast agents*, che girano sui router o su host particolari.

IGMP Le funzioni di IP multicasting sono supportate dal protocollo IGMP (Internet Group Management Protocol), definito negli RFC 1112, 1122, 1812, 2236, 2715, 2933 e 3228.

3.8 Protocolli di address resolution

3.8.1 ARP

Address Resolution Protocol: Due host Internet possono comunicare solamente conoscendo l'uno l'Indirizzo MAC dell'altro.
L'host A, per sapere l'indirizzo fisico di B, invierà a tutti gli host una richiesta ARP contenente l'Indirizzo IP di B e il proprio indirizzo MAC; B, vedendo la chiamata, risponderà scrivendo il MAC

[11] url: www.tecmint.com/ifconfig-vs-ip-command-comparing-network-configuration

address di A in una cache di consultazione e reinviando il proprio MAC address ad A.
La cache di consultazione permette di tenere traccia delle connessioni recenti in modo che, senza dover reinviare una richiesta ARP, sia possibile reinviare dati al suddetto host. Le informazioni nella cache possono però diventare obsolete, per questo un timer ne fa scadere la validità.
Occorre considerare alcuni problemi:

- il Jitter provocato degli aggiornamenti della cache;
- l'impatto sull'operatività di altri protocolli in presenza di richieste ARP pendenti.

3.8.2 RARP

Reverse ARP: Consente, al contrario dell'ARP, di risalire al proprio Indirizzo IP dal Indirizzo MAC. Viene utilizzato ad ogni avvio dagli host diskless (senza memoria secondaria) per determinare il proprio indirizzo IP, chiedendolo a dei particolari server RARP che contengono le informazioni in specifici file di configurazione. É reso obsoleto dal DHCP.

3.9 Routing

Il routing consiste nella scelta del cammino migliore da percorrere per trasmettere un datagram da un host all'altro, passando attraverso i nodi di una rete basata sul protocollo IP. Si divide in:

- **routing minimale**: la tabella di routing viene definita al momento della configurazione dell'Interfaccia di rete;
- **routing statico**: utilizzato quasi solamente per gli host, prevede, oltre alla configurazione delle interfacce, la definizione manuale delle varie *route*. In Unix-Linux le route possono essere aggiunte usando il comando

  ```
  $ route add -net <indirizzo di rete> netmask <netmask
  x.y.z.q> gw <indirizzo gateway>
  ```

  Per rendere permanenti le modifiche, i comandi `route` devono essere salvati in un file di configurazione eseguito all'avvio della macchina (in sistemi Unix-Linux, il path di tale file è `/etc/init.d/rc.local`);
- **routing dinamico**: utilizzato nei router, sfrutta i diversi Protocolli di routing.

Alla ricezione di un pacchetto, ogni nodo delle rete esegue le seguenti operazioni:

- determina la classe dell'Indirizzo IP di destinazione del pacchetto;
- controlla se tale indirizzo è locale ed eventualmente vi applica la Netmask per poi inviarlo direttamente all'host destinatario;
- se l'indirizzo non è locale, cerca la rete di destinazione nella Tabella di routing e, se presente, instrada il datagram verso il Gateway corrispondente.

3.9.1 Tabella di routing

Presente in ogni nodo di rete, contiene le informazioni per il routing.
Nella tabella di routing ogni riga rappresenta una "strada", composta da:

- indirizzo dell'host o sottorete di destinazione;
- indirizzo dell'eventuale prossimo gateway da attraversare;
- "distanza" dalla destinazione, detta Metric.

Nei sistemi Unix-Linux, si visualizza tramite il comando `netstat -r`[12] o `route`.

```
    netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         141.250.216.1   0.0.0.0         UG        0 0          0 wlp3s0
towelie.unipg.i 141.250.216.1   255.255.255.255 UGH       0 0          0 wlp3s0
141.250.216.0   *               255.255.248.0   U         0 0          0 wlp3s0
link-local      *               255.255.0.0     U         0 0          0 docker0
172.17.0.0      *               255.255.0.0     U         0 0          0 docker0
```

Figura 33: Output del comando `netstat -r`

É possibile utilizzare la specifica `-n` per ottenere gli indirizzi di destinazione in forma numerica. Il significato delle *flag* è il seguente:

- `U` (*up*) indica che l'Interfaccia di rete è attiva;
- `G` indica un'uscita verso un'altra rete tramite Gateway;
- `H` indica che la destinazione è l'indirizzo completo di un host;
- `D` indica una route aggiunta da un ICMP redirect.

[12] Attenzione: il campo `Genmask` indica la netmask.

3.9.2 Metric

Il concetto di distanza tra due nodi di una rete, a seconda del contesto e del protocollo, può essere dato da:

- *path length* (o *hop-count*): numero di nodi da attraversare;
- *reliability* (affidabilità): poiché le condizioni della rete sono variabili, viene solitamente misurata ad intervalli regolari. Talvolta è tuttavia impostata ad un valore costante;
- *load*: traffico, anch'esso misurato ad intervalli regolari;
- *delay*: tempo necessario al router per trasmettere un datagram, misurato in μs;
- *bandwidth* (ampiezza di Banda);
- *communication cost*: numero intero che indica arbitrariamente quanto un percorso sia conveniente. Valori più bassi indicano un percorso migliore.

3.10 Famiglie di protocolli di routing

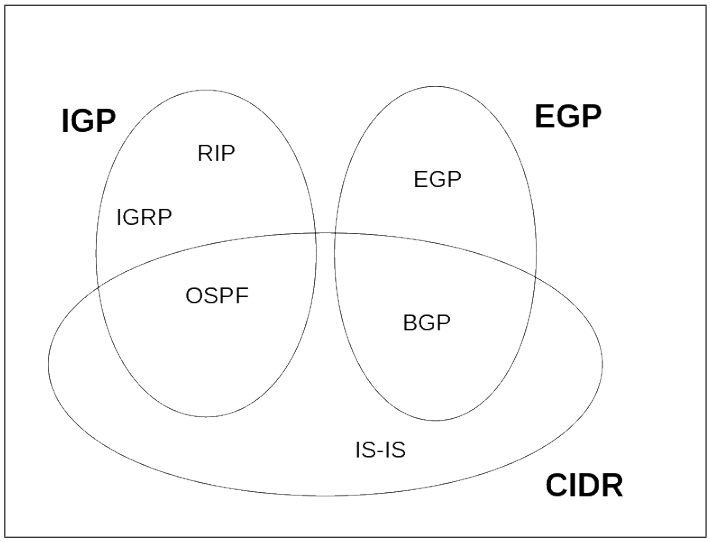


Figura 34: Protocolli di routing

3.10.1 IGP

Interior Gateway Protocol: famiglia di protocolli per il routing interno ad un AS (*intra-domain routing*), include RIP, IGRP e OSPF.

3.10.2 EGP

Exterior Gateway Protocol: famiglia di protocolli per il routing tra più diversi AS (*inter-domain routing*), include il protocollo EGP (storico), BGP (versione 4 attualmente in uso) e IDRP (OSI Inter-Domain Routing Protocol) che dovrebbe rimpiazzare il BGP una volta divenuto obsoleto.

3.10.3 CIDR

Classless Inter-Domain Routing: include OSPF, BGP e IS-IS.

3.10.4 Distance-vector

Un algoritmo del tipo distance-vector prevede che ogni router mantenga la propria Tabella di routing aggiornata effettuando scambi regolari con tutti gli altri router raggiungibili. Questi aggiornamenti sono in forma di coppie del tipo **(rete di destinazione, distanza)**.
La distanza può essere misurata in *hops* o in base al tempo di propagazione (vedi Criteri di valutazione in base alle prestazioni).
Il RIP è basato su un algoritmo di questo tipo.

3.10.5 Link-State

In un algoritmo di routing di tipo link-state ogni nodo della rete acquisisce informazioni sullo stato dei collegamenti adiacenti ed le inoltra a tutti gli altri nodi della rete tramite un pacchetto detto appunto *link-state*.
L'utilizzo di un protocollo link-state presenta diversi vantaggi:

- può gestire reti composte da un gran numero di nodi;
- converge rapidamente al cammino minimo;
- difficilmente genera cammini ciclici;
- è facile da comprendere poiché ogni nodo salva la mappa della rete nel proprio *Link-State Database* o *topological database*.

Appartengono a questa categoria i protocolli OSPF e IS-IS.

3.11 Protocolli di routing

I protocolli di routing mantengono aggiornata la Tabella di routing di ogni dispositivo che gestiscono tramite lo scambio di appositi messaggi; questi aggiornamenti prevalgono su eventuali configurazioni statiche. Un router può essere gestito da più protocolli di routing contemporaneamente.

3.11.1 RIP

Routing Information Protocol: Protocollo sviluppato nel 1988 come parte di ARPANET e basato sull'algoritmo di Bellman-Ford; è definito negli RFC 1058 e 1023.
Utilizza UDP come protocollo di trasporto sulla porta riservata 520.
Misura la Metric in *hops* ed ha 15 come limite di distanza su cui effettuare il routing. Un numero di hop pari a 16 equivale dunque a infinito ed è usato per indicare le *route* inaccessibili che non verranno aggiunte alla Tabella di routing.
Il RIP ha due forme a seconda dell'utente:

- Forma passiva, usata dagli host: riceve messaggi ma non ne invia;
- Forma attiva, usata dai router: riceve ed invia in *broadcast* messaggi.

Questi messaggi prendono il nome di *routing updates* e consistono nella porzione di Tabella di routing in cui si è trovato un percorso migliore.
I router inviano aggiornamenti in due occasioni:

- ad ogni tick di clock del *routing-update timer*, cioè a cadenza regolare (abitualmente ogni 30 secondi);
- quando cambia la topologia della rete dei router confinanti.

Un altro timer utilizzato è il *route timeout*: se una route non viene aggiornata nella tabella entro un tempo limite, viene segnata come *invalid* e successivamente rimossa allo scadere del *route-flush timer*.

Rispetto all'OSPF, il RIP converge meno rapidamente ed è potenzialmente più soggetto a generazione di *routing loops*. Di contro, ha il vantaggio di essere più leggero in termini di risorse utilizzate e risulta più semplice nell'implementazione e nella gestione.

Al fine di evitare frequenti cambi nella routing table per percorsi di costo uguale, il RIP impone di mantenere gli instradamenti esistenti finché non ne è presente un altro di costo più basso (*isteresi*[13]).

I problemi legati alla convergenza lenta vengono arginati mediante le seguenti tecniche:

- *split horizon update*: gli aggiornamenti non vengono propagati ai router che li hanno generati;
- *hold-down timer*: quando un router riceve un messaggio di rete irraggiungibile, questo ignorerà per un certo periodo (di solito 60 secondi) tutti gli aggiornamenti inerenti tale rete;

[13] *Istèresi*: fenomeno per cui il valore assunto da una grandezza dipendente da altre è determinato, oltre che dai valori istantanei di queste ultime, anche dai valori che avevano assunto in precedenza

- *triggered update*: obbliga i router ad annunciare subito la scomparsa di route, ignorando eventuali timer;
- *poison reverse*: la scomparsa di un collegamento nella rete viene annunciata più volte per un certo lasso di tempo.

Timers	Default Value	Uses
Hold down timer	180 seconds	Used to hold the routing information for the specified time.
Invalid route timer	180 seconds	Used to keep track of discovered routes
Route update timer	30 seconds	Used to update routing information
Route flush timer	240 seconds	Used to set time interval for any route that becomes invalid and its deletion from the routing table.

Figura 35: Timer usati da RIP e loro durate standard

In RIP v1 non sono supportate subnet variabili.
In RIP v2 ogni router invia messaggi di aggiornamento soltanto ai propri *neighbor* (vicini, a distanza 1 hop) mediante *unicast updates* e non più in broadcast, alleggerendo il traffico.

RIP è presente di default sui sistemi Unix/Linux (daemon `routed`).

Router A:

```
interface serial 0
ip address 130.10.62.1 255.255.255.0
interface serial 1
ip address 130.10.63.1 255.255.255.0
interface ethernet 0
ip address 130.10.8.1 255.255.255.0
interface tokenring 0
ip address 130.10.9.1 255.255.255.0
router rip
network 130.0.0.0
```

Router B:

```
interface serial 0
ip address 130.10.62.2 255.255.255.0
interface serial 1
ip address 130.10.63.2 255.255.255.0
interface ethernet 0
ip address 130.10.17.2 255.255.255.0
interface tokenring 0
ip address 130.10.16.2 255.255.255.0
router rip
network 130.0.0.0
```

Router C:

```
interface serial 0
ip address 130.10.63.3 255.255.255.0
interface serial 1
ip address 130.10.64.3 255.255.255.0
interface ethernet 0
ip address 130.10.24.3 255.255.255.0
router rip
network 130.0.0.0
```

Figura 36: RIP: Esempio di configurazione

3.11.2 OSPF

Open Shortest Path First: Protocollo Open Source sviluppato nel 1988 dall'IGP working group di IETF e divenuto standard nel 1990 (RFC 1247), è basato sull'algoritmo di Dijkstra per lo shortest path.
Supporta subnet variabili, routing in base al tipo di servizio ed autenticazione ed esegue il bilanciamento del carico.
L'OSPF supporta sistemi gerarchici, ovvero la divisione della rete in **aree**: ogni router conserva il *topological database* della sua area, dove salva la lista dei router adiacenti, indicando quelli designati a svolgere il ruolo di "rappresentanti dell'area", cioè DS (*Designated Routers*) e BDR (*Backup Designated Routers*).
Le varie aree sono collegate tra loro dalla cosiddetta *backbone area* o area 0, i cui nodi non sempre sono collegati fisicamente: nel caso in cui non lo siano, vengono definiti collegamenti virtuali (*virtual-link*) tra router di backbone e router di altre aree, che funzionano come collegamenti fisici diretti (**la topologia logica può essere diversa da quella fisica**).
La divisione in aree porta a due tipi diversi di routing (*intra-area* ed *inter-area*) e a quattro diversi tipi di router:

- **IR (Internal Router)**: router interno ad un'area;
- **ABR (Area Border Router)**: a confine tra più aree, mantengono il *topological database* di ogni area che collegano;
- **BR (Backbone Router)** router dell'area di backbone;
- **ASBR (AS Boundary Router)**: router di confine tra AS.

L'OSPF utilizza pacchetti di tipo LSA (Link-State Advertisement), in particolare presenta cinque tipi di pacchetto:

- Tipo 1: Hello,
- Tipo 2: Database Description,
- Tipo 3: Link State Request,
- Tipo 4: Link State Update,
- Tipo 5: Link State Acknowledgment.

Header Comune a tutti i pacchetti, è composto da **versione** del protocollo OSPF, **tipo** di pacchetto, **lunghezza** del pacchetto, **ID del router**, **ID dell'area**, **check-sum** per il controllo degli errori e **autenticazione**.

Hello Primo pacchetto ad essere inviato quando si abilita l'OSPF su un'interfaccia, esso è il mezzo attraverso il quale i router vengono a conoscenza l'uno dell'altro e viene reinviato periodicamente.

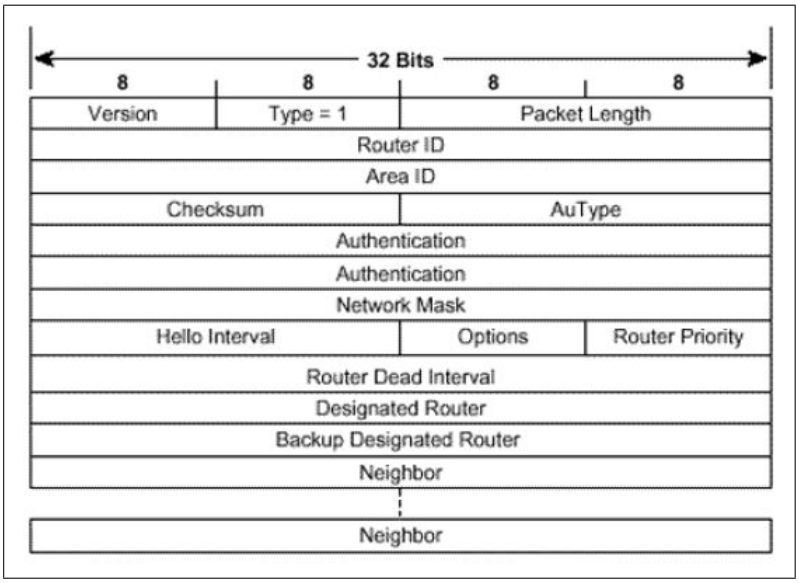


Figura 37: Struttura di un pacchetto Hello

- **Netmask**: necessaria perché solo i router che concordano sulla suddivisione della rete si connettono tra loro;
- **Hello Interval**: stabilisce l'intervallo in secondi tra due pacchetti *Hello*; due router con differente hello interval non stabiliranno una connessione;
- **Options**: indica le funzionalità del mittente per verificare, prima della connessione, che siano compatibili con quelle del destinatario;
- **Router Priority**: indica la priorità del router;
- **Router Dead Interval**: numero di secondi che il mittente aspetterà prima di dichiarare morto il destinatario;
- **Designed Router**: indirizzo IP dell'interfaccia del DR conosciuto, se non è ancora stato eletto è 0.0.0.0.
- **Backup Designed Router**:indirizzo IP dell'interfaccia del BDR conosciuto; se non è ancora stato eletto è 0.0.0.0;
- **Neighbor**: lista dei router con i quali il mittente è in contatto; serve a generare il *topological database*.

Database Description Utilizzato quando viene stabilito un contatto tra due router al fine di confrontare i pacchetti LSA ricevuti. Uno dei due router assume il ruolo di *master* e l'altro di *slave* e si scambiano una serie di messaggi contenenti gli header dei LSA.

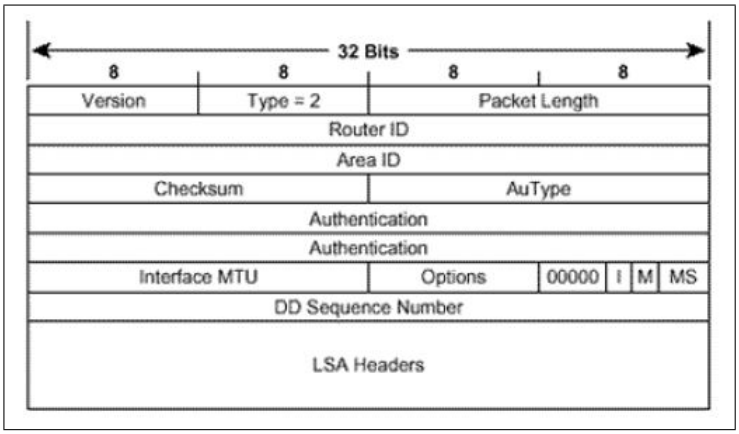


Figura 38: Struttura di un pacchetto Database Description

- **Interface MTU**: dimensione in ottetti del più grande datagram che il mittente può trasmettere senza frammentazione;
- **Options**: indica le funzionalità del mittente per permettere una selezione dei LSA trasmessi;
- **I**: Initial bit: ha valore 1 solo se il pacchetto è il primo della serie;
- **M**: More bit: ha valore 0 solo se il pacchetto è l'ultimo della serie ;
- **MS**: Master/Slave bit, 1 se il mittente è il Master, 0 se è lo Slave;
- **DD Sequence Number**: assicura la ricezione di tutta la sequenza di pacchetti di Database Description; è impostato dal master nel primo pacchetto e viene incrementato in ogni pacchetto seguente per mantenere la sincronizzazione;
- **LSA Headers**: lista di header di pacchetti LSA ricevuti dal mittente.

Link State Request Quando, in seguito ad un messaggio di Database Description, un router si accorge di non aver ricevuto uno dei LSA ricevuti dall'altro, richiede che gli venga ritrasmesso tramite un pacchetto LSR.

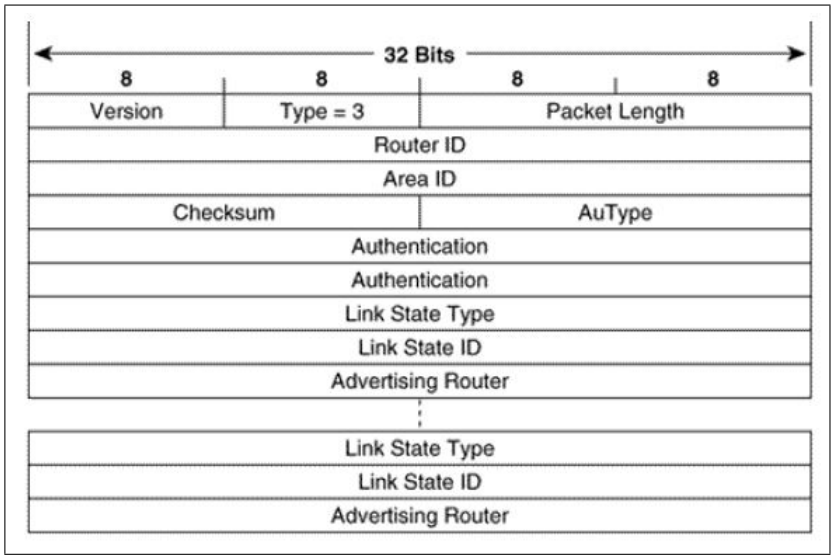


Figura 39: Struttura di un pacchetto Link State Request

Dopo l'header si ripetono i seguenti tre campi per ogni pacchetto LSA richiesto:

- **Link State Type**: tipo di LSA richiesto;
- **Link State ID**: codice identificativo del LSA in funzione del tipo;
- **Advertising Router**: ID del router che ha originato l'LSA.

Link State Update Inviato in risposta ad un pacchetto Link State Request, il pacchetto LSU contiene le informazioni degli LSA richiesti. In caso il richiedente non sia connesso direttamente al mittente, verrà inviato un LSU con le stesse informazioni da router a router fino alla destinazione.

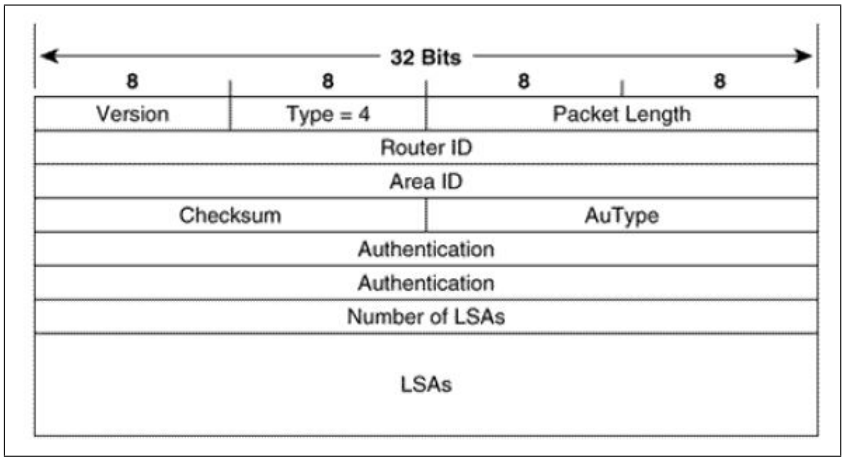


Figura 40: Struttura di un pacchetto Link State Update

- **Number of LSAs**: numero di LSA contenuti;
- **LSAs**: descrizione completa degli LSA;

Link State Acknowledgment Usati per confermare la ricezione degli LSA via Link State Update; ne contengono la lista degli header.

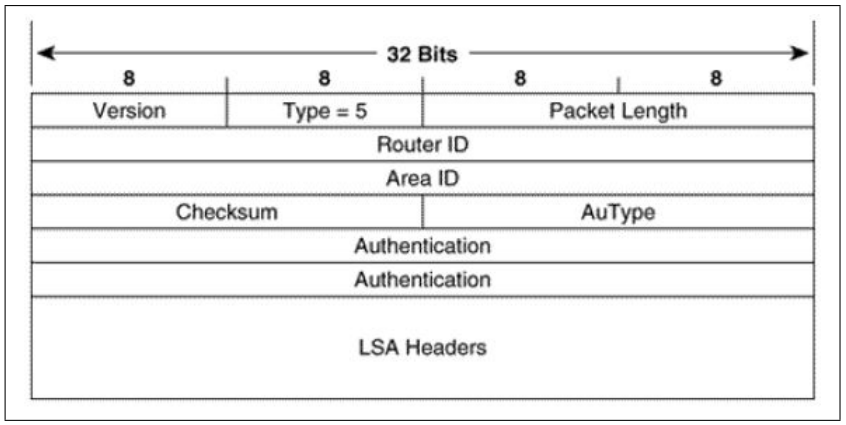


Figura 41: Struttura di un pacchetto Link State Acknowledgment

3.11.3 BGP

Il protocollo BGP (Border Gateway Protocol), descritto nella sua versione corrente nell'RFC 1771[14], è un protocollo EGP, ma ne esiste anche una versione *intradomain*, l'iBGP, che verrà illustrata più avanti. Esso mette dunque in comunicazione particolari router appartenenti ad AS differenti, detti -come suggerito dal nome del protocollo- *gateway di confine*. Un protocollo apposito è necessario perché, a differenza di quanto avviene all'interno di un singolo AS, un protocollo che metta in comunicazione più domini di routing deve tenere in conto le differenze tra le policy adottate dai diversi ISP che gestiscono tali domini. La principale funzione del BGP è lo scambio di informazioni sulla raggiungibilità delle reti, volta al mantenimento di una visione unitaria della topologia della rete da parte dei diversi router.
Perché due router possano comunicare, devono essere innanzitutto definiti come *BGP neighbors*, detti anche *peers* tramite una configurazione manuale che ha per risultato la creazione di una sessione TCP sulla Porta 179. A questo punto, i peer si invieranno l'un l'altro la Tabella di routing in formato CIDR ed una serie di messaggi:

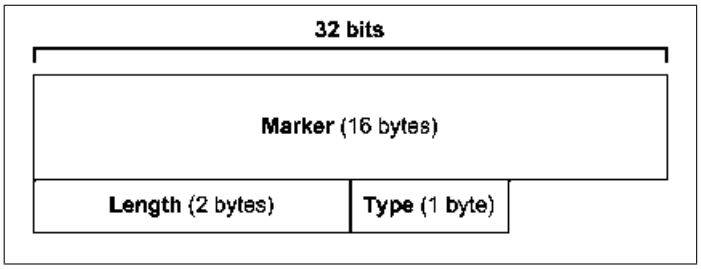


Figura 42: Header di un messaggio BGP. Il campo **Marker** contiene un valore riconosciuto da entrambi i peer, importante per sincronizzazione ed autenticazione

- **OPEN**: messaggio che i peers si scambiano all'apertura della connessione e negoziarne i parametri;
- **KEEPALIVE**: conferma dell'apertura della connessione; continua poi ad essere inviato periodicamente da ogni nodo per segnalare la propria attività, in modo tale che la connessione venga mantenuta;
- **UPDATE**: messaggio tramite il quale vengono aggiornate le tabelle di routing dopo il primo scambio. All'aggiornamento, viene modificato il numero di versione della tabella, che deve essere lo stesso per tutti i *peer*;
- **NOTIFICATION**: viene trasmesso in condizioni particolari, ad esempio al rilevamento di un errore. Serve inoltre a chiudere una connessione e ad avvisare gli altri router del perché;
- **REFRESH**: richiesta di reinvio delle informazioni di routing.

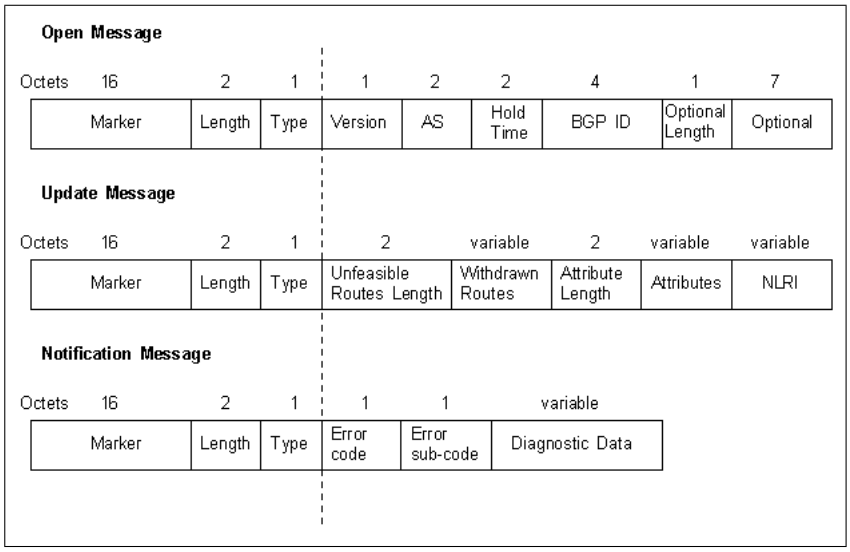


Figura 43: La struttura di alcuni messaggi BGP

[14]Le precedenti versioni del BGP sono descritte negli RFC 1105, 1163, 1267 e 1654.

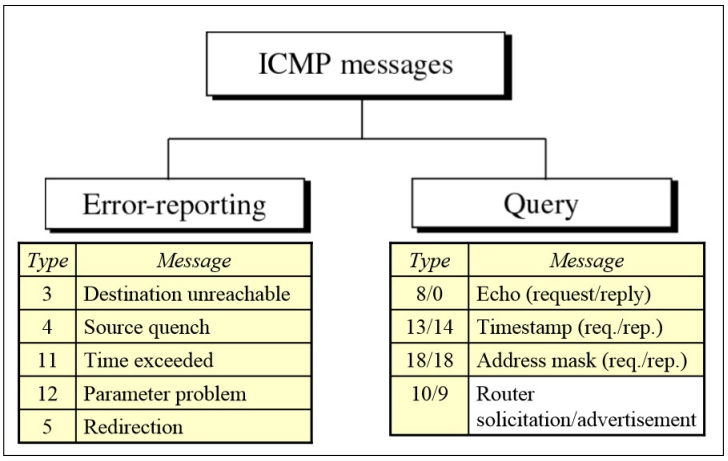
La Metric utilizzata dal BGP è il *communication cost*, assegnata ad ogni nodo dall'amministratore di rete.

Una tipologia particolare di *inter-domain routing* è il *pass-through autonomous system routing*, che avviene tra due rotuer BGP che si scambiano traffico tramite un terzo AS che non esegue BGP: esso fa dunque solo da "ponte", in quanto non è né emittente né destinatario delle comunicazioni.

iBGP Come accennato, iBGP sta per "internal BGP" ed è coinvolto nell'*intra-domain routing*. La sua funzione è quella di stabilire quale sia il router ottimale come punto di connessione con gli AS esterni.

3.12 ICMP

Il protocollo ICMP (Internet Control Message Protocol) definito negli RFC 792, 1256, 1788, 2463 e 2521, è progettato per verificare lo stato della rete e riportare eventuali malfunzionamenti nel routing. Esso comporta che i router inviino messaggi ICMP ai mittenti dei datagram che presentano problemi. I possibili tipi di messaggio sono illustrati in figura.



Type	*Message*
3	Destination unreachable
4	Source quench
11	Time exceeded
12	Parameter problem
5	Redirection

Type	*Message*
8/0	Echo (request/reply)
13/14	Timestamp (req./rep.)
18/18	Address mask (req./rep.)
10/9	Router solicitation/advertisement

Figura 44: Tipi di messaggi ICMP

In particolare, il messaggio **redirection** indica la necessità di reinstradare i pacchetti in modo migliore, segnala cioè che un router è stato attraversato inutilmente, ossia ha dovuto ritrasmettere il messaggio sulla rete di provenienza dello stesso. Alla ricezione di un messaggio di questo tipo, l'host ricevente associa a quella destinazione un router diverso da quello di default. I messaggi **address mask request/reply** consentono invece ad un'interfaccia di scoprire la netmask utilizzata in una rete.
I comandi `ping` e `traceroute` (vedi Qualità delle trasmissioni) sfruttano il protocollo ICMP.

4 Livello di trasporto

4.1 Terminologia

4.1.1 Porta

Identificata da un numero intero detto *portnumber*, rappresenta un punto di destinazione astratto che consente ad un host di effettuare più connessioni contemporanee verso altri, facendo in modo che i dati contenuti nei pacchetti in arrivo vengano indirizzati specificamente al processo applicativo che li attende. É il sistema operativo dell'host che si fa carico di fornire i meccanismi di interfaccia che i processi utilizzeranno per specificare una porta o per accedervi. L'accesso ad una porta dall'esterno richiede la conoscenza dell'IP dell'host e del portnumber del protocollo utilizzato dal processo destinatario (IP e portnumber, assieme, sono detti *socket*). Le porte $0 - 1023$ sono quelle raccomandate per i protocolli TCP e UDP.

4.1.2 Connectionless

In un servizio connectionless, ogni pacchetto contiene tutte le informazioni sul destinatario ed è instradato secondo queste ultime, indipendentemente dagli altri. L'ordine di arrivo dei pacchetti è arbitrario.

4.1.3 Connection-oriented

Un servizio connection-oriented, di cui è un esempio la rete telefonica, richiede che venga creato un canale di comunicazione -sia esso logico o fisico- prima dell'invio dei dati. Questo metodo è considerato affidabile, poiché è garantito che i dati arriveranno nell'ordine in cui sono stati inviati. In termini più tecnici, le principali caratteristiche di un servizio connection-oriented sono:

- **orientamento dello stream**: l'ordine di invio dei byte viene mantenuto;
- **connessione di circuito virtuale**: la trasmissione ha luogo solo quando emittente e destinatario hanno verificato la sussistenza delle condizioni necessarie.

4.2 Protocolli di trasporto

4.2.1 UDP

L'UDP (User Datagram Protocol) è un protocollo di tipo Connectionless. Pur essendo, di conseguenza, poco affidabile, esso è vantaggioso per applicazioni *time-sensitive* perché molto veloce, ed è spesso impiegato, ad esempio, per la trasmissione di informazioni audio-video in tempo reale, come nel caso delle trasmissioni VOIP (Voice Over IP). L'UDP fornisce soltanto i servizi basilari del livello di trasporto, ovvero la verifica dell'integrità dei dati mediante una checksum, inserita nell'header del pacchetto e la multiplazione delle connessioni, ottenuta attraverso il meccanismo di assegnazione delle porte. Un programma applicativo che utilizzi l'UDP si assume dunque la responsabilità di fornire soluzioni per quel che riguarda l'affidabilità.

4.2.2 TCP

A differenza dell'UDP, il TCP (Transmission Control Protocol) è un protocollo Connection-oriented. La prima definizione del TCP si trova nell'RFC 793, ma le molteplici modifiche che essa ha subito, formalizzate in altrettanti RFC, hanno portato alla necessità di pubblicare un ennesimo RFC, il 4614: una sorta di guida ai documenti sul TCP. Affidabile e di applicabilità generale, è progettato per adattarsi dinamicamente alle peculiarità delle diverse reti che compongono Internet, contribuendo ad isolare le applicazioni dai dettagli di networking. Più specificamente, oltre a quelle di qualsiasi protocollo Connection-oriented, le principali caratteristiche del TCP sono:

- **trasferimento bufferizzato**: il trasferimento viene ottimizzato creando pacchetti di dimensione il più possibile simile;
- **stream non strutturato**: la comprensione della forma dei dati trasmessi sta all'applicazione che utilizza il protocollo in oggetto;
- **connessione Full-Duplex**;

- affidabilità garantita mediante **riscontro positivo con ritrasmissione** (*acknowledgement*): alla ricezione di un pacchetto, il destinatario risponde con un "ACK", ossia una conferma di ricezione. Il mittente dovrà poi ritrasmettere i pacchetti persi o, eventualmente, chiudere la connessione;
- trasmissione ottimizzata tramite la tecnica della *finestra scorrevole* (vedi ARQ).

5 Livello delle applicazioni

Il quinto livello del Modello di riferimento ISO/OSI racchiude tutte le applicazioni dedicate all'utente finale. É qui che la differenza fra protocollo e servizio si fa sempre piú labile: molto spesso, la stessa parola indica sia il protocollo che la sua implementazione, la quale, la maggior parte delle volte, é un comando Linux.

5.1 Terminologia

5.1.1 URI

Uniform Risource Identifier: sequenza di caratteri che identifica univocamente una risorsa. Esistono due tipi di URI:

- L'**URL** (Uniform Resource Locator) che fornisce anche i mezzi per agire sulla risorsa, descrivendo il suo meccanismo di accesso o la sua ubicazione in una rete. Il suo formato è il seguente:

  ```
  protocollo:[//[username[:password]@]host[:porta]]
  [/path][?query][#fragment]
  ```

  Esempio: https://en.wikipedia.org/wiki/URL#Syntax;

- L'**URN** (Uniform Resource Name) si limita ad identificare la risorsa tramite un nome riferito ad un particolare namespace.

5.1.2 Web server

Software in grado di gestire le richieste di trasferimento di pagine Web di un client (browser).
Le possibili architetture sono due:

- *prefork*: ad ogni richiesta ricevuta viene avviato un nuovo processo tramite fork del processo server;
- *threaded*: ad ogni richiesta viene avviato un *thread*.

5.1.3 Pagina statica

Documento HTML che ha sempre lo stesso contenuto ad ogni visualizzazione. Quando richiesto, il web server si limita ad inviarlo al browser.

5.1.4 Pagina dinamica

Documento HTML generato da un'applicazione Web, realizzata tramite un linguaggio di scripting lato server (ad esempio PHP). La richiesta di una pagina dinamica innesca un processo più articolato:

1. Il client (browser) invia la richiesta (HTTP request) al Web server;
2. Il server Web determina quale *application server* debba essere utilizzato per eseguire la richiesta del browser, attraverso una lista di *application mapping*. Essa associa alle estensioni dei file richiesti gli application server appositi;
3. L'applicazione Web viene eseguita dell'*application server* il quale genera il documento e lo passa al web server;
4. Il server Web invia la risposta (HTTP response) contente il documento al browser.

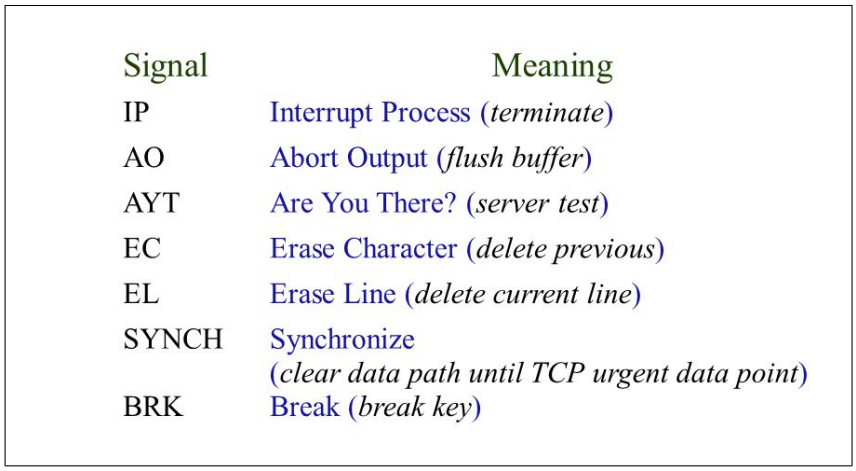
Questo processo è detto *round trip* in quanto, essendo il protocollo HTTP *stateless*, finite le operazioni i server tornano alla situazione iniziale senza modificare alcuna informazione. Per questo i linguaggi di scripting lato server mettono a disposizione le *variabili di sessione*[15] che permettono all'utente di salvare alcune informazioni sui server per un certo periodo di tempo.

[15] Diverse dai *cookies*, che vengono salvati localmente.

5.2 Servizi di rete

5.2.1 Telnet

Telnet, definito negli RFC 854 e 855, nasce come protocollo di rete per sistemi Unix in grado di gestire una comunicazione standardizzata fra due DTE. Nei sistemi Windows è implementato da un programma autonomo, di cui è un esempio Putty. Basato su TCP, Telnet consente di accedere da remoto ad una macchina, emulandone il terminale tramite un **NVT** (Network Virtual Terminal), che fornisce un'interfaccia standard. Il client ascolta sulla porta predefinita (23) e l'utente stabilisce una connessione utilizzando IP, nome utente e password di un utente del server. Inizialmente vi é una negoziazione dei parametri, dalla quale dipendono le funzionalità attivate per la sessione. Le funzioni di controllo standard sono illustrate in figura.



Signal	Meaning
IP	Interrupt Process (*terminate*)
AO	Abort Output (*flush buffer*)
AYT	Are You There? (*server test*)
EC	Erase Character (*delete previous*)
EL	Erase Line (*delete current line*)
SYNCH	Synchronize (*clear data path until TCP urgent data point*)
BRK	Break (*break key*)

Figura 45: Funzioni di controllo standard

L'unico grande problema di Telnet riguarda la sicurezza. Si tratta infatti di un protocollo non criptato: la password, il nome utente e tutte le altre informazioni sono inviate in chiaro. A questa problematica pone rimedio SSH.

5.2.2 Comandi r

Progettati per i sistemi BSD Unix e anch'essi basati sul TCP, i comandi r hanno funzionalità analoghe a quelle di Telnet:

- `rlogin` (*remote login*) permette di amministrare una serie di macchine autenticandosi una sola volta (*one time login*);
- `rsh` (*remote shell*) consente di eseguire da remoto singoli comandi;
- `rcp` (*remote copy*) abilita alla copia di file attraverso la rete.

Anche in questi casi non vi è alcuna forma di crittografia ed SSH sopperisce a questa mancanza.

5.2.3 FTP

Definito nell'RFC 959, il File Transfer Protocol, impiegato per il trasferimento di file in rete, è basato sul TCP. Ogni trasferimento coinvolge due processi, che si traducono in due connessioni distinte:

- **PI** (Protocol Interpreter), volto alla trasmissione dei comandi, che usa la porta 21;
- **DTP** (Data Transfer Protocol), che consiste nel vero e proprio trasferimento ed utilizza la porta 21. In questa fase client e server si scambiano i ruoli. Ad oggi, gran parte delle richiese FTP non avviene da linea di comando, ma da browser, ad esempio specificando un url.

I comandi FTP si suddividono in quattro categorie:

- controllo dell'accesso:
  - `OPEN` *`nomehost`*,

  - `USER` *nomeutente*,
  - `PASS` *password*,
  - `QUIT`;
- configurazione dei parametri per il trasferimento:
  - `PORT` *socket in forma IP:Porta*,
  - `PASV`;
- trasferimento dei file:
  - `TYPE` (ASCII o binario),
  - `RECV` o `GET` *fileremoto filelocale*,
  - `SEND` o `PUT` *filelocale fileremoto*;
- gestione di directory e file, usati dal client, con effetto sul server:
  - `DELETE` *fileremoto*,
  - `CD`,
  - `MKDIR`,
  - `RMDIR`,
  - `LS` o `DIR`;

Nell'ambito dell'FTP, si parla di *sessione anonima* quando si utilizza il protocollo in sola lettura; in tal caso si usa `anonymous` come account.
Un alternativa più leggera all'FTP standard, pensata per l'ambito LAN, è il TFTP (Trivial FTP) utilizzata dalle macchine diskless per ottenere l'immagine del sistema operativo. Essa sfrutta l'UDP al posto del TCP. Anche l'FTP è carente dal punto di vista della sicurezza, ragion per cui l'RFC 2228 introduce nuovi comandi ad essa correlati:

- `AUTH`: definizione del meccanismo di autenticazione da utilizzare;
- `PROT` *lv*: dichiarazione del livello di protezione da utilizzare, da configuare tramite ulteriori comandi appositi, a scelta tra:
  - `clear` (trasmissione in chiaro),
  - `safety` (richiesta verifica integrità dati, comando `MIC`),
  - `confidential` (trasmissione cifrata, comando `CONF`),
  - `private` (trasmissione cifrata e con richiesta verifica integrità dati, comando `ENC`).

5.2.4 SSH

Come si è anticipato, Telnet, i Comandi r ed FTP sono stati rimpiazzati da SSH (Secure SHell), che permette di instradare connessioni TCP in un canale cifrato, accorpandone tutte le funzionalità. Inoltre, con la specifica `-x`, SSH permette di trasmettere anche il desktop, funzionalità in precedenza fornita da un programmi appositi. Il vantaggio di SSH è appunto l'impiego di crittografia asimmetrica. Le chiavi pubbliche (*authorized keys*) vengono salvate in un file ASCII del server, mentre il client memorizza i *known hosts*. La chiave privata del client viene controllata alla sua prima connessione con il server.
Del protocollo esistono due versioni, SSH1 ed SSH2, tra loro incompatibili.
L'implementazione FLOSS del protocollo, Open SSH (si veda il sito ufficiale `www.openssh.com` per i dettagli sulla licenza), comprende una vasta gamma di programmi:

- `ssh`, che sostituisce `rlogin` e Telnet;
- `scp`, che sostituisce `rcp`;
- `sftp`, che sostituisce FTP;
- `ssh-add`, `ssh-agent` ed `ssh-keygen`, una serie di programmi per la generazione e la gestione delle chiavi;

- i demoni `sshd` ed `sftp-server`.

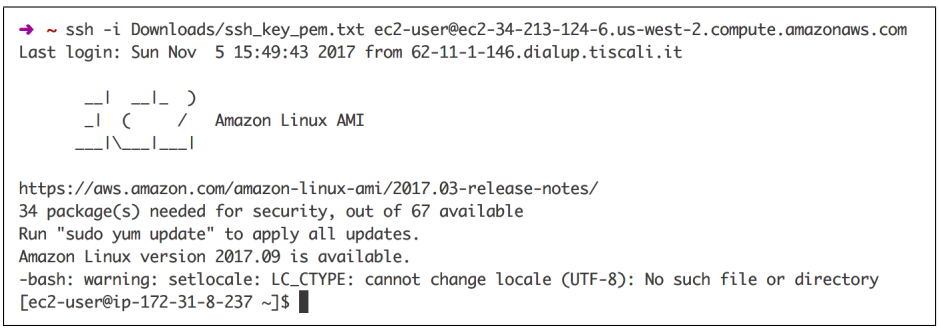


Figura 46: Connessione SSH ad un' instanza Linux Amazon, notare la sintassi `ssh -i ChiavePrivata NomeUtente@IndirizzoIp`

5.2.5 DHCP

Il protocollo DHCP (Dynamic Host Configuration Protocol) permette agli *host* di una rete locale di ricevere ad ogni richiesta di accesso a una rete IP tutte le informazioni di configurazione necessarie a connettersi ed operare.
Non è utilizzato per la configurazione dei router.

Il DHCP si basa sul modello *client-server*:

- **client**: host che necessita un indirizzo IP per collegarsi alla sottorete;
- **server**: host designato all'assegnazione degli indirizzi ai client che li richiedono. Anche un *router* può assolvere, tra le altre cose, tale ruolo.

È un protocollo nato come complemento del **BOOTP** (Bootstrap protocol, RFC 821), il quale raccoglie informazioni per la configurazione degli host sfruttando l'UDP (sulla porta 67 del server e 68 del client) ed assegna gli indirizzi IP tramite messaggi *broadcast*.
Il DHCP lo estende (RFC 1534) aggiungendo nuove opzioni di configurazione, tra cui la scelta fra tre metodi di assegnamento degli indirizzi:

- *automatic allocation*: i client che si connettono ricevono dal server un indirizzo IP permanente;
- *dynamic allocation*: ad ogni nuova connessione il client riceve un indirizzo IP, il quale ha un tempo di validità (*lease*), al cui termine ritorna nella *pool* degli indirizzi disponibili. Ciò permette di riutilizzare indirizzi non più in uso dai client;
- *manual allocation*: il DHCP si limita a comunicare al client l'indirizzo scelto per lui dall'amministratore di rete.

Il DHCP permette di riservare indirizzi IP per specifici client tramite l'associazione al relativo Indirizzo MAC (*DHCP Client Reservation*).

Il processo di assegnamento degli indirizzi si divide in 4 fasi:

1. *Discovering*: il client chiede che gli venga assegnato un indirizzo tramite il messaggio `DHCPDISCOVER` inviato in *broadcast*;
2. *Offering*: i server che ricevono la richiesta rispondono (se hanno indirizzi liberi a disposizione) con il messaggio `DHCPOFFER`, in cui propongono un indirizzo IP e gli altri parametri di configurazione al client;
3. *Requesting*: una volta ricevute le offerte dei server, il client le valuta e risponde con `DHCPREQUEST` (sempre in broadcast) per comunicare quale server ha scelto;
4. *Acknowledgment*: se l'assegnamento è avvenuto con successo, il server invia al client la conferma tramite `DHCPACK`; in caso di errori viene invece inviato il messaggio `DHCPNACK` (*negative acknowlegment*).

Si noti che, nella fase 1, il client non ha ancora configurato completamente l'Internet protocol suite (TCP/IP) in quanto è sprovvisto di indirizzo IP e il messaggio avrà come mittente 0.0.0.0 e 255.255.255.255 come destinatario.

Step di configurazione di un server DHCP :

1. Installazione del software (dipende dal sistema operativo del server);
2. Configurazione della pool di indirizzi: definizione degli intervalli di indirizzi assegnabili ed eventuale *tempo di lease*;
3. Definizione delle opzioni con cui verranno configurati i client nel momento in cui ricevono un indirizzo IP (ad esempio la forma della *subnet mask*, l'elenco dei router della rete, l'elenco degli indirizzi dei DNS server accessibili ...).

In reti con più segmenti si può evitare di definire un server per ogni sottorete ricorrendo ai **DHCP Relay Agent**: è sufficiente configurarne uno per ogni segmento di rete al fine di rilevare i pacchetti inviati in *broadcast* (`DHCPDISCOVER` o `DHCPREQUEST`) ed inoltrarli ai server di destinazione, aggiungendo ad ogni pacchetto il proprio indirizzo.

Il DHCP presenta considerevoli problemi di sicurezza. Infatti, l'assenza di autenticazione e di cifratura nei messaggi sono il punto debole del protocollo: è possibile sovraccaricare di richieste i server tramite attacco *DoS*, esaurendo gli indirizzi disponibili (*address starvation*) e lasciando sprovvisti i client legittimi.
Inoltre, un host malevolo può assumere il ruolo di server DHCP, controllando di conseguenza gli assegnamenti di indirizzi: da questa posizione può, quando un client richiede un nuovo indirizzo IP, cambiare il *gateway* di default del bersaglio con il proprio indirizzo ed effettuare attacchi *man in the middle*.
Nei sistemi Unix, una possibile implementazione del DHCP è rappresentata dal demone ISCDHCPd (Internet Software Consortium Dynamic Host Configuration Protocol daemon), la cui configurazione viene eseguita mediante un file di testo chiamato `dhcpd.conf`.

5.2.6 DNS

Il DNS (*Domain Name System*) è un servizio utilizzato per associare i nomi degli host, più semplici da ricordare per l'utente, ai relativi indirizzi IP. In tal modo è inoltre possibile attribuire più nomi allo stesso indirizzo IP, per rappresentare servizi diversi forniti da uno stesso host, o viceversa, per rappresentare più host che forniscono lo stesso servizio).

Cenni storici Nei primi anni di Internet Jon Postel aggiornava manualmente la lista di coppie nome-indirizzo salvata su un server FTP.
Nel 1983, quando questo modello diventò insostenibile, assieme a Paul Mockapetris e Craig Partridge ideò il *Domain Name Scheme*, su cui si basa il DNS, introdotto nell'RFC 882 e ridefinito nei 1032 e 1035.

Spazio dei nomi gerarchico Garantisce l'aggiornamento di tutta la rete. L'insieme dei nomi viene suddiviso in zone, dette *domini*, che possono coprire più host ed essere suddivise in sottodomini e così via, formando una struttura ad albero in cui i nodi rappresentano i nomi:

- I domini di primo livello o **TLD** (*Top Level Domain*) sono i figli del nodo radice ".", suddivisi in:
  - **gTLD** (*generic TLD*), ad esempio `.com`, `.edu`[16] etc.;
  - **ccTLD** (*country-code TLD*) ad esempio `.it`, `.fr`, `.uk` etc;
  - **infrastrutturali**: `.arpa`, usato per la risoluzione inversa dei nomi.

  Essi sono assegnati da ICANN alle organizzazioni o alle autorità responsabili locali (per l'Italia l'IIT CNR). La loro lista completa è disponibile all'indirizzo `www.iana.org/domains/root/db`.
- I domini di secondo livello, in genere, appartengono alle organizzazioni che li hanno registrati e comprendono il loro nome e il dominio di primo livello separati da un punto (es. `unipg.it`);

[16] gTLD riservati: `.example`, `.invalid`, `.localhost`, `.test`

- I successivi *sotto-domini* vengono creati per rendere la gestione del DNS modulare e seguono la stessa logica dei domini di secondo livello;
- Infine, le foglie corrispondono ai singoli host.

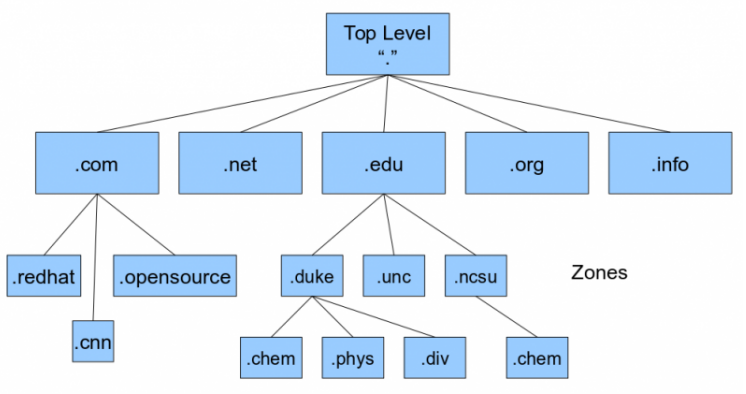


Figura 47: Spazio gerarchico dei nomi

Al contrario di quanto avviene con gli indirizzi IP, dunque, in un nome la parte più importante è la prima partendo da destra (il TLD). Ad ogni dominio è associato un Resource Record (RR), ossia un file ASCII che contiene record del database DNS.

Risoluzione La conversione di un nome in un indirizzo è detta *risoluzione*, mentre la conversione di un indirizzo in nome è detta *risoluzione inversa*.
La risoluzione può essere statica (mapping stabilito permanentemente tramite una *host table*) o dinamica (mapping stabilito ad ogni avvio dell'host).
Per eseguire la risoluzione, il client utilizza il resolver, il quale invia un pacchetto UDP ad un server DNS locale (*primary server*) che cerca il nome e, se è presente nella sua cache, lo restituisce, mentre in caso contrario interroga ricorsivamente i server partendo da un *root server* del TLD fino ad arrivare ai server autoritativi del nome richiesto (*authoritative server*), i quali invieranno la loro risposta al client.

BIND *Berkeley Internet Name Domain* è l'implementazione più comune del DNS su ambiente Unix ed è disponibile sul sito dell'*Internet Software Consortium* (ISC) `www.isc.org`. BIND è composto da una parte client, il *resolver*, ed una parte server, `named`. La prima è una libreria volta a generare ed inviare query al server dei nomi; la seconda un demone che risponde a suddette richieste. BIND può essere configurato come

- ***caching-only***: reindirizza ogni richiesta del resolver ad altri server e memorizza le risposte in una cache locale;
- ***authoritative***: ha una zona di competenza, della quale contiene le informazioni. In tal caso può essere:
  - ***primary***, qualora gestisca esso stesso le informazioni relative al proprio dominio, salvate negli Zone file, configurati dall'amministratore di rete,
  - ***secondary***: scaricano gli Zone file dal primary server e li memorizzano in appositi file detti *zone file transfer*.

Configurazione del resolver Il file relativo alla configurazione del resolver è `(/etc/resolv.conf)`.
Qualora non si voglia utilizzare la configurazione di default è necessario specificare:

- indirizzo del server dei nomi cui saranno inviate le richieste (sintassi: `nameserver` *`IP-address`*).
  Si possono specificare fino a tre nameserver, nell'ordine in cui si vuole che vengano interrogati;
- nome del dominio di default che verrà concatenato a sinistra di ogni nome host non contenente il carattere "`.`"; in caso di fallimento omette i domini meno significativi, fino a concatenare solo il TLD (sintassi: `domain` *`name`*). Un'alternativa per ottenere un risultato analogo è `search` *`names`*, che offre la possibilità di elencare più nomi da provare a concatenare, ma non risale i domini in caso di fallimento.

Configurazione del server dei nomi (`named`) La configurazione di `named` coinvolge più file:

- `/etc/named.conf` contiene i parametri generali di configurazione e i puntatori agli Zone file dei domini gestiti dal server.

  – Se si sta configurando un **caching-only** server, la configurazione è assai concisa:

    * `primary 0.0.127.IN-ADDR.ARPA /etc/named.local`
      indica che il server locale è primary server solo ed esclusivamente per il proprio dominio di loopback e specifica il file contenente le relative informazioni
    * `cache . /etc/named.ca`
      impone a `named` di memorizzare in una cache locale le risposte dei nameserver cui redirige le richieste dei resolver e di inizializzare suddetta cache con la lista dei root server, contenuta in `/etc/named.ca`

  – Se si sta configurando un **primary** server occorre, appunto, inoltre specificare il dominio per cui il server è primario e specificare il file contenente le associazioni IP-hostname (righe 2-3 dell'esempio sottostante, in cui il dominio è`unipg.it`)

```
directory /etc
primary     unipg.it                  named.hosts
primary     250.141.IN-ADDR.ARPA      named.rev
primary     0.0.127.IN-ADDR.ARPA      named.local
cache       .                         named.ca
```

  – Se si sta configurando un **secondary** server, bisogna invece specificare il server primario di riferimento per i vari domini e il file in cui memorizzare le risposte ottenute (righe 2-3 dell'esempio sottostante, riferito anch'esso al dominio unipg.it)

```
directory /etc
secondary   unipg.it                141.250.1.1      unipg.it.hosts
secondary   250.141.IN-ADDR.ARPA    141.250.1.1      250.141.rev
primary     0.0.127.IN-ADDR.ARPA                     named.local
cache       .                                       named.ca
```

- `/etc/named.ca` contiene i puntatori ai root domain server;

- `/etc/named.local` è lo zone file per la traduzione del reverse domain `0.0.127.IN-ADDR.ARPA` (lookback). In pratica, permette la conversione di `127.0.0.1` in `localhost`. Si noti, nell'esempio che segue, il simbolo `@`: esso verrà sostituito col nome di dominio corrispondente a questo file, definito in `named.conf`

```
$TTL   86400
@      IN     SOA         localhost.  root.localhost.  (
                          2014030101  ; Serial
                          10800       ; Refresh after 3 hours
                          3600        ; Retry after 1 hour
                          604800      ; Expire after 1 week
                          86400 )     ; Minimum TTL of 1 day
       IN     NS          localhost.
1      IN     PTR         localhost.
```

- `/etc/named.hosts` è lo zone file per la risoluzione diretta;

- `/etc/named.rev` è lo zone file per la risoluzione inversa.

```
$ORIGIN example.com.     ; designates the start of this zone file in the namespace
$TTL 1h                  ; default expiration time of all resource records without their own TTL value
example.com.  IN  SOA   ns.example.com. username.example.com. ( 2007120710 1d 2h 4w 1h )
example.com.  IN  NS    ns                    ; ns.example.com is a nameserver for example.com
example.com.  IN  NS    ns.somewhere.example. ; ns.somewhere.example is a backup nameserver for example.com
example.com.  IN  MX    10 mail.example.com.  ; mail.example.com is the mailserver for example.com
@             IN  MX    20 mail2.example.com. ; equivalent to above line, "@" represents zone origin
@             IN  MX    50 mail3              ; equivalent to above line, but using a relative host name
example.com.  IN  A     192.0.2.1             ; IPv4 address for example.com
              IN  AAAA  2001:db8:10::1        ; IPv6 address for example.com
ns            IN  A     192.0.2.2             ; IPv4 address for ns.example.com
              IN  AAAA  2001:db8:10::2        ; IPv6 address for ns.example.com
www           IN  CNAME example.com.          ; www.example.com is an alias for example.com
wwwtest       IN  CNAME www                   ; wwwtest.example.com is another alias for www.example.com
mail          IN  A     192.0.2.3             ; IPv4 address for mail.example.com
mail2         IN  A     192.0.2.4             ; IPv4 address for mail2.example.com
mail3         IN  A     192.0.2.5             ; IPv4 address for mail3.example.com
```

Figura 48: Esempio di zone file

Zone file File di testo che descrive un sottoinsieme di domini (o, più spesso, un singolo dominio). Ogni riga viene detta *Resource Record* (RR) ed è in forma

name	ttl	record class	record type	record data

Figura 49: Formato di un RR.

dove:

- **name** è il nome di dominio (in genere si usa `@` per riferirlo al dominio definito nello zone file);
- **ttl (time to leave)** è il tempo di permanenza del RR nella cache di un sistema remoto;
- **record class** ha sempre valore `IN`. Indica che il record è un INternet DNS RR;
- **record type** indica il tipo di RR;
- **record data** contiene informazioni specifiche del tipo di RR.

I record più comuni in uno Zone file sono chiamati *standard resource record* e sono:

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy

Figura 50: Tipi di record RR

- `SOA` (Start Of Authority): segna l'inizio di uno Zone file (in genere è il primo record; ne esiste uno per zone file);
- `NS` (Name Server): nome del server che ha autorità sul dominio;
- `A` (Address record): associa un hostname ad un indirizzo IP;
- `PTR` (domain name PoinTeR): permette di associare indirizzi IP ad un hostname;
- `MX` (Mail eXchanger): definisce il server che gestisce la posta per un host o un dominio;
- `CNAME` (Canonical NAME): definisce un alias per il nome di un host.

Per avviare il servizio DNS si usa il comando `named`, con la sintassi

```
named [

      -c configfile     //path di named.conf
      -d level          //attiva il debugging
      -p portnumber     //default:  53
      -n ncpus          //sfrutta i sistemi multiprocessore
      -t directory
      -u user
]
```

Debugging I principali strumenti di debugging del DNS sono: `dig` e `nslookup` (obsoleto).

5.2.7 NIS

Network Information Service: inizialmente chiamato **YP** (Yellow Pages), è un servizio spesso utilizzato nel contesto di applicazioni parallele e distribuite che permette di definire delle risorse di amministrazione comuni ad un insieme di host, in modo che l'utente possa utilizzare host differenti mantenendo gli stessi username, password, cartella home e permessi. Funziona per mezzo di un database (in formato **NIS map**) collocato nel master server, il che permette un controllo centralizzato e la condivisione automatica delle risorse. Le NIS map sono rese disponibili ai client tramite il processo `ypserv` e vengono aggiornate dinamicamente tramite il demone `ypbind`. Sia il server che i client fanno parte di uno stesso *NIS domanin*, il cui nome può essere stabilito tramite il comando `domainname` *`domain`*, mentre `ypwhich` serve a visualizzare l'indirizzo del server.

5.2.8 HTTP

HyperText Transfer Protocol: principale sistema che permette la trasmissione di informazioni sul Web, al fine di realizzare sistemi informativi distribuiti, collaborativi ed ipermediali (ossia composti da *multimedialità* distribuita nella rete ed acceduta mediante *hyperlink*[17]). Utilizza il protocollo TCP sulla porta 80.

Storia HTTP è utilizzato dal WWW dal 1990. Se ne sono susseguite diverse versioni:

- **HTTP/0.9**: semplice protocollo per il trasferimento di dati grezzi sulla rete Internet, gestito dal W3C;
- **HTTP/1.0** (RFC 1945): pur consentendo il trasferimento di messaggi di tipo MIME, non era adatto a supportare la crescita esponenziale del WWW;
- **HTTP/1.1**: versione consolidata del protocollo, usato per 15 anni per lo sviluppo del Web;
- **HTTP/2** (RFC 7540): nuovo standard basato sul protocollo SPDY/2, quest'ultimo sviluppato da Google. Questa nuova versione migliora di molto le prestazioni, senza bisogno che le applicazioni preesistenti necessitino di modifiche.

Funzionamento L'HTTP ha un'architettura di tipo client/server *stateless*[18] e comprende due tipi di messaggi: quelli di richiesta e quelli di risposta.

- **HTTP Request**: inviato dal client verso un server, è composta da:
  - **request line**: riga di richiesta composta da metodo di richiesta (`GET`, `POST`, `HEAD`, `PUT`, `DELETE`, `TRACE`, `OPTIONS` o `CONNECT`), URI e versione del protocollo;
  - **header**: riga che contiene informazioni aggiuntive, tra cui l'host e l'*user-agent* (tipo di client), seguita da una riga vuota;
  - **body**: corpo del messaggio.
- **HTTP Response** inviato dal server, è di tipo testuale ed è composto da:
  - **status line**: riga di stato che riporta un codice a tre cifre per identificare lo stato della risposta (`1xx`: informational, `2xx`: successful, `3xx`: redirection, `4xx`: client error, `5xx`: server error);
  - **header**: è composto da i campi server (tipo di server) e content-type (tipo di contenuto restituito in codifica MIME) e seguito da una riga vuota;
  - **body**: contenuto della risposta.

HTTPS Adattamento dell'HTTP per comunicazioni sicure, utilizza un protocollo crittografico a doppia chiave. La comunicazione criptata avviene sulla porta 443. Esiste in due varianti che differiscono per il protocollo crittografico utilizzato:

- SSL (Secure Sockets Layer): ogni server deve avere un certificato X.509, emesso da una *certificate authority* (CA) e contenente:
  - chiave pubblica,

[17] Collegamenti ipertestuali.
[18] Un protocollo di comunicazione stateless non salva informazioni sulla sessione e quindi interpreta ogni messaggio indipendentemente dagli altri.

- *distinguished name* del server (nome ed indirizzo),
- numero di serie o data di pubblicazione dei certificato,
- data di fine validità del certificato;

- TLS (Transport Layer): è l'evoluzione di SSL, definita nell'RFC 2246 (SSL 3.1). Si articola nelle seguenti fasi:

  1. Negoziazione degli algoritmi da utilizzare,
  2. Scambio delle chiavi,
  3. Autenticazione,
  4. Cifratura simmetrica.

5.2.9 NFS

Network File System: permette di condividere directory e file su rete, riducendo l'occupazione dello spazio su disco locale.
Lato client, l'inserimento di una directory collocata in un host remoto viene detto *mounting* ed è realizzato tramite il comando `mount`.
Lato server, la condivisione di una cartella con un host specifico è detta *sharing* ed è ottenuta mediante il comando `export`. NFS è modulare, suddiviso in tre parti indipendenti:

- **NFS**, implementata da:
  - `nsfd [nserver`[19]`]`, demone lato server che gestisce le richieste NSF,
  - `biod [nserver]` demone lato server che gestisce l'I/O dei client;
- **RPC** (Remote Procedure Code), implementata da:
  - `rpc.locked` demone che gestisce i *lock files* che bloccano istanze multiple di processi specifici,
  - `rpc.statd` demone che controlla lo stato della rete,
  - `rpc.mountd` demone lato server che risponde alle richieste di mount;
- **XDR** (eXternal Data Representation), che consente la condivisione dei file a prescindere dalla codifica specifica di ognuno.

5.2.10 SNMP

Simple Network Management Protocol: protocollo per la gestione di reti internet che permette ad uno o più DTE detti *manager* di accedere e modificare, attraverso UDP sulle porte 161 e 162, alcune informazioni elementari dei vari dispositivi di rete, detti *agents*. Le informazioni gestiste nei vari *agents*, dette oggetti (in inglese *managed objects*), vengono raccolte in un database chiamato MIB. La terza versione del protocollo rimedia alle carenze in merito a sicurezza e privacy delle versioni precedenti tramite un sistema di autenticazione e strumenti di controllo degli accessi. In particolare, maschera le informazioni per proteggerle da modifiche non autorizzate (*authentication*) e ne garantisce la riservatezza.

MIB Management Information Base: archivio di informazioni di gestione inserite dagli *agent*.

SMI Structure of Management Information: insieme delle regole, specificate per mezzo dell'ASN.1 che definiscono i nomi e la codifica delle variabili MIB.

OID Object IDentifer: contiene i criteri per definire un oggetto. Si segue una struttura ad albero di standard e si pone qualsiasi oggetto o standard in una regione precisa dell'albero.

5.3 Posta elettronica

La posta elettronica é un servizio che coinvolge due programmi: il **Mail User Agent** ed il **programma di trasporto**, di cui è un esempio *SendMail*.

[19] Numero di processi da eseguire

5.3.1 MUA

Il Mail User Agent costituisce un'interfaccia utente che offre funzionalità di composizione, visualizzazione, archiviazione ed eliminazione (automatica, tramite filtri, o manuale) dei messaggi. I principali protocolli che consentono l'interazione tra MUA e protocollo di trasporto sono POP3 e IMAP.

POP3 Il Post Office Protocol, noto anche come *Popper*, permette l'accesso da remoto ad un server di posta elettronica in ascolto sulla porta 110. Si tratta di un'applicazione client-server in cui la connessione é stabilita tramite il protocollo TCP/IP. Client e server si scambiano comandi (sintassi: `keyword` *`argomento`*) e risposte (sintassi: `state keyword info`), in un dialogo articolato in quattro fasi:

1. apertura di una connessione TCP/IP e invio di un messaggio di benvenuto al client da parte del server;
2. **authorization**: il client effettua il login in chiaro, tramite i comandi `USER` e `PASS`;
3. **transaction**: il client richiede azioni al server. I comandi utilizzati sono:
   - `STAT`, che restituisce numero e dimensione totale dei messaggi),
   - `LIST [msg]`, che elenca id e dimensione del/i messaggio/i specificato/i,
   - `RETR msg`, per la ricezione del/i messaggio/i specificato/i,
   - `DELE msg`, per la cancellazione del/i messaggio/i specificato/i,
   - `NOOP`,
   - `LAST`, che indica il messaggio con id più alto ricevuto,
   - `RSET`, per la marcatura dei messaggi da cancellare;
4. **update**: rilascio delle risorse acquisite e chiusura della sessione, tramite il comando `QUIT`.

IMAP L'Interactive Mail Access Protocol, definito negli RFC 1064 e 2060 e attualmente alla sua quarta versione, è un metodo per l'accesso dinamico alle mailbox più moderno ed efficiente di POP3, specialmente nei casi, oramai all'ordine del giorno, in cui l'utente ha necessità di accedere alla propria casella di posta da più di un client simultaneamente. Esso è inoltre dotato di potenti strumenti di ricerca delle informazioni e di gestione dei contenuti multimediali (vedi MIME). IMAP, che utilizza la porta 143, associa ai messaggi delle flag di sistema, che ne definiscono lo stato, ad esempio `\Seen`, `\Answered`, `\Flagged`, `\Deleted`, `\Draft` e `\Recent Message`.

5.3.2 Programma di trasporto

Il programma di trasporto si occupa del trasferimento dei messaggi e del servizio di notifica all'utente, ossia della gestione della ricevuta di ritorno, utile per rilevare i casi in cui l'utente finale non riceve la mail.
Per trasferimento s'intende il meccanismo con il quale il messaggio viene effettivamente trasmesso: nel momento in cui il MUA procede all'invio di un messaggio, viene attivata una sessione con il server di destinazione e il programma di trasporto trasferisce l'e-mail tramite il protocollo **SMTP**.

SMTP Il Simple Mail Transfer Protocol é adibito al trasporto di messaggi, efficiente ed affidabile, in ambienti eterogenei. Il trasferimento é indipendente dal tipo di rete e avviene tra due interfacce IPCE (Inter Process Communication Environment). Ad ogni richiesta da parte dell'utente, tramite il comando `HELO` viene attivato un canale di comunicazione bidirezionale sulla porta 25 tra il server SMTP trasmettitore (*sender*), che invia i comandi, e quello ricevente (*receiver*), che invia le risposte. Una volta creato il canale, l'SMTP-sender invia il comando `MAIL`[20], che contiene i dati riguardanti il mittente, e il receiver risponde con `OK`.
Il sender invia poi il comando `RCPT`, contenente i dati del destinatario, seguito da `DATA`. Se il receiver non puó rispondere, invia un codice di reject. Ogniqualvolta il receiver interpreta correttamente un messaggio risponde con `OK`. Altri comandi utilizzati durante la sessione sono `NOOP`, `HELP`, `EXPN` e `VRFY`. La sessione termina sempre con `QUIT`. Tale dialogo é bloccante.

[20] Comandi alternativi a `MAIL` sono `SEND`, `SOML` e `SAML`

Configurazione di Sendmail La configurazione manuale di Sendmail (file `sendmail.cf`) è diventata nel tempo talmente complessa da essere sconsigliata. Essa viene semplificata tramite uno pseudolinguaggio compilato, **M4**.

MIME Per poter far fronte alle nuove esigenze di codifica di caratteri speciali e contenuti multimediali, gli RFC 1341 e 1521 hanno introdotto lo standard di codifica MIME (Multipurpose Internet Mail Extensions). Esso aggiunge nuovi header rispetto al RFC 822 senza influire sul normale funzionamento del programma di trasporto, tra i quali il content-type, che descrive il tipo di contenuto.

Mail relay Quando un dominio di posta è particolarmente importante, occorre definire un gestore di posta secondario, che in caso di malfunzionamenti sia in grado di salvare temporaneamente i messaggi in transito, facendo le veci del server di destinazione, in modo che eventuali anomalie non abbiano conseguenze sul mittente. Tale funzione, tuttavia, è stata a lungo sfruttata dagli spammer, che si fingevano server secondari. Attualmente si suole dunque indicare espressamente gli host dai quali si accetta relaying in un'apposita tabella.

Posta elettronica privata La crittografia ed i certificati digitali permettono di garantire la segretezza della corrispondenza. Esiste la possibilità, difatti, di configurare il proprio MUA per l'uso, ad esempio, di GPG (GNU Privacy Guard, equivalente libero di PGP) tramite il plugin Enigmail. La PEC (Posta Elettronica Certificata) è la modalità di attuazione italiana, istituzionalizzata, del concetto di posta elettronica privata.

6 Sicurezza di rete

Minacce Ogni host connesso ad una rete è sottoposto ad un gran numero di minacce, ad esempio **accessi non autorizzati** o **DoS** (*Denial of Services*, la negazione di servizi all'utente autorizzato). Esistono diversi strategie per proteggere una rete da questi ed altri attacchi, le principali delle quali sono Oscuramento, Hardening e uso di Firewall.

6.1 Oscuramento

Per oscuramento si intende il garantire la sicurezza nascondendo le risorse di rete mediante strumenti come Packet filtering, IP Masquerading, GPG e trasmissioni crittografate.

6.1.1 Encryption

Limita gli accessi ai dati trasmessi, crittografando i contenuti. In ambienti Unix, si usano i comandi `crypt` e `des`.

6.2 Hardening

Per hardening si intende la gestione della sicurezza a livello del singolo host.

6.2.1 TCP-wrapper

I TCP-wrapper consentono di limitare l'accesso ai servizi basandosi sull'IP e l'hostname del client. Le richieste verso l'host vengono elaborate dal wrapper, che verifica che l'indirizzo del chiamante sia incluso nell'elenco di `/etc/hosts.allow`: se è così, o se non è incluso in `/etc/hosts.deny`, permette l'accesso. Tramite le seguenti **keyword** è possibile inoltre specificare host o gruppi di host:

- `ALL` (tutti gli host),
- `LOCAL` (tutti gli host locali),
- `KNOWN` (host riconosciuti dal sistema),
- `UNKNOWN` (host non riconosciuti),
- `PARANOID` (host il cui nome non corrisponde all'indirizzo).

In entrambi file è anche possibile definire delle **regole di filtraggio**, che hanno effetto dal basso verso l'alto; inoltre quelle di `hosts.allow` hanno la precedenza su quelle di `hosts.deny`. Il formato delle regole è:

`<elenco-servizi> : <elenco-client> [: spawn`[21] `<comando-shell>]`

6.2.2 xinetd

Demone che estende le funzionalità di `inetd`, non si limita a gestire l'accesso ai servizi di rete, ma controlla anche i servizi stessi al Livello delle applicazioni. Viene configurato mediante `/etc/xinetd.conf` ed altri file (uno per ogni servizio) posti nella directory `/etc/xinetd.d`, da importare nel file di configurazione generale di xinetd mediante il comando `includedir`.

6.3 Firewall

Sistema hardware e/o software che costituisce un intermediario tra la rete locale (o singolo host) ed una o più reti esterne (tipicamente internet), filtrando il traffico. Tipicamente, un firewall è un DTE con più schede di rete che costituisce l'unico punto di collegamento tra le reti coinvolte.
Nella rete interna ci saranno i servizi di base (come NFS, NIS, LDAP etc.) rivolti agli utenti della sottorete interna; nella rete esterna i servizi di networking (ad esempio DNS, SMPT, FTP etc.), rivolti sia ad utenti interni che esterni e dunque esposti a rischi.
Nonostante permetta di isolare la rete dal mondo esterno, non è in grado di proteggerla da attacchi interni o condotti da linee da lui non controllate. Si distinguono due tipi di firewall:

- firewall **stateless**, che prendono decisioni basate esclusivamente sulla specifica connessione. Un esempio di questo tipo di firewall è `ipchains`;

[21] permette di eseguire normali comandi da shell qualora una richiesta entrante soddisfi una regola.

- firewall **stateful**, più sofisticati, che tengono traccia delle connessioni e prendono dunque decisioni basate anche, ad esempio, su frequenza e circostanze delle varie connessioni. Un esempio di questo tipo di firewall è il firewall implementato nell'attuale kernel linux (vedi Packet filtering), che ha rimpiazzato `ipchains`.

Packet filtering Metodo con il quale un firewall limita il traffico di rete.
In Linux, a partire dal kernel 2.4, ***NetFilter*** è il filtro di pacchetti implementato nel kernel, la cui interfaccia è rappresentata dal comando `iptables`[22].
NetFilter contiene alcune tabelle (*tables*): ogni tabella è associata a un diverso tipo di elaborazione dei pacchetti. Essa contiene dunque una serie di catene (*chains*) di regole di filtraggio, almeno una delle quali viene attraversata sequenzialmente da ogni pacchetto. Una regola in una catena può causare un salto ad un'altra catena. Le regole (*rules* sono composte da un campo *match* ed un campo *target*).
Nel corso dell'attraversamento di una catena, si controlla se il pacchetto soddisfa il campo *match*: se così accade, il pacchetto subirà il *target* e le regole successive saranno ignorate, altrimenti verranno applicate le regole base (*policy*), definibili a loro volta tramite `iptables`.
Le tabelle di iptables sono:

- **filter**: regolamenta il firewalling vero e proprio, inteso come filtraggio; permette cioè di far passare i pacchetti `ACCEPT`, rifiutarli ed avvisarne il mittente con un messaggio di errore `REJECT` o scartarli senza alcuna forma di notifica `DROP`. Le catene predefinite di suddetta tabella sono:
  - `INPUT`: vi passano i pacchetti destinati al firewall stesso,
  - `OUTPUT`: vi passano i pacchetti originati dal firewall stesso, diretti altrove,
  - `FORWARD`: vi passano i pacchetti che transitano nel firewall pur provenendo da altri host, diretti altrove;
- **nat**: regola le attività di natting, ossia di modifica degli indirizzi IP nell'ambito dell'Oscuramento. Consiste solitamente nel tradurre gli indirizzi di una rete privata, globalmente non univoci, in un unico indirizzo IP pubblico, in modo da consentire alla LAN di connettersi ad Internet e di nasconderla. Le catene predefinite di suddetta tabella sono:
  - `PREROUTING`: vi passano i pacchetti su cui non sono ancora state fatte scelte di routing,
  - `POSTROUTING`: vi passano i pacchetti su cui sono già state fatte scelte di routing,
  - `OUTPUT`: come in filter, vi passano i pacchetti originati dal firewall stesso, diretti altrove;

  `PREROUTING` e `POSTROUTING` sono state introdotte per consentire di realizzare particolari comportamenti: ad esempio, se si vuole cambiare l'indirizzo di destinazione di un pacchetto sarà importante farlo prima che venga deciso da dove fare uscire il pacchetto (se così non fosse, il pacchetto uscirebbe dall'interfaccia sbagliata, mentre quando si cambia l'indirizzo del mittente di un pacchetto potrebbe essere importante farlo dopo che una decisione di routing è stata presa. I possibili target sono:
  - `SNAT`, che consente di cambiare l'indirizzo ip sorgente di un pacchetto (`POSTROUTING`). Questa azione viene solitamente intrapresa per avere la possibilità di avere indirizzi privati già utilizzati da altre LAN senza creare conflitti o per nascondere la rete privata dall'esterno sotto un indirizzo pubblico (IP Masquerading).
  - `DNAT`, che consente di cambiare l'indirizzo ip destinazione di un pacchetto (`PREROUTING`),
  - `MASQUERADE`: tipo particolare di `SNAT`, che fa in modo che i pacchettini abbiano come mittente l'indirizzo IP della interfaccia di rete dalla quale usciranno (`POSTROUTING`),
  - `REDIRECT`, versione semplificata del `DNAT` che consente di cambiare la porta di destinazione di un pacchetto (`PREROUTING`);
- **mangle**: responsabile delle modifiche alle opzioni dei pacchetti. Ha per catene predefinite:
  - `PREROUTING`: esamina tutti i pacchetti che entrano nel sistema (prima di sapere se sono destinati allo stesso o se devono essere inoltrati);
  - `OUTPUT`: tutti i pacchetti generati dal sistema passano per questa catena.

[22] In questo documento si accennerà solamente alla configurazione di un firewall con `iptables`. Per una guida pratica completa, si rimanda a IPtables for Fun.

NetFilter è inoltre in grado di stabilire il *contesto* del pacchetto, cioè se esso è `NEW` (appartenente ad una nuova connessione), `ESTABLISHED` (appartenente ad una connessione esistente), `RELATED` (legato ad una connessione esistente) o `INVALID` (pacchetto sospetto, non legato ad alcuna connessione stabilita) e può essere configurato per comportarsi di conseguenza.
Il packet filtering opera al Livello di rete, per cui non si preoccupa di quali siano le applicazioni che generano il traffico. Tuttavia, non tutti i firewall operano allo stesso livello: ad esempio, un firewall che lavora anche al Livello delle applicazioni è il Proxy.

Architetture di firewall Un firewall può essere configurato in diverse modalità:

- **Screening router** o **firewall router**: il firewall opera un routing filtrato sul traffico tra gli host interni e l'esterno. Sistema basilare, usato per proteggere sottoreti;
- **Dual-homed host**: un host con almeno due interfacce di rete divide il traffico di rete e garantisce i servizi base di rete. Sistema economico ma a *single point of failure*;
- **Screened host**: oltre al firewall router, il traffico tra la rete interna ed esterna passa attraverso un host della rete interna *(bastion host)* il quale fornisce servizi di base. Lo *screening-router* accetta solo pacchetti da e verso il bastion host. L'Hardening del *Bastion Host* deve essere molto curato, in quanto rappresenta il *single point of failure* della rete;
- **Screened sub-net**: viene creata una *rete intermedia* (**DMZ** - De-Militarized Zone) usando un firewall router esterno ed uno interno; i bastion host risiedono nella DMZ rimanendo isolati dalla rete interna, non rappresentando più un punto critico, come anche le workstation che forniscono i servizi più vulnerabili. Il firewall router esterno si limita ad un filtraggio di base in modo da garantire ampia fruibilità dei servizi, mentre quello interno opera un maggior controllo.

6.3.1 Proxy

Con il termine *proxy* si indica un server collocato tra un host e un web server il quale funge da intermediario fra i due, disaccoppiando l'accesso ad internet dal browser. Non occorre forse ricordare che il termine *server* non indica propriamente una macchina, ma un software che vi gira: un proxy è dunque un prodotto software, di cui è un noto esempio SQUID, distribuito sotto la GNU GPL[23]. Più specificamente, un proxy mantiene una cache di pagine visitate di recente e la mette a disposizione dei vari client il cui browser è configurato per utilizzarla, in modo tale da limitare il consumo di banda (anche in maniera consistente, specialmente nei contesti, per esempio aziendali, in cui i diversi utenti, cui il proxy è totalmente trasparente, si servono spesso tutti quanti delle stesse pagine) e, soprattutto, poter filtrare le pagine accessibili in base al loro contenuto. I proxy sono dunque largamente impiegati come Firewall al Livello delle applicazioni, oltre a poter essere utilizzati in catena per garantire l'anonimato in internet (si pensi in particolare al progetto TOR).

6.4 Sicurezza nel web

La capillare diffusione del WWW lo rende forse il servizio più critico.

Cookies Introdotti con Netscape 2.0, i cookies (RFC 2109) sono stringhe di caratteri ASCII che vengono passate dal web server al web browser. Essi vengono inviate dal client ad ogni successivo accesso al sito e hanno la funzione di tenere traccia delle scelte dell'utente per meglio orientare il telemarketing. I cookies pongono problemi nell'ambito della privacy dell'utente. In risposta è nato *eTrust*, un programma messo a punto dalla EFF (Electronic Frontiers Foundation) per definire uno standard per la privacy online.

6.5 Monitoraggio

C'è la possibilità di effettuare un monitoraggio continuo sul sistema usando gli **IDS** (Intrusion Detecting Systems), che possono essere:

- Host-based IDS: verifica periodicamente i log dei servizi di rete e di sistema e controlla l'integrità dei dati e dei filesystem (comandi `diff` ed `rpm -V`)

[23] General Public License

- Network-based IDS: scandisce il traffico di rete alla ricerca di pacchetti sospetti, segnalandoli ed assegnandogli un livello di pericolosità in base a dei database. Lavora impostando in *modalità promiscua* l'interfaccia di rete.

In alternativa agli IDS, si possono utilizzare i comandi Unix-Linux:

- `ps -aux`: mostra i processi attivi;
- `who`: restituisce la lista degli utenti collegati al sistema;
- `last`: mostra il contenuto del file `/usr/adm/wtmp` (registro dei collegamenti al sistema);
- `ls -lR`: crea una lista con le informazioni su ogni file di sistema, la quale può essere poi confrontata con con una precedente tramite il comando `diff`.

Audit trail Detto anche *audit log*, è costituito da uno o più registri che documentano in ordine cronologico le attività svolte entro un sistema, utile per permettere la ricostruzione degli eventi.

Riferimenti bibliografici

[1] Slides e appunti delle lezioni tenutesi nell'ambito dei corsi di *Architettura Reti* e *Reti di calcolatori: protocolli* presso il Dipartimento di Matematica ed Informatica dell'Università degli studi di Perugia, , A.A. 2017-'18

[2] Tanenbaum, Wetherall, *Computer networks*

[3] Contavalli, *IPtables for Fun – Implementare un firewall in Linux*

[4] www.learnnetworks.wordpress.com

[5] www.linktionary.com

[6] www.wikipedia.org

[7] www.duricomeilmetallo.net

[8] www.di-srv.unisa.it

[9] www.fiberopticshare.com

[10] www.tecmint.com

[11] unix.stackexchange.com