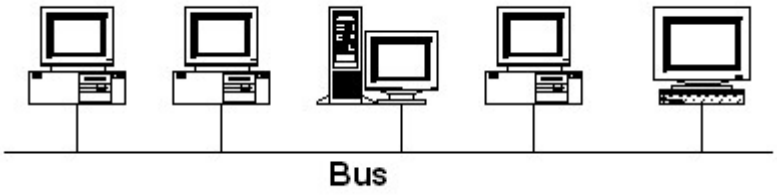
Protocolli e standard di LAN
IEEE 802.3 - CSMA/CD (Ethernet)

Nel documento IEEE 802.3 è standardizzato il sottolivello **MAC** di una rete locale basata sul protocollo **Carrier Sense Multiple Access with Collision Detection** (**CSMA/CD**).



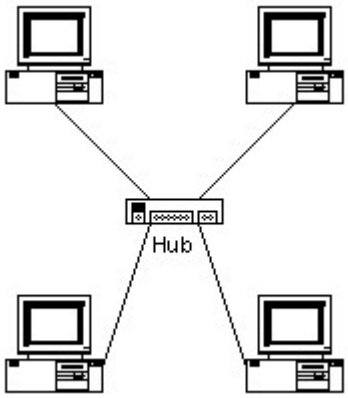
La topologia adottata da questo **protocollo** è quella a **bus**, realizzato tipicamente con **cavo coassiale** a 10 Mb/s. CSMA/CD è un protocollo distribuito privo di **master**, quindi operante in modo paritario su tutte le macchine della LAN, che permette alle stazioni di condividere l'utilizzo del mezzo trasmissivo. Il protocollo, essendo di tipo ad accesso casuale al mezzo, non esclude il verificarsi di collisioni; prevede quindi un meccanismo di riconoscimento delle collisioni da parte delle stazioni coinvolte, in modo che esse possano ritentare la trasmissione in un tempo successivo. Con questo approccio, comunque non è possibile evitare il fenomeno delle collisioni per via dei tempi di propagazione non nulli e della lunghezza delle trame trasmesse.

Lo standard 802.3 proposto da **IEEE** è l'evoluzione di una soluzione per reti locali proposta nei primi anni '80 da un consorzio formato da *Digital*, *Intel* e *Xerox*, chiamata **Ethernet**. Le differenze tra i due standard sono talmente minime da renderli compatibili: su una stessa rete locale ci possono essere contemporaneamente alcune macchine che implementano l'802.3 ed altre che usano *Ethernet*.

Evoluzione di Ethernet

La rete locale di tipo **Ethernet** (o 802.3) ha avuto un notevole successo commerciale nell'ambito dell'automazione d'ufficio, tale da renderla la rete locale per antonomasia e da farne oggetto di continui miglioramenti ed evoluzioni.

Un cambiamento importante è avvenuto nel tipo di mezzo trasmissivo utilizzato: dal **cavo coassiale**, delicato e soggetto a rotture, si è passati all'utilizzo del più robusto ed economico **doppino** telefonico, che nella sua forma più evoluta presenta una larghezza di **banda** molto maggiore, tale da permettere velocità di trasmissione di 100 Mb/s (***Fast Ethernet***). Inoltre, a differenza del coassiale, non essendo il doppino adatto alla realizzazione di un **bus**, è stata necessaria anche un'evoluzione della topologia fisica di *Ethernet*: il *bus* collassa in un apparato chiamato **hub** al quale le stazioni sono connesse tramite collegamenti punto-punto realizzati con doppini, il tutto a formare una topologia a stella di cui l'*hub* rappresenta il centro. L'*hub* è quindi un dispositivo multiporta che agisce solo allo strato 1 ripetendo il segnale proveniente da una **porta** su tutte le altre: esso in pratica simula il mezzo trasmissivo condiviso tra più stazioni.

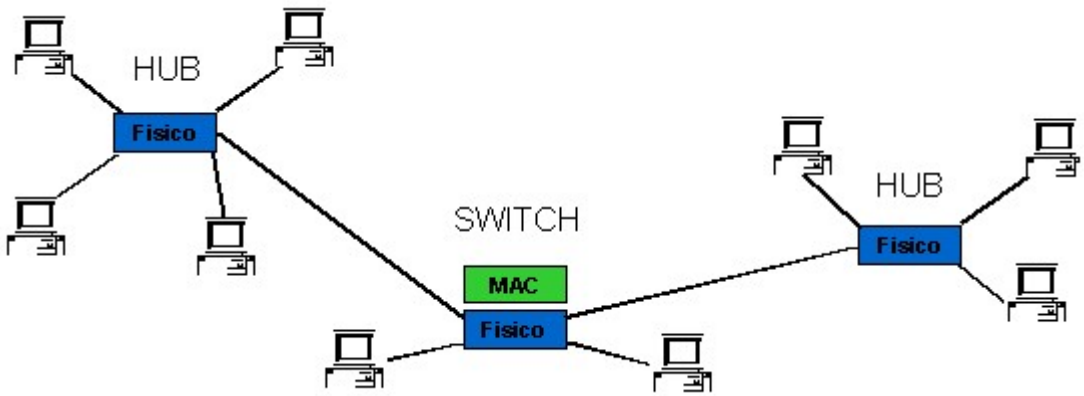


Fattori come la coesistenza di tecnologie diverse, le prestazione limitate in caso di molti utenti e/o di elevato traffico, la ridotta estensione geografica specialmente nel caso di **LAN** ad alte velocità, hanno comportato la scelta di suddividere una LAN in più parti e interconnetterla con i dispositivi appositamente progettati che dialogano a livello **MAC** e che prendono il nome di **bridge**. Inizialmente i *bridge* si limitavano a interconnettere due LAN, successivamente l'evoluzione della topologia da *bus* a stella ha favorito l'adozione di *bridge* multiporta come centro stella, che diventano dei veri e propri commutatori (**switch**). Fra le stazioni direttamente connesse ad uno *switch* non esiste più la condivisione del mezzo e lo *switch* si comporta come un commutatore tra **stazione** sorgente e stazione ricevente.

Ulteriori evoluzioni hanno portato ad una versione di *Ethernet* a 1 Gb/s (***Gigabit Ethernet***), già disponibile sul mercato, e ad un'altra a 10 Gb/s, ancora in fase di sviluppo e basata su collegamenti in fibra ottica.

Domini di collisione

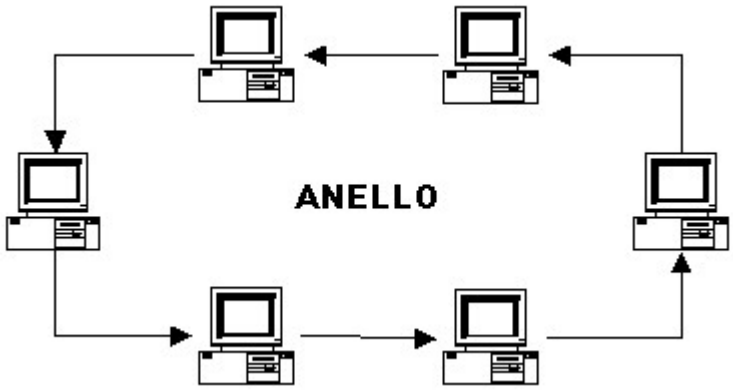
In una rete **Ethernet** si definisce **dominio di collisione** l'insieme delle stazioni che condividono lo stesso mezzo trasmissivo e che quindi possono fra loro collidere in fase di trasmissione. Ad esempio, l'insieme delle stazioni connesse al medesimo spezzone di **cavo coassiale** oppure allo stesso **hub** formano un dominio di collisione. Alle porte dello **switch** possono essere connessi degli *hub*, realizzando in questo modo un'architettura a stella gerarchica, in cui si mantengono separati i domini di collisione. Uno *switch* risulta più efficiente di un *hub* perché isola il traffico locale a ciascuna porta: le stazioni connesse direttamente allo *switch* vedranno solo il traffico **broadcast** e quello diretto a loro stesse, migliorando così l'utilizzazione del mezzo trasmissivo.



IEEE 802.5 - Token Ring

Nel documento **IEEE 802.5** è standardizzato il sottolivello **MAC** di una rete locale basata sul

protocollo **Token Ring**.



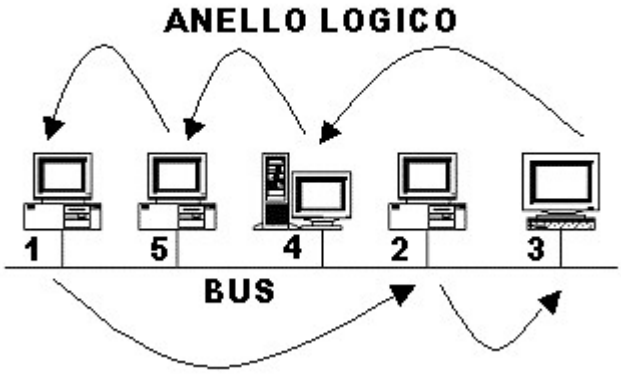
La topologia adottata da questo protocollo è quella ad anello: quando una macchina deve trasmettere, inserisce il messaggio sull'anello, trasmettendolo alla macchina a valle. Ogni macchina riceve il messaggio e lo ritrasmette in avanti, fino a tornare alla macchina sorgente, che toglie il messaggio dall'anello. La macchina destinataria, oltre a ricevere e ritrasmettere il messaggio, in genere ne modifica una parte per confermare al mittente l'avvenuta corretta ricezione. Le velocità di trasmissione consentite dall'802.5 sono 4 e 16 Mb/s.

Il protocollo *Token Ring* è del tipo ad accesso controllato, in cui il trasmettitore deve acquisire il controllo del **canale** prima di poter inviare il messaggio. Il controllo del canale viene realizzato attraverso il possesso di un **token** (gettone), che è un particolare **pacchetto** che ciascuna **stazione** riceve dal segmento a monte e ritrasmette sul segmento a valle; il possesso del *token* indica ad una stazione che l'anello è libero e che, se necessario, si può trasmettere.

Una stazione che intenda trasmettere deve aspettare la ricezione del *token*, catturarlo e quindi trasmettere. Il *token* circola continuamente sull'anello anche se le stazioni non hanno dati da trasmettere. Esso viene generato inizialmente dalla stazione che si è guadagnata il diritto di essere l'*active monitor* della rete e viene ripetuto da tutte le stazioni. Quando una stazione cattura il *token*, essa può trasmettere uno o più pacchetti, in funzione della loro lunghezza e di un parametro detto THT (*Token Holding Time*), che indica il tempo massimo per cui una stazione può trattenere il *token*. A fine trasmissione il *token* viene rimesso in circolazione. Questa metodologia di accesso al mezzo trasmissivo risulta immune alle collisioni. Inoltre, poiché ogni stazione può trattenere il *token* per un tempo al massimo pari a THT, a differenza dell'802.3 il tempo di attesa di ciascuna stazione prima di poter trasmettere di nuovo è limitato superiormente: se ci sono N stazioni nell'anello e, nel caso peggiore, tutte devono trasmettere, il tempo di attesa da quando si rilascia il *token* a quando lo si ottiene di nuovo è al massimo pari a (N-1)XTHT.

IEEE 802.4 - Token Bus

Nel documento IEEE 802.4 è standardizzato il sottolivello **MAC** di una rete locale basata sul protocollo ***Token Bus***. La topologia fisica su cui questo protocollo lavora è, come per l'802.3, un **bus** bidirezionale a 10 Mb/s, ma dal punto di vista logico le stazioni sono disposte secondo un certo ordine: ciascuna **stazione** conosce l'**indirizzo** di chi la precede e di chi la segue e la successiva all'ultima è la prima. In questo modo si crea una topologia logica ad anello, nella quale l'ordine in cui sono disposte fisicamente le macchine è indifferente.

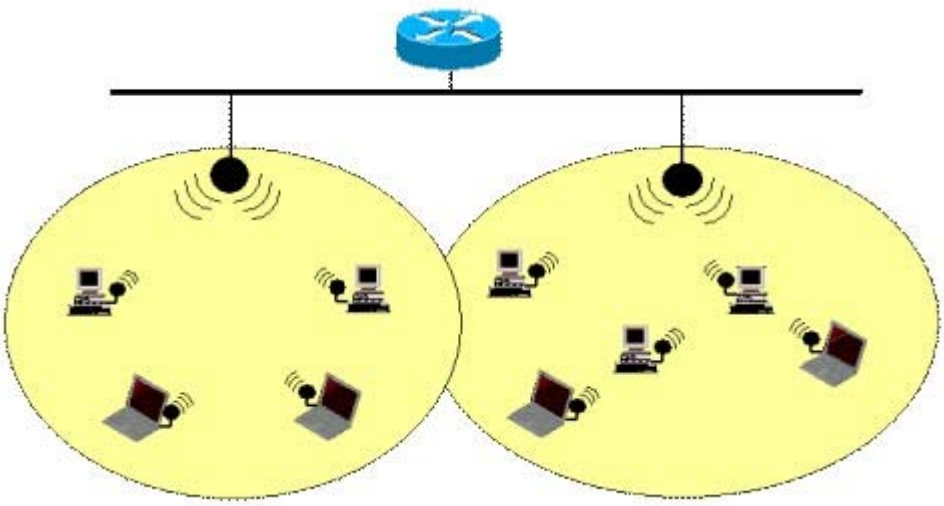


Il funzionamento del protocollo di accesso è simile a quello del **Token Ring**: un **token**, che rappresenta il completo possesso del **canale** e quindi la possibilità di trasmettere senza collisioni, viene trasmesso da una stazione alla successiva rispettando l'ordine dell'anello logico. Anche in questo caso il tempo di attesa del *token* è limitato superiormente.

Il *Token Bus* è una soluzione ibrida nata dalle esigenze di automazione delle linee di produzione nelle fabbriche: da un lato conviene avere una topologia fisica a *bus* (come nell'802.3) che si adatta meglio alla struttura delle catene di montaggio ed è più robusta dell'anello, dall'altro è richiesto un tipo di accesso che offra un tempo di attesa limitato e la sicurezza di assenza di collisioni (come nell'802.5). Naturalmente la gestione dell'anello logico comporta una complicazione del protocollo di accesso, che deve essere in grado di far fronte a disconnessioni di stazioni in spegnimento o malfunzionanti e ad inserimenti di nuove, mantenendo l'integrità dell'ordine logico.

IEEE 802.11 - Wireless LAN

Nel documento IEEE 802.11 è standardizzato il sottolivello **MAC** di una rete locale senza fili (***Wireless LAN***). Questo protocollo nasce dall'esigenza di offrire *connettività mobile* agli elaboratori, cioè dalla necessità di avere una rete locale che copra un'area più o meno limitata in cui la connessione dei *computer* sia realizzata tramite il mezzo radio, superando quindi le limitazioni di mobilità tipicamente causate dal cablaggio.



Lo strato fisico definito nel documento IEEE 802.11 prevede attualmente tre sistemi di trasmissione:

- **Infrarosso**: con velocità di 1 o 2 Mb/s su una lunghezza d'onda tra gli 850 ed i 950 nm;

- ***Spread Spectrum Frequency Hopping***: con velocità di 1 o 2 Mb/s sulla **banda** a 2.4 GHz;
- ***Spread Spectrum Direct Sequenze***: con 7 canali da 1 o 2 Mb/s sulla banda a 2.4 GHz;

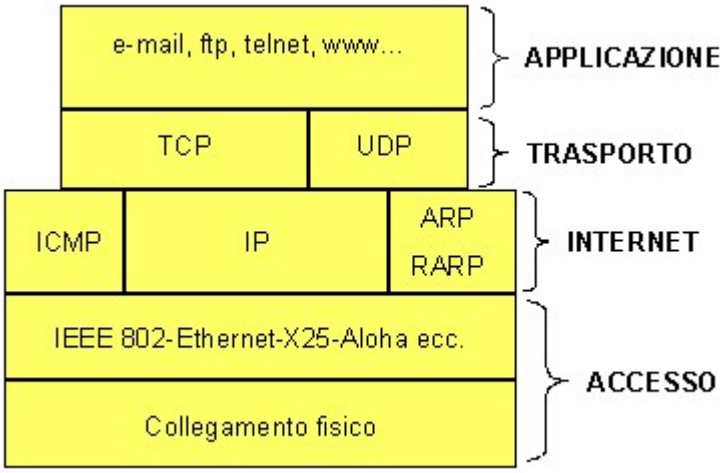
Per la definizione delle problematiche di accesso al mezzo il MAC 802.11 propone due soluzioni possibili:

- una basata su un meccanismo di controllo dell'accesso di tipo distribuito, chiamato ***Carrier Sense Multiple Access with Collision Avoidance*** (**CSMA/CA**), che funziona attraverso un sistema di rilevazione della portante simile al **CSMA/CD** ma che prevede la conferma di ogni **trama** ricevuta correttamente per sapere se c'è stata o meno **collisione**;
- un'altra che utilizza un meccanismo di tipo centralizzato in base al quale l'arbitraggio è comandato da un gestore centrale.

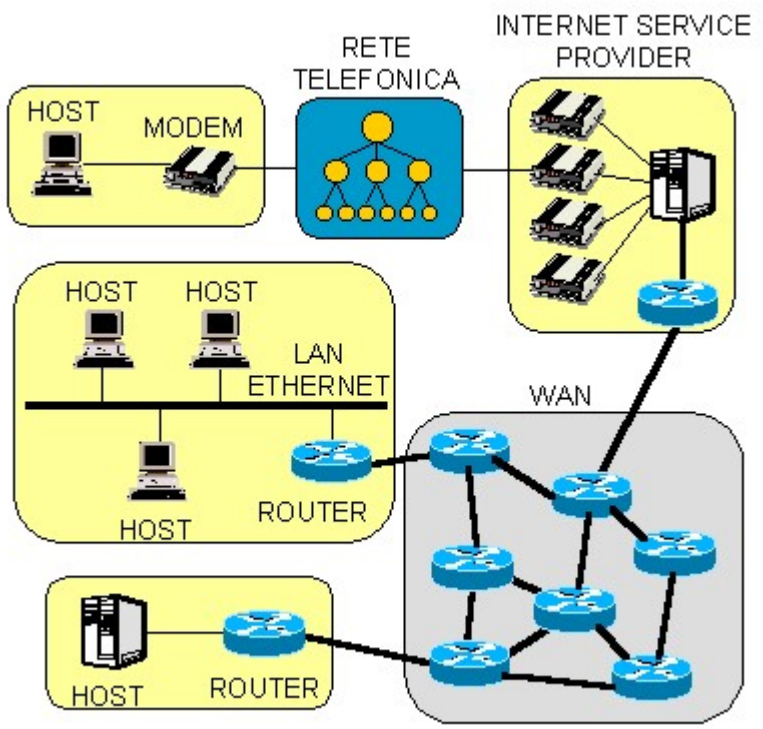
La versione distribuita dimostra particolare efficienza nella gestione di stazioni che colloquiano direttamente oppure in presenza di traffico con caratteristiche impulsive. Un protocollo di tipo centralizzato, invece, si applica tipicamente quando le stazioni *wireless* comunicano fra loro tramite una stazione base interconnessa ad una **LAN** cablata e si scambiano dati sensibili al ritardo e di alta priorità.

La famiglia di protocolli TCP/IP

Si è già visto che la rete **Internet** adotta un modello a strati simile all'ISO-OSI ma con soli quattro strati: Accesso, Internet, Trasporto e Applicazione. Lo **standard TCP/IP** definisce una famiglia di protocolli che lavorano negli strati Internet e Trasporto, i più importanti dei quali sono **Internet Protocol** (**IP**) e **Transmission Control Protocol** (**TCP**).



La rete Internet e la famiglia di protocolli TCP/IP nascono per l'***Internetworking***, tecnica che consente di far comunicare reti differenti nascondendo i dettagli *hardware* di ognuna. In generale si può dire che Internet è una grande *rete di reti*: i *computer*, chiamati **host**, sono distribuiti su tutto il territorio coperto da Internet (che oggi coincide con quasi tutta la parte abitata del globo terrestre) e sono collegati a reti di tipo diverso, che a loro volta sono interconnesse tramite dispositivi, chiamati **router**, capaci di adattarsi a qualunque tipo di struttura fisica e topologica delle varie reti.



Nessuna specifica è fornita per gli strati sotto **IP**, in quanto relativi alla singola sottorete di appartenenza degli *host* o *router*. IP svolge funzioni di rete e instradamento dei pacchetti (tipici dello strato 3 OSI), mentre **TCP** svolge le funzioni di controllo della connessione *end-to-end* (relativi allo strato 4 OSI). Lo strato di applicazione definisce programmi e protocolli utilizzati per fornire servizi all'utente, quali la navigazione sul *Web*, la posta elettronica, il trasferimento di file e molti altri.

Il protocollo di rete IP

Il collante che tiene insieme la rete **Internet** è il **protocollo** di livello rete, comunemente chiamato **IP** (***Internet Protocol***). A differenza dei vecchi protocolli di livello rete, il protocollo IP è stato progettato tenendo in mente le problematiche di *Internetworking*. Il compito del protocollo IP è quello di fornire una modalità ***best-effort*** (cioè senza garanzie di affidabilità) per trasportare dei **datagrammi** (pacchetti) IP dall'origine alla destinazione senza preoccuparsi se le macchine si trovino nella stessa rete o se ci siano altre reti tra le due macchine.

Il protocollo IP fornisce i seguenti servizi:

- trasmissione di un datagramma *host-to-host*, grazie ad un opportuno schema di indirizzamento;
- funzioni di **routing**, cioè di corretto instradamento delle informazioni attraverso nodi intermedi;
- frammentazione e riassemblaggio dei datagrammi.

Il protocollo, essendo *best-effort*, non fornisce:

- **controllo di flusso**;
- **controllo d'errore**;
- **controllo di sequenza**.

I **router** in rete elaborano il **pacchetto** fino al livello IP, per conoscere quale sia l'**indirizzo** di destinazione; attraverso la **tabella di instradamento** viene quindi deciso su quale interfaccia di rete inviare il pacchetto. La tabella di instradamento è il risultato dell'esecuzione di un particolare

algoritmo di *routing* (statico o dinamico, centralizzato o distribuito). Nella rete Internet sono utilizzati sia protocolli di tipo **Distance Vector** (RIP) che di tipo **Link State** (**OSPF**).

IP supporta le operazioni di frammentazione e riassemblaggio dei datagrammi: il termine frammentazione indica un'operazione in cui una **PDU** (in questo caso il datagramma IP) viene suddivisa o segmentata in unità più piccole. Questa funzione è necessaria perché non tutte le reti adottano la stessa dimensione per le PDU. Senza l'impiego della frammentazione, sarebbe più complicato gestire le incompatibilità tra le dimensioni delle PDU di diverse reti. IP risolve il problema fissando regole di frammentazione per i *router* e regole di riassemblaggio nell'**host** destinazione.

Schema di indirizzamento IP

L'indirizzamento **IP** è parte integrante del processo di instradamento dei messaggi sulla rete. Gli indirizzi IP, che devono essere univoci nell'ambito di tutta la rete **Internet**, sono lunghi 32 bit (4 *byte*) e sono espressi scrivendo i valori decimali di ciascun *byte* separati dal carattere punto (notazione *dotted decimal*). Un **indirizzo** IP ha la seguente struttura:

Il ***Net-ID*** identifica la rete, mentre l'***Host-ID*** identifica l'**host** all'interno della rete. L'indirizzo con i bit relativi alla parte di *host* posti a zero risulta essere l'indirizzo della rete in cui si trova l'*host*, mentre quello con i bit di *host* posti tutti a uno indica l'indirizzo **broadcast** di quella rete, cioè quello usato per inviare pacchetti a tutti gli *host* della rete. Quindi il numero di *host* possibili in una certa rete è pari alla dimensione dello spazio di indirizzamento della parte di *host-id* diminuita di 2 unità. Ad esempio:

- indirizzo IP = 132.125.18.36;
- *net-ID* = 132.125;
- *host-ID* = 18.36;
- indirizzo della rete = 132.125.0.0;
- indirizzo *broadcast* = 132.125.255.255;
- indirizzi possibili = da 132.125.0.1 a 132.125.255.254;
- numero di *host* possibili = (256x256) - 2 = 65.534.

Non sono i nodi ad avere un indirizzo IP, bensì le interfacce. Quindi se un **nodo** ha tre interfacce (ad esempio un **router**), esso ha tre indirizzi IP. Gli indirizzi IP sono univoci a livello mondiale e sono assegnati da un'unica autorità (in realtà l'autorità assegna al gestore di una rete un indirizzo di rete; sarà poi il gestore a decidere quali indirizzi di quella rete assegnare alle proprie macchine). Inoltre, l'indirizzo IP non identifica l'*host* in quanto tale, ma la connessione di un *host* alla relativa rete. Di conseguenza, se una macchina *host* viene spostata in un'altra rete, il suo indirizzo deve essere cambiato.

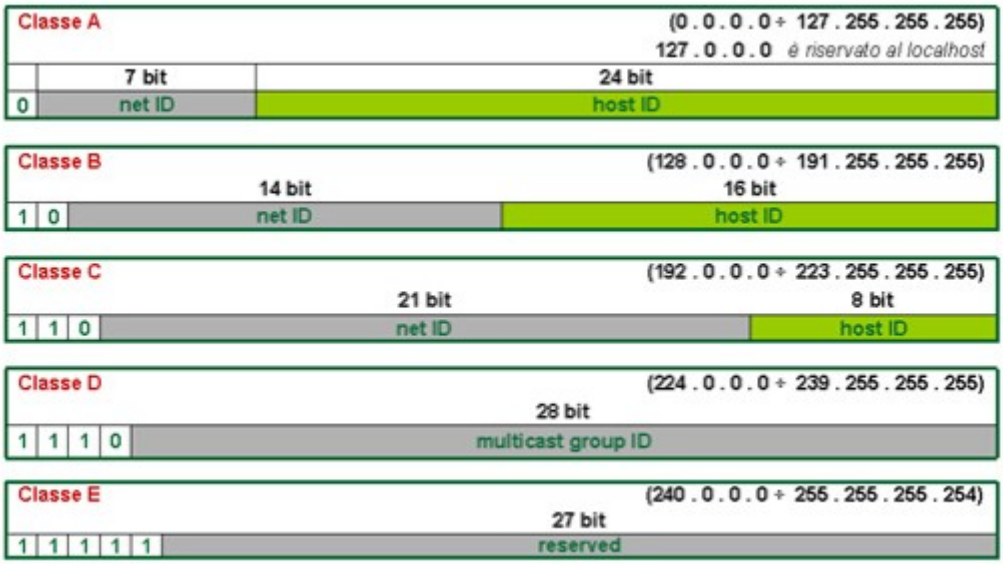
Classi di indirizzi IP

In base al numero di bit assegnati a *net-ID* e *host-ID*, gli indirizzi IP sono suddivisi in cinque classi:

- **Classe A** - Utili per reti che hanno un numero cospicuo di **host**. Il campo *host-ID* è di 24 bit, pertanto possono essere identificati circa 16 milioni di *host* per ogni rete di questo tipo. Sette bit sono dedicati al *net-ID*, per un massimo di 128 reti di classe A.
- **Classe B** - Sono utilizzati per reti di dimensioni intermedie. Il *net-ID* è di 14 bit, per cui si

possono avere al massimo circa 16.000 reti di classe B, ciascuna con una dimensione massima di circa 65.000 indirizzi (*host-ID* da 16 bit).
- **Classe C** - Sono utilizzati per numerose reti con pochi *host*. Le reti di classe C contengono meno di 256 *host* (*host-ID* da 8 bit) e sono individuate da 21 bit nell'ID di rete.
- **Classe D** - Sono riservati al **multicasting**, cioé all'indirizzamento di gruppi di *host*.
- **Classe E** - Sono riservati per usi futuri.

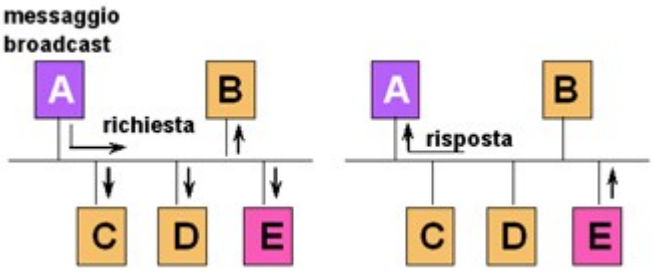
Lo spazio di indirizzamento va partizionato tra le varie classi di indirizzi, in modo che non vi siano sovrapposizioni tra classi diverse. Questo si ottiene fissando, per ogni classe, particolari configurazioni nel primo *byte*.



Corrispondenza tra indirizzi IP e indirizzi MAC

Si è visto come nell'ambito della rete **Internet** ciascun **host**, per poter essere raggiungibile, debba essere connesso tramite un'interfaccia di rete a cui è assegnato un **indirizzo** IP univoco. L'interfaccia di rete (**modem**, scheda *Ethernet*, eccetera) a sua volta implementa un **protocollo** di livello 2 che dipende dal tipo di rete fisica a cui la macchina è connessa. Si è visto anche che, nel caso di reti **LAN**, l'interfaccia deve avere un indirizzo univoco anche a livello MAC, che è cablato nella circuiteria stessa della scheda di rete. Inoltre, un *host* in una LAN deve incapsulare il **datagramma** IP in un pacchetto MAC e quindi inviarlo ad un *host* o ad un **router** nella LAN stessa: per fare ciò è necessario conoscere l'**indirizzo MAC** del destinatario. Nasce così l'esigenza di porre in corrispondenza biunivoca l'indirizzo MAC e l'indirizzo IP di un'interfaccia di rete.

Per effettuare questa operazione, lo standard TCP/IP fornisce un protocollo di risoluzione degli indirizzi chiamato **Address Resolution Protocol** (**ARP**), che gestisce la traduzione degli indirizzi IP in indirizzi fisici e nasconde questi ultimi agli strati superiori. Generalmente, ARP funziona con tabelle di mappatura, definite *cache* ARP, che forniscono la corrispondenza tra un indirizzo IP e un indirizzo fisico. In una LAN, ARP prende l'indirizzo IP di destinazione e cerca l'indirizzo fisico corrispondente nella *cache* ARP: se lo trova lo restituisce al richiedente. Se l'indirizzo richiesto non viene reperito nella *cache* ARP, il modulo ARP effettua una trasmissione **broadcast** sulla rete: questa prende il nome di richiesta ARP (ARP *request*) e contiene l'indirizzo IP richiesto. Di conseguenza, se una delle macchine che ricevono la richiesta riconosce il proprio indirizzo IP nel messaggio di ARP, restituisce una risposta ARP (*ARP reply*) all'*host* richiedente. Il **frame** contiene l'indirizzo fisico dell'*host* interrogato. Quando riceve questo *frame*, l'*host* richiedente inserisce l'indirizzo nella propria *cache* ARP: i datagrammi che verranno successivamente inviati a questo particolare indirizzo IP potranno essere tradotti nell'indirizzo fisico accedendo alla *cache*.



Le informazioni presenti nella *cache* di una **stazione** hanno un tempo di vita che è legato alla specifica implementazione e configurazione del TCP/IP, ma comunque dell'ordine di grandezza dei minuti. Il motivo della temporaneità di tali informazioni è legato al fatto che la corrispondenza tra indirizzi IP e MAC deve essere dinamica e può variare nel tempo (ad esempio a causa di una sostituzione della scheda di rete o di un cambiamento di indirizzo IP).

A volte risulta utile effettuare l'operazione inversa, cioè risalire all'indirizzo IP a partire dall'indirizzo *Ethernet*; tali funzionalità sono assicurate dal protocollo **RARP** (***Reverse Address Resolution Protocol***).

Il protocollo di trasporto TCP

Il **Transmission Control Protocol** (**TCP**) è stato progettato al fine di offrire alle applicazioni un servizio *end-to-end*, orientato alla connessione e perfettamente affidabile, tenendo conto che la rete sottostante (IP) non è affidabile. Il TCP accetta dal livello superiore messaggi di lunghezza illimitata, li segmenta in pacchetti di piccole dimensioni e li invia incapsulandoli in **datagrammi**. Le funzioni svolte dal protocollo TCP sono:

- controllo di errore;
- **controllo di flusso**;
- controllo di sequenza;
- multiplazione delle connessioni su un singolo **indirizzo** di rete.

TCP riceve i dati a flussi dai protocolli di strato superiore che li inviano a *byte*, uno alla volta; quando arrivano allo strato TCP, i *byte* vengono raggruppati in segmenti TCP, che vengono quindi passati a **IP** per essere trasmessi alla destinazione successiva. La lunghezza dei segmenti è determinata da TCP.

Le funzionalità del protocollo TCP vengono garantite mediante la numerazione dei datagrammi e l'invio di messaggi di riscontro (*acknowledgment*) da parte della destinazione ogniqualvolta viene ricevuto correttamente il giusto datagramma della sequenza. Nel caso di connessioni interattive bidirezionali si usa la tecnica del **piggybacking** (*acknowledgment* contenuto nelle risposte). Inoltre, i numeri di sequenza servono a TCP per il riordinamento dei segmenti ricevuti, qualora questi giungano alla destinazione finale in ordine errato. TCP adotta una tecnica di riconoscimento globale, che comprende tutti i *byte* fino al numero di riconoscimento meno uno.

Il modulo TCP ricevente può anche eseguire il controllo del flusso dei dati del mittente, molto utile per evitare la perdita di dati per superamento della capacità del **buffer** e l'eventuale saturazione della macchina ricevente. Il meccanismo si basa sull'emissione di un valore di *finestra* alla **stazione** trasmittente, la quale può inviare un numero specificato di *byte* all'interno di tale finestra; al raggiungimento di questo numero, la finestra viene chiusa e l'entità trasmittente deve interrompere l'invio dei dati.

Poiché TCP è un protocollo che opera in modalità orientata alla connessione, ogni trasmissione di

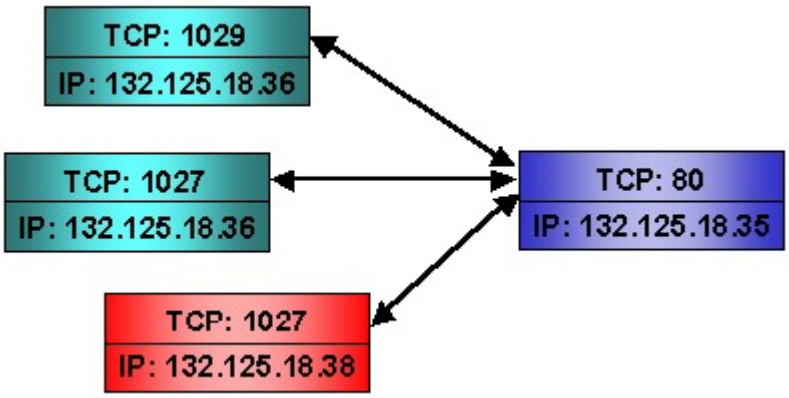
dati deve essere preceduta da una fase di attivazione della connessione e seguita da una fase di rilascio.

Multiplazione e socket

Compito di **TCP** è anche quello di distinguere tra i diversi programmi applicativi e i diversi utenti che fanno uso di uno stesso sistema, quindi di uno stesso **indirizzo** IP. Per questo si è stabilito che ogni sistema contenga un insieme di punti di destinazione TCP chiamati porte. Ogni **porta** è identificata da un intero positivo, che rappresenta un'applicazione attiva nello strato superiore. L'indirizzo completo di un'applicazione su **Internet** è quindi dato dall'insieme di indirizzo IP e porta TCP ed è denominato **socket**; ad esempio:

- indirizzo IP = 132.125.18.35;
- porta TCP = 80;
- *socket* = 132.125.18.35:80.

Il numero di porta è contenuto nell'intestazione del segmento TCP, mentre l'indirizzo IP è contenuto nell'intestazione del pacchetto IP. Questo significa che tutte le sessioni di comunicazione in atto tra due specifici sistemi useranno lo stesso indirizzo IP di sorgente e lo stesso indirizzo IP di destinazione; saranno perciò distinte solo a livello TCP e individuabili tramite la coppia porta sorgente e porta destinazione. Ne segue che queste sessioni sono *multiplate* su un'unica coppia di indirizzi IP, ovvero su un unico **canale** IP di comunicazione. In TCP, quindi, una connessione è identificata da una coppia di *socket*, relativa ai due processi che hanno stabilito la connessione. Ad esempio una connessione tra la porta 1029 dell'**host** 132.125.18.36 e la porta 80 dell'*host* 132.125.18.35 sarà identificata dalla coppia (132.125.18.36:1029,132.125.18.35:80). Grazie a tale meccanismo, un indirizzo di porta di un sistema può supportare connessioni multiple; la porta 80 dell'*host* 132.125.18.35 potrebbe gestire contemporaneamente le seguenti connessioni (ed anche altre):



Well-knows ports

Tipicamente le applicazioni in **Internet** seguono un modello del tipo *client/server*, in cui alcuni *applicativi server* mettono a disposizione determinati servizi che gli *applicativi client* richiedono connettendosi ad essi attraverso TCP/IP. Per identificare i processi applicativi *server*, sono stati definiti dei numeri di porta ben noti (**well-known ports**); per richiedere un certo servizio, un applicativo *client* deve aprire una connessione con la macchina di destinazione sulla ben nota porta *server* che individua quel particolare servizio. Un *client* FTP, ad esempio, per connettersi ad un *server* FTP, deve conoscere e indicare l'**indirizzo** IP dell'elaboratore remoto e il numero della porta associata al servizio **FTP**.

Le porte sono individuate da un numero intero rappresentato con 16 bit. Questo spazio di numerazione è diviso in due gruppi:

- da 0 a 1023 è lo spazio riservato per le porte privilegiate o *well known ports*, che servono per indirizzare un certo servizio;
- lo spazio da 1024 a 65535 è lasciato libero per le porte utenti, cioè quelle scelte dall'applicativo *client* come porta sorgente.

Nella tabella seguente vengono riportati i numeri di porta di alcuni tra i servizi più noti:

Numero porta	**Nome**	**Tipo di servizio**
21	FTP	trasferimento file
22	SSH	terminale virtuale criptato
23	TELNET	terminale virtuale in chiaro
25	SMTP	invio posta elettronica
53	*DOMAIN*	*server* DNS
80	HTTP	*server Web*
110	POP	accesso posta elettronica