Ministero dell'Istruzione, dell'Università e della Ricerca
Servizio Automazione Informatica e Innovazione Tecnologica

Modulo 5

Conoscenze fondamentali sulle reti

ForTIC

Piano Nazionale di Formazione degli Insegnanti sulle Tecnologie dell'Informazione e della Comunicazione

Percorso Formativo C

Materiali didattici a supporto delle attività formative

2002-2004

Promosso da:

- Ministero dell'Istruzione, dell'Università e della Ricerca, Servizio Automazione Informatica e Innovazione Tecnologica
- Ministero dell'Istruzione, dell'Università e della Ricerca, Ufficio Scolastico Regionale della Basilicata

Materiale a cura di:

- Università degli Studi di Bologna, Dipartimento di Scienze dell'Informazione
- Università degli Studi di Bologna, Dipartimento di Elettronica Informatica e Sistemistica

Editing:

CRIAD - Centro di Ricerche e studi per l'Informatica Applicata alla Didattica

Progetto grafico:

Campagna Pubblicitaria - Comunicazione creativa

Scopo e obiettivi del modulo

In questa sezione verrà data una breve descrizione del modulo.
Gli scopi del modulo consistono nel mettere in grado di identificare e descrivere:

- Vantaggi e svantaggi degli ambienti di rete e non di rete.
- Gli aspetti relativi alla sicurezza, *privacy*, ridondanza, eccetera connessi agli ambienti di rete.
- Aspetti relativi alle convenzioni per i nomi (*user-id*, *e-mail*, *password*, eccetera).
- Protocolli e standard di rete

Il modulo è strutturato nei seguenti argomenti:

- **Ambienti di rete**
  - Illustrare vantaggi e svantaggi di ambienti di rete e non di rete.
  - Descrivere ambienti di rete quali *peer-to-peer* e *client/server*.
  - Identificare e discutere aspetti (sicurezza, *privacy*, ridondanza, eccetera) connessi agli ambienti di rete.
  - Identificare e discutere aspetti relativi alla convenzioni per i nomi di *user-id*, *e-mail*, *password*, dispositivi di rete.
- **Modelli correnti e standard**
  - Elencare e definire gli strati dei protocolli di rete TCP/IP e OSI.
  - Identificare e descrivere i più importanti standard di rete IEEE.
- **Topologie LAN**
  - Illustrare le topologie di rete più diffuse.
  - Identificare vantaggi e svantaggi di ogni topologia.
- **Protocolli e standard di LAN**
  - Descrivere le principali funzioni di protocolli *hardware* per LAN.
  - Descrivere protocolli *software* per LAN come TCP/IP.
  - Discutere la natura degli indirizzi IP e degli indirizzi MAC e la relazione tra i due.

Introduzione

Ambienti di rete

Franco Callegati,
Walter Cerroni

Reti di telecomunicazioni

La parola telecomunicazione unisce la radice di origine greca *tele* (lontano) con il verbo latino *comunicare* e significa *trasmissione di informazioni a distanza*.
Trasmettere informazioni a distanza, superando il limite fisico dei nostri sensi, è da sempre un obiettivo dell'uomo, si pensi ad esempi quali la comunicazione tramite luce riflessa da specchi nelle navi da guerra (già utilizzata dagli antichi romani) o la comunicazione con segnali di fumo degli indiani d'america.

Nei tempi moderni si è imparato ad utilizzare i segnali elettromagnetici per la comunicazione a distanza e gli sviluppi della tecnologia nel campo delle **comunicazioni elettriche** e dell'**elettronica** hanno permesso la nascita delle moderne telecomunicazioni.

Una volta che risultino disponibili strumenti per la telecomunicazione, emergono una serie di altri problemi legati all'organizzazione del sistema che si rende necessario per garantire accesso a questo servizio a grandi popolazioni di utenti (siano essi esseri umani o calcolatori). Questi sistemi complessi sono le **reti di telecomunicazioni**.

Alcune importanti date nella storia delle reti di telecomunicazioni sono:

- 1835: viene varato il sistema telegrafico, si può considerare l'inizio delle moderne telecomunicazioni;
- 1846: viene inventata da *Siemens* la telescrivente, il primo terminale automatico;
- 1866: viene posato il primo cavo transatlantico telegrafico;
- 1876: viene brevettato da *Graham Bell* il telefono;
- 1885: nasce la radio con il primo esperimento di Guglielmo Marconi;
- 1887: vengono inventate (*Strowger*) le prime centrali telefoniche automatiche;
- 1956: viene posato il primo cavo transatlantico telefonico;
- 1969: viene realizzata la prima rete di calcolatori, *ARPAnet*, che poi diventerà **Internet** .

Si tenga poi presente che la trasmissione dei segnali elettrici a grande distanza presenta numerosi problemi di carattere tecnico, per cui è molto importante l'ausilio offerto dall'elettronica. A questo proposito due date fondamentali sono:

- 1904: *Hartley* inventa il triodo e nasce l'elettronica;
- 1947: *Shottky* inventa il *transistor* allo stato solido.

Vale la pena sottolineare che sia *Hartley* sia *Shottky* lavoravano per la stessa società di telecomunicazioni statunitense (*Bell System*).

Vantaggi di un ambiente di rete

Il calcolatore elettronico è uno strumento avente lo scopo di elaborare e gestire informazioni. Tali elaborazioni vengono generalmente effettuate sfruttando risorse interne al calcolatore; il processore, le memorie volatili (RAM), le memorie di massa (dischi rigidi, nastri, eccetera). L'interazione fra utente umano e calcolatore, al fine di comandare e/o ottenere i risultati di queste elaborazioni avviene tramite interfacce quali monitor, tastiera, stampante, eccetera, che possono anch'esse essere considerate parte delle risorse a disposizione del calcolatore.

Avere una rete di telecomunicazioni fra calcolatori ha l'ovvio vantaggio di permettere lo scambio di informazioni fra gli utenti dei calcolatori stessi, come ***e-mail*** , documenti ed immagini, eccetera, ma offre anche la possibilità di realizzare una **condivisione delle risorse** di un calcolatore con tutti gli altri nella rete.

Tramite una rete di calcolatori è possibile avere accesso a risorse, siano esse di elaborazione, di memorizzazione, di stampa o quant'altro che altrimenti potrebbero non essere disponibili per tutti, per ragioni di costo, di complessità, eccetera.

Per questo con la progressiva diffusione dei calcolatori si è sempre più sentita la necessità della interconnessione in rete degli stessi, al fine di aumentarne le funzionalità e quindi l'utilità. La rete di calcolatori può quindi essere visto come una sorta di calcolatore esteso che, tramite le funzioni di comunicazione, fa di un insieme di calcolatori isolati un sistema integrato che rende disponibili ad una più vasta popolazione di utenti una serie di risorse.

Ambienti Client/Server e Peer-to-Peer

Nelle reti di calcolatori fino ad oggi tipicamente si è sempre utilizzata una comunicazione di tipo *client/server*. Con questi termini si intende che alcuni calcolatori ben identificabili detti *server* mettano a disposizione informazioni e servizi a cui gli altri calcolatori della rete accedono con modalità opportune. Un tipico esempio è il **WWW** in cui i *server* mettono a disposizione dei *client* pagine di testo, immagini, eccetera, che siano reperibili e visualizzabili

tramite i normali ***browser*** (*Internet Explorer*, *Netscape*, Opera, eccetera).
Questo modello di dialogo è di tipo asimmetrico nel senso che i due soggetti partecipanti alla comunicazione svolgono funzioni diverse: il *server* mette a disposizione le informazioni, il *client* le reperisce e le rende consultabili localmente dall'utente.
Per svolgere questa funzione i *server* devono essere sempre disponibili, quindi sempre accessi, sempre connessi alla rete e sempre pronti ad accettare nuove comunicazioni. Inoltre i *server* devono essere opportunamente configurati al fine di salvaguardare il più possibile l'integrità delle informazioni e del servizio.

Più di recente si sono sviluppati sulla rete **Internet** dei servizi di comunicazione che utilizzano un diverso modello di dialogo, detto *peer-to-peer*. Ciò che cambia è la modalità di fornitura e di reperimento delle informazioni. In pratica il *server* smette di esistere e tutti i calcolatori connessi alla rete possono contemporaneamente agire come *server* e/o come *client*. Nel dialogo *peer-to-peer* si perde quindi la nozione di *server* e tutti i calcolatori possono allo stesso tempo rendere disponibili informazioni e reperirne dagli altri. In questo caso esistono ancora alcuni calcolatori che svolgono funzione di *server* solamente per le funzioni di centralizzazione degli indici di informazioni disponibili. Tramite questi indici i singoli *computer* possono scoprire chi metta a disposizione certe informazioni sulla rete e collegarsi direttamente a questi per il loro reperimento. Il dialogo relativo alle informazioni vere e proprie è quindi sempre diretto fra il fornitore ed il fruitore di informazioni senza l'intermediazione di un *server*. I *server* per l'indicizzazione sono necessari in quanto i singoli calcolatori possono collegarsi e scollegarsi alla rete di dialogo. I singoli calcolatori una volta collegati in rete si connettono a questi *server* per comunicare quali informazioni loro rendano disponibili e per conoscere quali informazioni siano già disponibili e presso chi.

Il primo esempio eclatante di servizio utilizzante un dialogo *peer-to-peer* è il famoso sistema *Napster* per la distribuzione di brani musicali che tanta risonanza ha avuto anche sui mezzi di comunicazione a seguito della battaglia legale per la tutela dei diritti d'autore con le case discografiche.

Sicurezza di un ambiente di rete

Una rete di calcolatori, oltre ad offrire i vantaggi descritti precedentemente, pone un importante problema legato alla sicurezza del sistema informatico.
Le problematiche di sicurezza di un sistema informatico sono state discusse estensivamente in un precedente modulo; qui ci limitiamo ad accennare quali siano i problemi prettamente legati all'ambiente di rete.
La connessione in rete di un calcolatore implica che la rete venga utilizzata per scambiare dati con altri calcolatori e per fornire servizi (*server* di stampa, *server* Internet, eccetera). Le problematiche di sicurezza tipiche di questo scenario sono quindi legate alla riservatezza della comunicazione e al mantenimento dell'integrità dei servizi.

Per quanto riguarda la riservatezza della comunicazione, è necessario evitare:

- che i dati relativi ad una particolare comunicazione fra calcolatori possano essere intercettati e letti, anche senza interromperne il normale flusso (***sniffing***), in quanto questi dati possono essere di tipo sensibile (*password*, dati personali, numero di carta di credito, eccetera);
- che un calcolatore possa comportarsi in modo malevole prendendo il posto di un altro calcolatore, ad esempio assumendone gli indirizzi di rete (***spoofing***), sostituendosi ad esso nella comunicazione con altri al fine di appropriarsi di dati sensibili o per l'uso di servizi a lui non permessi.

Per quanto riguarda invece l'integrità dei servizi è necessario garantirsi dall'eventualità che utenti malevoli, utilizzando la rete di calcolatori possano interferire con il normale funzionamento di sistemi *server*. Un esempio di questo tipo, che ha avuto particolare rilevanza anche sulla stampa, è relativo agli attacchi ai *server* Internet di grandi enti, non avente lo scopo di attentare alla sicurezza dei dati, ma semplicemente di interferire con il normale funzionamento dei *server* (rendere impossibile l'uso della posta elettronica o dei *server Web*, eccetera).

Struttura, funzioni e modo di trasferimento di una rete

Una rete di telecomunicazioni è un sistema che si compone di:

- apparati **terminali** con cui si interfaccia direttamente l'utente finale del servizio di telecomunicazione (spesso l'essere umano);
- **linee di collegamento** che permettono fisicamente la trasmissione a distanza delle informazioni sotto forma di segnali elettromagnetici;
- **nodi di rete** che svolgono le funzioni necessarie a garantire il corretto trasferimento delle informazioni all'interno della rete.

Una rete di comunicazione deve svolgere quattro fondamentali funzioni:

- **Trasmissione**: trasferimento fisico del segnale da punto a punto o da un punto a molti punti.
- **Commutazione**: reperimento delle risorse all'interno della rete necessarie per realizzare un opportuno trasferimento delle informazioni.
- **Segnalazione**: scambio di informazioni fra utente e rete oppure internamente alla rete necessario per il corretto funzionamento della comunicazione e della rete stessa.
- **Gestione**: tutto ciò che concerne il mantenimento delle funzioni della rete; riconfigurazione di fronti a guasti o cambiamenti strutturali, allacciamento di nuovi utenti, tariffazione, eccetera.

Una rete di telecomunicazioni è caratterizzata da un modo di trasferimento, cioé dalla modalità con cui avviene il trasferimento delle informazioni al suo interno. Il modo di trasferimento è, a sua volta, caratterizzato da:

- **schema di multiplazione**: modalità con cui le unità informative condividono le linee di collegamento;
- **modalità di commutazione**: come si realizza la funzione di commutazione;
- **architettura dei protocolli**: la suddivisione delle funzioni di comunicazione e la loro distribuzione fra gli apparati di rete.

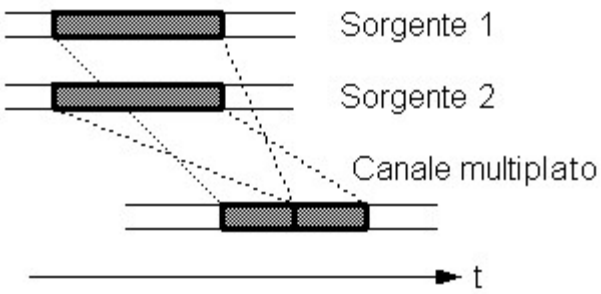
La multiplazione

La multiplazione definisce le modalità secondo cui segmenti informativi emessi da sorgenti diverse condividono la capacità di trasferimento delle informazioni di una linea di collegamento. Infatti solitamente le linee di collegamento di una rete hanno una capacità di trasferimento delle informazioni superiore, anche di molto, a quanto richiesto da una singola sorgente. Si pensi ad esempio ad un cavo telefonico transatlantico, in grado di trasportare in contemporanea centinaia o addirittura migliaia di chiamate telefoniche.

Vi sono diversi tipi di multiplazione:

- multiplazione a divisione di tempo (TDM - *time division* **multiplexing**); il **canale** trasmissivo viene suddiviso in intervalli temporali non sovrapposti assegnati alle diverse sorgenti;
- multiplazione a divisione di frequenza (FDM - *frequency division multiplexing*); la **banda** di frequenze del canale multiplato viene divisa in intervalli assegnati univocamente alle diverse sorgenti;
- multiplazione a divisione di lunghezza d'onda (WDM - *wavelenght division multiplexing*); è usata di recente nelle fibre ottiche, vengono suddivise delle bande di lunghezza d'onda del fascio luminoso entro le quali operano le singole sorgenti;
- multiplazione a divisione di codice (**CDM** - *code division multiplexing*); la banda del canale trasmissivo è condivisa da tutte le sorgenti che risultano distinguibili in funzione della particolare codifica dei bit, diversa da sorgente a sorgente.

Si noti che la tecnica WDM che è un particolare caso della FDM. Attualmente la tecnologia ottica rende possibile avere numerosi canali (fino a 128 e oltre) a diversa lunghezza d'onda (colore) sulla stessa fibra. In questi casi casi si parla di WDM denso o DWDM (*Dense Wavelength Division Multiplexing*).



La commutazione

Per un **nodo** della rete, la **commutazione** è il modo secondo cui una qualsiasi linea di ingresso al nodo viene associata logicamente o fisicamente con una qualsiasi linea di uscita. Lo scopo è di operare uno scambio sul flusso di informazioni dall'ingresso verso l'uscita.

Una commutazione è operata per mezzo delle funzioni di:

- **Instradamento (*routing*)**: è la parte decisionale dell'operazione di commutazione, effettuata dal nodo, che deve stabilire la direzione verso cui inviare un'unità di informazione affinché possa raggiungere la sua destinazione finale;
- **Inoltro (*forwarding*)**: è la parte attuativa dell'operazione di commutazione, che realizza quanto deciso dalla funzione di instradamento, e perciò può essere eseguito solo se quest'ultima è stata applicata.

E' possibile operare due diversi tipi di commutazione: **a circuito** e **a messaggio** o **pacchetto** .

La commutazione di circuito

La rete crea un **canale** di comunicazione dedicato fra due terminali che vogliono colloquiare detto **circuito**. Il circuito è riservato ad uso esclusivo dei terminali chiamante e chiamato. Esiste quindi un ritardo iniziale dovuto al tempo necessario per instaurare il circuito, dopodiché la rete è *trasparente* per gli utenti ed equivale ad un collegamento fisico diretto.

Si possono quindi evidenziare le seguenti fasi della comunicazione:

- Instaurazione del circuito: prima che le informazioni di utente possano essere trasmesse la rete deve instaurare un circuito fra terminale chiamante e terminale chiamato tramite un'opportuna fase di segnalazione.
- Dialogo: i due terminali si scambiano informazioni utilizzando il circuito.
- Disconnessione del circuito: al termine del dialogo il circuito deve essere rilasciato, al fine di poter essere utilizzato per altre chiamate.

L'esempio tipico di rete a **commutazione di circuito** è la *rete telefonica*.

La commutazione di messaggio o pacchetto

Trasporta informazioni in forma numerica.

Le informazioni di utente sono strutturate in **messaggi** unitamente ad opportune informazioni di segnalazione quali indirizzamento,verifica della correttezza delle informazioni, eccetera.

Per ragione di opportunità tecnologica i messaggi vengono solitamente suddivisi in sotto-blocchi detti **pacchetti** , nel qual caso si parla di **commutazione di pacchetto** .

I messaggi o i pacchetti vengono trasmessi da un **nodo** di commutazione all'altro utilizzando in tempi diversi le medesime linee di collegamento (multiplazione a divisione di tempo).

La tecnica a pacchetto si può implementare in due modi:

- nel primo modo vengono creati servizi di rete con connessione;
- nel secondo vengono creati servizi di rete senza connessione.

Nel modo di trasferimento a pacchetto con connessione (a circuito virtuale), viene creato un **canale** virtuale non dedicato tra la sorgente e la destinazione. Al momento della richiesta di comunicazione, ogni nodo assegna un ramo per dare luogo a un connessione logica. I pacchetti verranno instradati sempre lungo il canale virtuale. Al momento di abbattere la comunicazione, i nodi rilasceranno la connessione instaurata.

Un servizio di rete senza connessione (**datagramma**) invece tratta ogni **pacchetto** informativo come una **entità** a sé stante, ogni nodo decide il percorso migliore per il pacchetto nel momento in cui lo riceve, pertanto è possibile che pacchetti facenti parte dello stesso flusso informativo seguano strade diverse, per poi essere ricostruiti a destinazione.

Esempi di reti a commutazione di pacchetto sono la rete telegrafica e tutte le moderne reti di calcolatori, compresa **Internet** .

Pro e contro di circuito e pacchetto

La **commutazione di circuito** offre vantaggi per quanto riguarda la trasparenza temporale del dialogo:

- il circuito è dedicato e garantisce sicurezza ed affidabilità;
- il tempo di trasferimento delle informazioni è costante e dipende solamente dalla distanza fra i terminali e dal numero di nodi da attraversare, in quanto la rete è trasparente al dialogo;
- le procedure di controllo sono limitate ad inizio e fine chiamata.

Al contrario, per le stesse ragioni la commutazione di circuito offre minore flessibilità:

- la velocità di trasferimento delle informazioni è fissata dalla capacità del circuito e non si può variare se non attivando più circuiti in parallelo;

e potenzialmente una minore efficienza:

- se le sorgenti di informazione hanno un basso tasso di attività il circuito è sottoutilizzato.

A proposito di quest'ultima considerazione se si prende ad esempio il circuito che collega il nostro telefono a quello del chiamato quando eseguiamo una telefonata, questo è utilizzato per una percentuale di tempo dell'ordine del solo 30-40%. La ragione di questo è che, in termini medi, durante una telefonata per metà del tempo parliamo e per l'altra metà ascoltiamo, quindi non utilizziamo il circuito in ciascuna direzione all'incirca per il 50% del tempo, a cui si aggiungono le normali pause del parlato portando questo valore a oltre il 60%.

La **commutazione di pacchetto** al contrario risulta più flessibile nell'uso delle risorse di rete, ma meno trasparente:

- poiché le linee di collegamento sono condivise in modo dinamico da più chiamate l'efficienza nella loro

utilizzazione risulta maggiore;
- la rete può supportare dialoghi a diverse velocità ed effettuare anche conversioni tramite memorizzazione;
- è possibile implementare priorità per favorire certi flussi di dati rispetto ad altri.

Tutto questo va a scapito della trasparenza temporale:

- in generale è difficile garantire un predeterminato tempo di transito alle informazioni.

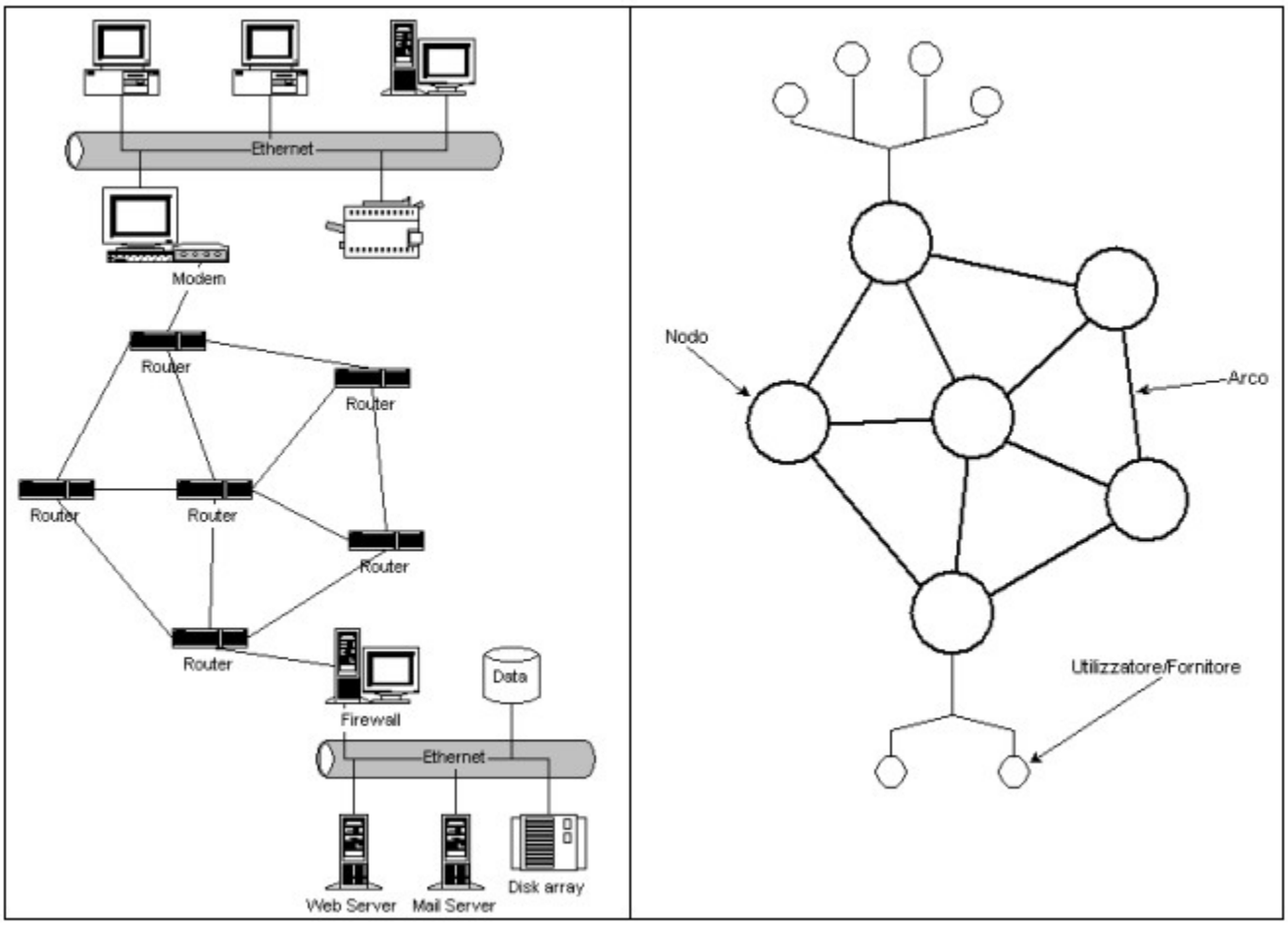
Questa caratteristica rende la commutazione di pacchetto meno adatta per tutti quei servizi che richiedono la consegna dei dati nel rispetto di precisi vincoli temporali, quali la comunicazione voce e video.

Topologie di rete

Una rete di telecomunicazioni può essere rappresentata con un grafo, ossia una struttura logica, composta da nodi e da archi.

I nodi sono gli elementi che raccolgono i dati e li instradano verso la loro destinazione, sono quindi posti in corrispondenza dei terminali e degli apparati che svolgono la funzione di **commutazione** . Possiamo suddividere quindi i nodi in *nodi di accesso* quando si tratta di terminali e ad essi sono connessi degli utilizzatori o dei fornitori di servizi, e *nodi di transito* quando ad essi non sono connessi gli utenti ma solo altri nodi di transito o nodi di accesso.

I rami sono gli elementi che permettono il trasferimento dei dati da un'estremità all'altra, sono posti in corrispondenza degli apparati che svolgono la funzione di multiplazione e con i sistemi trasmissivi di linea.

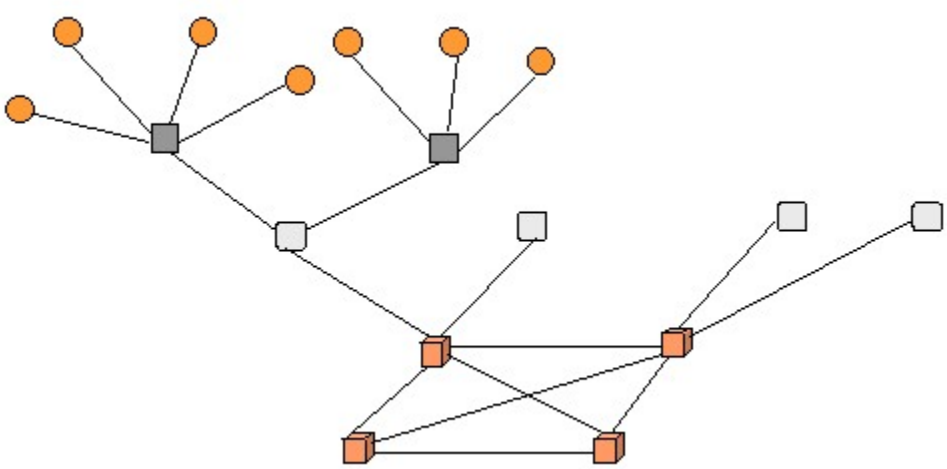


La struttura del grafo è anche **topologia** della rete.

La più semplice topologia possibile è quella a maglia completa, in cui tutti i nodi sono collegati fra loro a due a due. Questa topologia ha l'indiscutibile vantaggio di prevedere un collegamento punto-punto diretto fra qualunque coppia di nodi. Ha però il grande svantaggio di richiedere un numero di linee di collegamento che cresce con il quadrato del numero dei nodi. Per una rete di N nodi sono necessarie N(N-1)/2 linee. È quindi una topologia che poco si addice a reti con molti nodi.

Un'alternativa che invece richiede un minor numero di linee è quella a stella in cui una insieme di nodi di accesso viene collegato ad un **nodo** di transito che svolge la funzione di commutazione. La rete a stella ha il vantaggio di richiedere un minor numero di linee, ma è potenzialmente più vulnerabile ai guasti, in quanto se non funziona correttamente il nodo di transito tutta la rete smette di funzionare.

Ovviamente è anche possibile combinare queste soluzioni creando **reti gerarchiche** con topologie ibride. Un esempio è quello che segue, in cui due livelli di topologia a stella sono utilizzati per collegare i nodi di accesso con un primo livello di nodi di transito. A loro volta questi sono collegati a stella con un secondo livello di nodi di transito e poi con un terzo. I nodi di transito del terzo livello, meno numerosi dei precedenti sono infine collegati con una topologia a maglia completa. Questo si giustifica in quanto questa parte della rete risulta essere il **nocciolo** (*core*) del sistema e deve avere la massima affidabilità possibile.



Tipologie di collegamento

Esistono varie tipologie di collegamenti fra terminali o nodi di una rete:

- **Punto-punto**: due nodi comunicano fra loro agli estremi del collegamento.
- **Punto-multipunto** : un **nodo** può comunicare con tanti altri.
- ***Multicast*** : un nodo trasmette allo stesso tempo ad un sottoinsieme dei nodi della rete.
- ***Broadcast*** : un nodo trasmette allo stesso tempo a tutti i nodi della rete.

Inoltre su di una linea di collegamento fra i terminali A e B il flusso di informazioni può essere di tipo:

- **monodirezionale o *simplex*** : A invia dati a B;
- **monodirezionale alternato o *half duplex*** : A invia informazioni a B, quando A tace B può inviare informazioni ad A e viceversa;
- **bidirezionale o *full duplex*** : A e B possono contemporaneamente inviare informazioni all'altro.

Mezzi di trasmissione

I mezzi fisici utilizzati per la trasmissione dei dati sono di tre tipi:

- mezzi elettrici (cavi); si usa l'energia elettrica per trasferire i segnali sul mezzo;
- mezzi *wireless* (onde radio); in questo caso si sfruttano onde elettromagnetiche;
- mezzi ottici (LED, laser e fibre ottiche); con le fibre ottiche si usa la luce.

I parametri prestazionali di questi mezzi sono:

- **larghezza di banda** ; serve per determinare quanti bit al secondo è possibile trasferire;
- **affidabilità**; ogni mezzo presenta una certa probabilità di errore nella trasmissione;
- **prestazioni**; determinano la distanza massima in un collegamento;
- **caratteristiche fisiche**; a seconda del mezzo si usano fenomeni diversi per la trasmissione, occorre perciò sfruttare tecnologie differenti.

I mezzi elettrici più usati sono fondamentalmente il **cavo coassiale** e il **doppino** . Il doppino è il mezzo più vecchio e comune dei due. Consiste di due fili intrecciati ad elica tra loro, e può essere sia schermato (**STP** - *Shielded Twisted Pair*) che non schermato (**UTP** - *Unshielded Twisted Pair*). Il doppino viene utilizzato all'inizio per le connessioni terminali nella telefonia, cioé per quel tratto che va dall'apparecchio alla centrale. Una versione del STP con più avvolgimenti e un migliore isolamento viene usato per il traffico dati su lunghe distanze. Il cavo coassiale è composto da un conduttore centrale ricoperto di isolante, all'esterno del quale vi è una calza metallica. Il coassiale era usato per lunghe tratte telefoniche ma è stato sostituito dalla fibra ottica, ora rimane in uso per la televisione via cavo e per l'uso in reti locali.

Le fibre ottiche sono costituite da un sottilissimo cilindro centrale in vetro (*core*), circondato da uno strato di vetro esterno (*cladding*), con un diverso indice di rifrazione e da una guaina protettiva. Le fibre ottiche sfruttano il principio della deviazione che un raggio di luce subisce quando attraversa il confine fra due materiali diversi (*core* e *cladding* nel caso delle fibre). La deviazione dipende dagli indici di rifrazione dei due materiali. Oltre un certo angolo, il raggio rimane intrappolato all'interno del materiale. Le fibre ottiche hanno delle prestazioni eccellenti, possono raggiungere velocità di trasmissioni pari a 50.000 Gb/s, ossia 50 terabit al secondo con un bassissimo tasso d'errore. Le distanze massime per un collegamento di questo tipo sono di circa 30 kilometri, per collegamenti di lunghezza maggiore si introducono ripetitori e amplificatori lungo la tratta.

La trasmissione senza fili si effettua su diverse lunghezze d'onda, e sono le onde radio, microonde, raggi infrarossi, luce visibile e ultravioletti. Il comportamento di questo mezzo dipende dalla lunghezza d'onda e dalla banda utilizzata, le prestazioni possono variare ampiamente.

Classificazione delle reti in base alla distanza

La storia delle reti di telecomunicazioni ha visto nascere diverse soluzioni a problemi di tipo eterogeneo, che vanno dalla necessità di comunicare a grande distanza tramite il telegrafo o il telefono, fino alla possibilità di interconnettere tra loro *computer* residenti nella stessa stanza o edificio.

Questa diversità di problematiche ha comportato tradizionalmente una classificazione delle reti sulla base della distanza coperta dalle reti stesse:

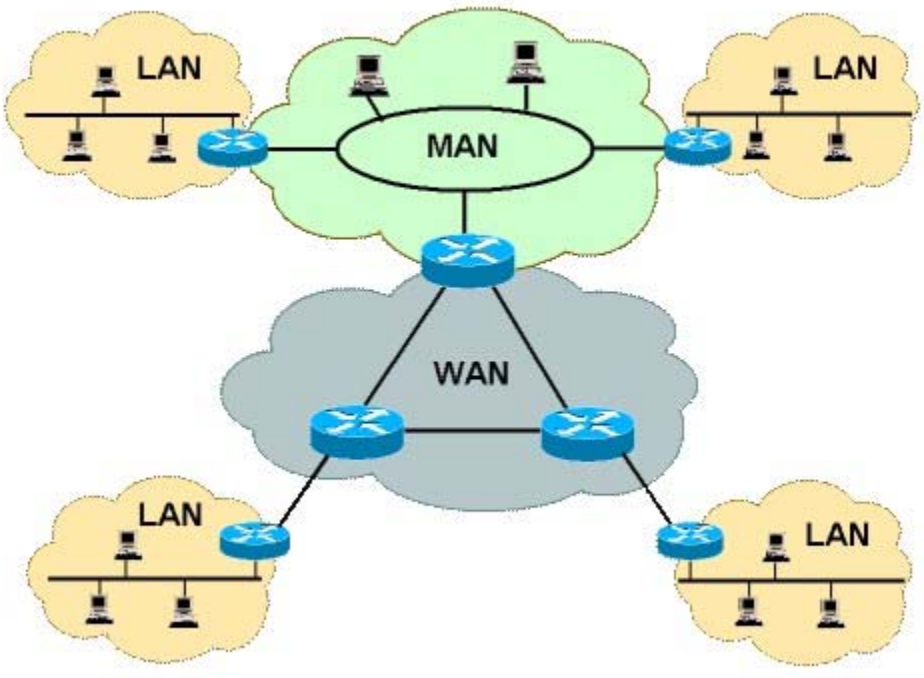
- **LAN** - *Local Area Network* o **reti locali**: tipicamente sono reti private per l'interconnessione di *computer* ed altri apparati appartenenti ad un unico ente o azienda;
- **MAN** - *Metropolitan Area Network* o **reti metropolitane**: possono essere reti private o pubbliche e fornire servizi di vario tipo in ambito urbano, dall'interconnessione di *computer*, alla telefonia, alla TV via cavo;
- **WAN** - *Wide Area Network* o **reti geografiche**: in passato erano le reti dei grandi gestori tipicamente pubblici che fornivano servizi e connettività a livello nazionale; oggi, dopo la *deregulation*, possono anche

appartenere a privati ed offrire connettività a livello mondiale.

La differenza tra questi tre tipi di reti in termini di distanza coperta è rappresentata nella tabella seguente:

Area coperta	Distanza	Tipo di rete
Stanza	10 metri	LAN
Edificio	100 metri	LAN
Campus	1 kilometro	LAN
Città	10 kilometri	MAN
Area metropolitana	100 kilometri	MAN
Stato o Nazione	1.000 kilometri	WAN
Continente	5.000 kilometri	WAN
Pianeta	10.000 kilometri	WAN

Un esempio di come reti eterogenee possono essere interconnesse è mostrato nella figura seguente:



Modelli correnti e standard

Franco Callegati,
Walter Cerroni

Gli standard e le reti di comunicazione

Per lo sviluppo delle telecomunicazioni risultano fondamentali gli standard, che definiscono delle serie di regole secondo cui i sistemi e le reti di telecomunicazioni devono operare. Grazie agli standard è possibile che reti di amministrazioni o paesi diversi possano interconnettersi (si pensi alla rete telefonica con la teleselezione internazionale), che i terminali di utente continuino a funzionare anche in reti diverse (si pensi alla radio, alla televisione, al telefono cellulare) e così via.

La problematica della definizione e negoziazione degli standard ha quindi accompagnato da sempre il mondo delle reti di telecomunicazioni.

L'ente internazionale che istituzionalmente si occupa dell'emanazione di questi standard è l'***International Telecommunication Union (ITU)***, nato nel 1865 e rimasto sempre operativo da allora.

L'ITU (http://www.itu.int) emana delle **Raccomandazioni** che sono standard per la realizzazione di sistemi e reti di telecomunicazioni.

Nonostante sia certamente un soggetto importante nello scenario della standardizzazione delle telecomunicazioni l'ITU non è l'unico ente che emana o ha emanato standard. Altri enti pubblici e privati si sono occupati di queste problematiche e sono stati, a vario titolo promotori di standard:

- **ISO** - **http://www.iso.org**;
- **ETSI** : - **http://www.etsi.org**;
- **IEEE** - **http://www.ieee.org**;
- **EIA** - **http://www.eia.org**;
- **IETF** - **http://www.ietf.org**;

Reti di calcolatori

Storicamente le prime reti di calcolatori vengono sviluppate negli anni '70. L'esperimento pilota, finanziato dall'agenzia statunitense *DARPA*, prende il nome di *ARPAnet* e nasce ufficialmente nel 1969.
A questa esperienza seguono, nel corso degli anni '70, numerose implementazioni di reti di calcolatori, molte delle quali di tipo proprietario, cioè sviluppate da un solo costruttore ed incompatibili con sistemi di altri costruttori. Alcune tra le più note furono **DECnet** della *Digital*, SNA di IBM e XNS della *Xerox*.
La caratteristica fondamentale di queste reti è quella di essere sistemi chiusi, ossia sostanzialmente incapaci di comunicare fra loro. Una volta che un utente decide di adottare una di queste reti è legato al relativo produttore, che è l'unico fornitore di apparati compatibili con la rete installata. Questo fenomeno detto di *captivity*, limita molto le scelte dell'utente, che è costretto a seguire l'evoluzione e le scelte tecnologiche del tipo di rete che ha scelto.

Al contrario sarebbe auspicabile che queste reti fossero sistemi aperti, ossia tali che qualunque calcolatore fosse in grado di comunicare con qualunque altro indipendentemente dalla sua architettura e dal suo costruttore. Un sistema aperto ha infatti alcuni importanti vantaggi:

- favorire la diffusione delle reti di calcolatori tramite l'interconnessione delle reti esistenti;
- rendere possibile agli utenti e ai costruttori di reti approvvigionarsi da qualunque produttore, favorendo la concorrenza.

Modello di comunicazione a strati

Per realizzare reti di calcolatori che siano sistemi aperti è necessario:

- delineare un modello di riferimento per la comunicazione fra calcolatori che sia base comune di questi sistemi;
- giungere alla definizione di standard universalmente accettati che specifichino in modo preciso le funzioni che sono necessarie per realizzare la comunicazione.

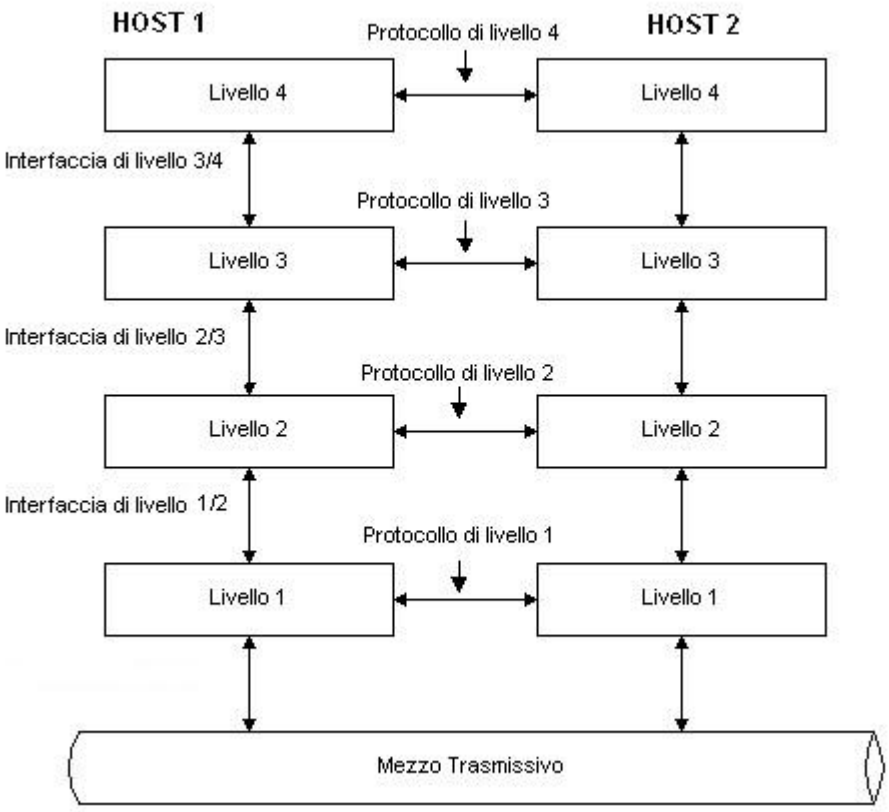
La comunicazione fra calcolatori di tipo diverso è in generale un problema abbastanza complesso. Per semplificare la progettazione dal punto di vista tecnico di una rete di calcolatori risulta quindi conveniente suddividere il problema complessivo in una serie di sottoproblemi ben confinati, chiarendo poi come essi debbano interagire.

Questo tipo di approccio è stato sostanzialmente comune a tutte le implementazioni di reti di calcolatori, anche quando queste si presentavano come sistemi chiusi.

I vantaggi che si hanno nell'operare un approccio a strati sono:

- riduzione della complessità nella costruzione di architetture protocollari introducendo livelli di astrazione;
- indipendenza per l'operatività e le strutture interne di ogni strato; ogni strato deve compiere un compito diverso dagli altri e la sua struttura non è vincolata da quella degli altri livelli;
- interazione tramite servizi; i livelli sono disposti a pila, uno sopra l'altro. Ogni livello fornisce servizi al livello superiore e usufruisce di servizi dal livello sottostante, comunicando tramite la loro interfaccia;
- facilità di attuare cambiamenti su uno strato senza alterare i restanti; gli strati interagiscono tra loro tramite servizi, essendo quindi indipendenti tra loro possono essere modificati nel tempo con nuove tecnologie senza che questo richieda interventi negli altri strati;
- possibilità di utilizzare differenti protocolli per compiti specifici con complessità più trattabile; potendo scegliere le modalità di funzionamento e il livello su cui operare le funzioni di **commutazione** e di multiplazione, si possono ottimizzare alcuni aspetti del modo di trasferimento.

Due livelli di pari grado posti su due calcolatori differenti comunicano tra loro tramite **protocollo** , mentre due livelli adiacenti della stessa macchina comunicano tra loro tramite **interfaccia**. L'obiettivo di un livello è quello di servire servizi al livello superiore nascondendo a questo il modo in cui i servizi sono realizzati.



Modello ISO-OSI

Nei primi anni '80 l' **ISO** promuove un'azione volta alla definizione di un modello di riferimento a strati e di una serie di standard per protocolli e interfacce atti a realizzare dei sistemi aperti. Questo lavoro prende il nome di ***Open System Interconnection*** o **OSI** .

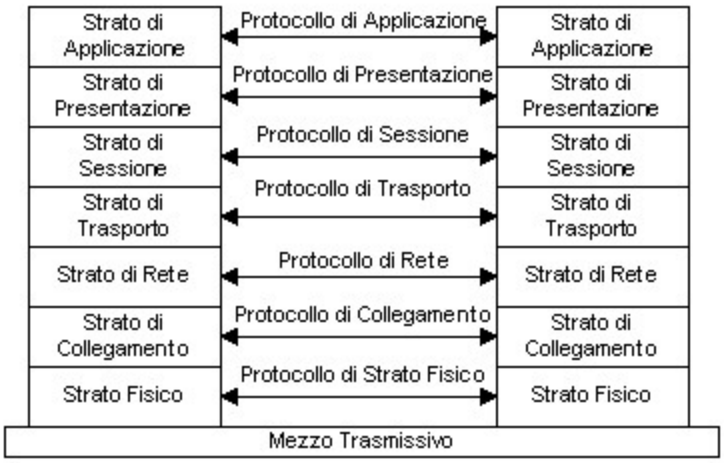
L' **ISO-OSI (*Open System Interconnection*) *Reference Model*** ha lo scopo di:

- fornire uno standard per la connessione di sistemi aperti;
- fornire una base comune per lo sviluppo di nuovi standard per l'interconnessione di sistemi;
- fornire un modello rispetto a cui confrontare le architetture di rete.

Il modello OSI non definisce di per sé dei protocolli specifici di comunicazione, non può essere considerato quindi come un'architettura di rete. Il numero di livelli che compongono il modello strutturale è stato scelto in modo da associare una specifica funzionalità per livello, senza presentare funzionalità ridondanti su più livelli.

OSI è costituito da 7 livelli:

- **strato fisico** ; ha come compito principale effettuare il trasferimento fisico delle cifre binarie tra i due sistemi in comunicazione;
- **strato di collegamento (*data link*)** ; la sua funzione fondamentale è quella di rivelare e recuperare gli errori trasmissivi che potrebbero essersi verificati durante il trasferimento fisico;
- **strato di rete (*network*)** ; rende invisibile allo strato superiore il modo in cui sono utilizzate le risorse di rete per la fase di instradamento;
- **strato di trasporto (*transport*)** ; fornisce le risorse per il trasferimento trasparente di informazioni;
- **strato di sessione (*session*)** ; assicura la possibilità di instaurare un colloquio tra due sistemi;
- **strato di presentazione (*presentation*)** ; è interessato alla sintassi e alla semantica delle informazioni da trasferire;
- **strato di applicazione (*application*)** ; ha lo scopo di fornire ai processi residenti nei due sistemi in comunicazione i mezzi per accedere all'ambiente OSI.



Modello Internet

La rete **Internet** si è sviluppata al di fuori dal modello ISO-OSI e presenta una struttura solo parzialmente aderente al modello **OSI** .

L'architettura di rete ***Internet Protocol Suite*** nota anche come architettura TCP/IP, è una architettura composta da 4 strati:

- strato di accesso alla rete (*network access layer*); comprende le funzioni che nel modello OSI sono comprese negli strati fisico, di collegamento e parte di quello di rete, non è specificato nell'architettura, perché prevede di utilizzare quelli delle varie piattaforme *hardware* e conformi agli standard;
- strato *Internet Protocol* (IP); è collocabile nella parte alta dello strato di rete del modello OSI, è di tipo senza connessione e *best effort*, si occupa di instradare e di controllo di congestione;

- strato di trasporto (TCO o **UDP**); corrisponde al livello di trasporto del modello OSI, ed è implementato in due versioni, **TCP** (*Transmission Control Protocol*) che è un **protocollo** con connessione ed affidabile, e UDP (*User Datagram Protocol*) che è senza connessione e non affidabile;
- strato di applicazione (*application protocol*); nell'architettura Internet non sono previsti gli strati di sessione e di presentazione, ma solo quello di applicazione; questo strato contiene i protocolli utilizzati poi dai programmi residenti sulle macchine. I protocolli utilizzati in questo strato sono **FTP** (*File Transfer Protocol* - per il trasferimento dei file), **POP** (*Post Office Protocol*) e **SMTP** (*Simple Mail Transfer Protocol*) per la posta elettronica, **Telnet** per il terminale virtuale, **HTTP** (*HyperText Transfer Protocol* - per le pagine *Web*), **DNS** (*Domain Name Service* - per convertire nomi alfanumerici in indirizzi IP), NNTP (*News Network Transfer Protocol* - trasferimento articoli dei *newsgroup*)

Le reti locali ed lo standard IEEE 802

Una **rete locale** (**LAN**) può essere definita come un'infrastruttura di telecomunicazioni che consente ad apparati *indipendenti* di comunicare in un'*area limitata* attraverso un *canale fisico condiviso* ad *elevata bit-rate* e con *bassi tassi di errore*.

Quindi, se si parla di reti locali, si intendono reti caratterizzate da estensione geografica limitata, dell'ordine di qualche chilometro al massimo, velocità di trasmissione (*bit-rate*) medio-alta, compresa tra 10-1000 Mbps (associata ad una bassa probabilità di errore per bit) e costi relativamente bassi. L'esigenza di contenere i costi porta alla scelta di topologie di rete molto semplici (a ***bus*** o ad anello), e a un utilizzo condiviso delle risorse trasmissive. L'utilizzo condiviso del mezzo trasmissivo è stato preferito ad un utilizzo esclusivo del mezzo anche per un'altra ragione. L'utente di LAN per la maggior parte del tempo non accede al mezzo trasmissivo, ma quando vi accede richiede delle prestazioni elevate. Se il mezzo fosse suddiviso in un numero di parti pari agli utenti che vi partecipano e ciascuna parte assegnata staticamente ed esclusivamente ad ogni utente, la velocità trasmissiva sarebbe notevolmente inferiore. Inoltre, i terminali interconnessi tramite una rete locale sono tipicamente indipendenti e tutti uguali tra loro, nel senso che non ce n'è uno che debba svolgere funzioni diverse dagli altri per il corretto funzionamento della LAN stessa, o che abbia diritto più degli altri all'utilizzo del mezzo condiviso.

A causa delle caratteristiche peculiari delle LAN, che ne fanno uno strumento utilissimo all'interno di uffici, fabbriche e laboratori, diversi produttori di macchine da ufficio in passato hanno proposto numerose soluzioni proprietarie per interconnettere apparati in un'area limitata. La necessità, poi, di regolamentare ed unificare tutte queste soluzioni ha portato allo sviluppo di veri e propri standard internazionali che definiscono in maniera precisa le caratteristiche tecniche di diversi tipi di LAN, derivandole comunque dai migliori e più diffusi prodotti commerciali.

In particolare l'organizzazione internazionale denominata **IEEE** (*Institute of Electrical and Electronics Engineers*) ha

sviluppato una serie di standard per le LAN attraverso il progetto **IEEE 802** , che si inquadra nei primi due strati del modello ISO-OSI: esso standardizza quindi strato fisico e strato di collegamento di diversi tipi di LAN. Proprio a causa del numero di problematiche eterogenee affrontate dallo standard IEEE 802, esso è stato suddiviso in diversi documenti (emanati dai relativi gruppi di lavoro in cui è suddiviso il comitato IEEE 802), i più importanti dei quali sono:

- **802.1** - introduce l'insieme degli standard e definisce l'architettura del modello 802;
- **802.2** - standardizza il livello più alto chiamato ***Logical Link Control*** ;
- **802.3** - standardizza il protocollo **CSMA/CD** , noto anche come ***Ethernet*** ;
- **802.4** - standardizza il protocollo *Token Bus*;
- **802.5** - standardizza il protocollo ***Token Ring*** ;
- **802.11** - standardizza un protocollo per reti locali via radio (*wireless LAN*).

IEEE 802.1 - Architettura

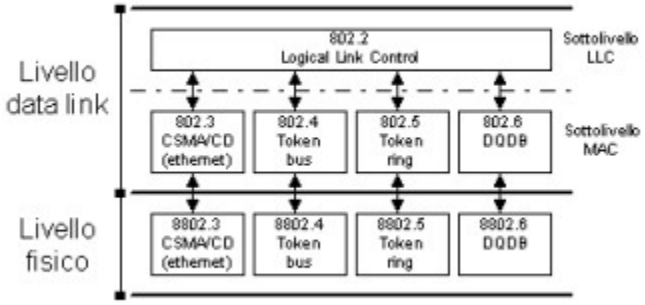
L'architettura degli standard **IEEE 802** per reti locali è definita nel documento 802.1.

Il modello IEEE 802 si conforma al modello ISO-OSI, inquadrandosi perfettamente nei primi due livelli, fisico e di collegamento. Tuttavia, il modello IEEE 802 suddivide il secondo livello in due sottolivelli:

- **LLC *(Logical Link Control)***, comune a tutti i tipi di **LAN** e avente lo scopo di fornire un'interfaccia unificata con il livello superiore (di rete);
- **MAC *(Media Access Control)***, diverso per ciascun tipo di LAN e strettamente legato al relativo livello fisico;

Inoltre lo strato fisico definisce la tipologia di mezzo trasmissivo da utilizzare, le caratteristiche elettriche e meccaniche dell'interfaccia a tale mezzo e la topologia da utilizzare, cioè come la rete locale deve essere strutturata fisicamente. Le più importanti topologie adottate nelle LAN sono:

- ***BUS*** ;
- STELLA;
- ANELLO;



Il sottolivello MAC

Per ciascun tipo di LAN, mentre il livello fisico specifica il mezzo trasmissivo da usare, la topologia e le modalità di trasmissione e ricezione dei bit di informazione, il sottolivello **MAC** si occupa delle seguenti problematiche:

- assemblamento dei dati provenienti dal sottolivello superiore **LLC** in trame con l' **indirizzo** sorgente, di destinazione ed il campo per il controllo degli errori;
- disassemblamento delle trame ricevute e consegna dei dati al sottolivello LLC;
- riconoscimento dell'indirizzo di destinazione;
- individuazione degli errori: il **canale** trasmissivo viene ritenuto sufficientemente esente da errori, per cui al più viene scartata la **trama** errata;
- regolamentazione dell'accesso al mezzo trasmissivo.

In particolare, il problema dell'accesso al mezzo è critico ed è legato al fatto che le reti locali utilizzano un unico mezzo condiviso tra i calcolatori connessi: reti di questo tipo sono dette **reti *broadcast*** , perché i dati trasmessi sul canale da una macchina vengono ricevuti da tutte le altre. Le stazioni collegate utilizzano il mezzo trasmissivo con tecnica di *multiplazione statistica*, cioè il **nodo** che ha necessità di trasmettere richiede l'accesso al mezzo finché non ne entra in possesso, eseguendo una procedura, definita nel **protocollo** di accesso del MAC, chiamata *Channel Access Procedure* (**CAP**). Il protocollo di accesso non ha un meccanismo di controllo centralizzato, ma è paritetico e distribuito; non esiste quindi un organo di arbitraggio con il compito di ricevere le richieste dalle stazioni e di assegnare la risorsa trasmissiva. La multiplazione non è centralizzata e deterministica, ma tutte le stazioni concorrono alla formazione del flusso informativo multiplato in maniera statistica. I possibili protocolli di accesso sono raggruppabili in due categorie:

- **protocolli ad accesso casuale**, in cui si trasmette senza acquisire il controllo della risorsa canale ed in cui è possibile la **collisione** fra più trasmissioni contemporanee; in tal caso la collisione, che provoca la perdita dell'informazione, va risolta dal protocollo stesso tramite un apposito algoritmo, detto *Collision Resolution Algorithm* (**CRA**);
- **protocolli ad accesso controllato**, secondo i quali prima di trasmettere bisogna acquisire il controllo esclusivo della risorsa canale, in modo da evitare qualsiasi tipo di collisione; la peculiarità di ciascun protocollo ad accesso controllato è la modalità di assegnazione del canale.

L'utilizzo di reti di tipo *broadcast*, inoltre, implica la necessità di avere un sistema di indirizzamento univoco a livello MAC: poiché i dati inviati da una **stazione** vengono ricevuti da tutte le altre, è necessario indicare nella trama MAC a chi sono effettivamente destinati (indirizzo di destinazione) e chi ne è il mittente (indirizzo sorgente).

IEEE 802.2 - Il sottolivello LLC

Il sottolivello **LLC** , i relativi servizi offerti ed il **protocollo** che li implementa sono standardizzati nel documento IEEE 802.2. L'utilizzo di LLC ha due scopi principali:

- servire da ponte tra i vari standard del sottolivello **MAC** e il livello di rete, offrendo un'interfaccia unificata e svincolata dalle differenze tra diversi tipi di LAN;
- fornire, se richiesto dal livello superiore, un servizio più sofisticato di quello offerto dai vari sottolivelli MAC, che offrono solo servizi a **datagramma** non affidabili; i servizi offerti da LLC sono:
  - servizio a datagramma non affidabile; in pratica non aggiunge nulla alla modalità prevista dal MAC;
  - servizio a datagramma confermato; prevede che, al momento della ricezione di una **trama** , il destinatario invii un messaggio che ne confermi la corretta ricezione; il mancato ricevimento, da parte della sorgente, della conferma comporta la **ritrasmissione** della trama non confermata;
  - servizio affidabile orientato alla connessione; prevede l'instaurazione di una connessione, l'invio dei dati e la chiusura della connessione, garantendo così che ogni trama sia consegnata correttamente e nell'ordine giusto.

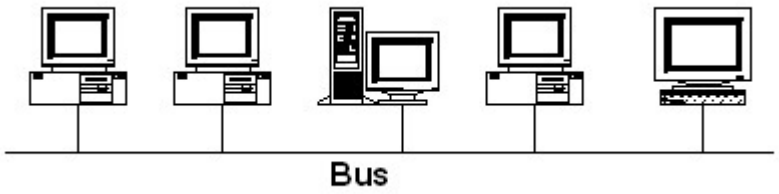
Mentre il sottolivello MAC si limita a rilevare gli errori e a scartare le trame errate, LLC invece espleta la gestione degli errori, richiedendo le eventuali ritrasmissioni delle trame errate. Il protocollo adottato per LLC è una versione semplificata di **HDLC** , in quanto non deve gestire problematiche come il ***bit stuffing*** e la delimitazione delle trame, visto che si appoggia sul sottolivello MAC.

Topologie LAN

Franco Callegati,
Walter Cerroni

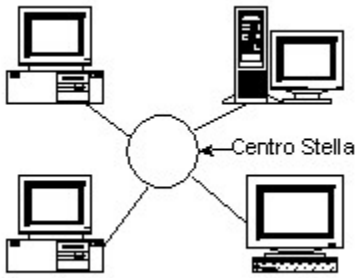
Topologia a bus

Richiede un mezzo trasmissivo bidirezionale, che ammetta cioè la propagazione del segnale in entrambe le direzioni. La trasmissione è di tipo ***broadcast*** , quindi quando una macchina trasmette, tutte le altre ricevono il segnale. I sistemi collegati al ***bus*** non si devono preoccupare di ripetere il segnale o di effettuare instradamento, in quanto tutti i calcolatori sono direttamente raggiungibili. La contropartita è che, essendo il mezzo trasmissivo fisicamente condiviso da tutte le stazioni, esso risulta soggetto a collisioni quando più macchine vogliono trasmettere contemporaneamente. I *bus* vengono realizzati tipicamente con **cavo coassiale** a 10 Mb/s.



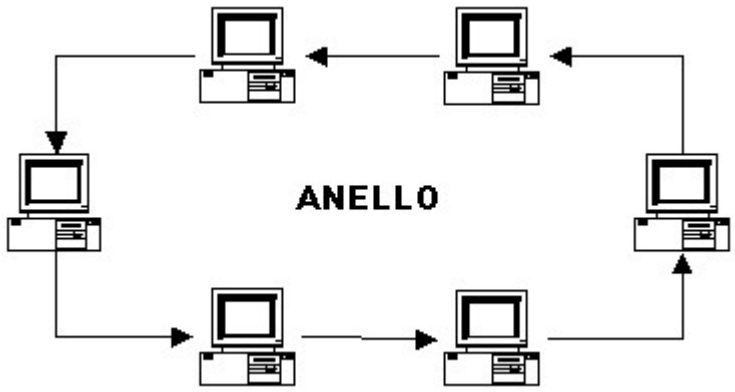
Topologia a stella

La stella si realizza collegando ogni macchina al *centro stella* attraverso un collegamento punto-punto, utilizzando tipicamente **doppino** ritorto o fibra ottica, a seconda della distanza da coprire. Il centro stella può operare in modo attivo realizzando una vera funzione di **commutazione** , oppure in modo passivo limitandosi a ripetere il segnale che riceve su tutte le altre interfacce di comunicazione. La soluzione a stella passiva assicura di per sé una trasmissione di tipo ***broadcast*** . D'altra parte la soluzione a stella attiva, permettendo il collegamento commutato fra stazioni, migliora l'efficienza del sistema.



Topologia ad anello

Prevede il collegamento fisico di ogni macchina alla macchina successiva, e l'ultima macchina viene collegata alla prima. Ne risulta un anello unidirezionale in cui ogni macchina ha anche la funzionalità di ripetizione dei messaggi delle altre. 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. Questa conferma è caratteristica solo della topologia ad anello.

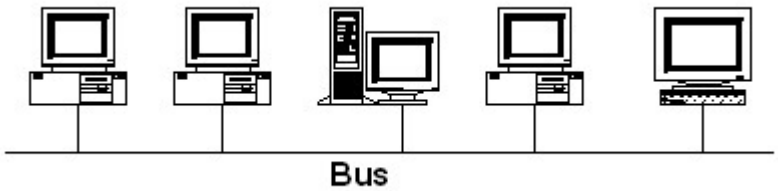


Protocolli e standard di LAN

Franco Callegati,
Walter Cerroni

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

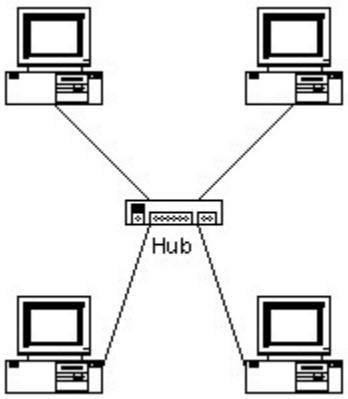
LAN, che permette alle stazioni di condividere l'utilizzo del mezzo trasmissivo. Il protocollo, essendo di tipo ad accesso casuale al mezzo, non esclude il verificarsi di collisioni; prevede quindi un meccanismo di riconoscimento delle collisioni da parte delle stazioni coinvolte, in modo che esse possano 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.

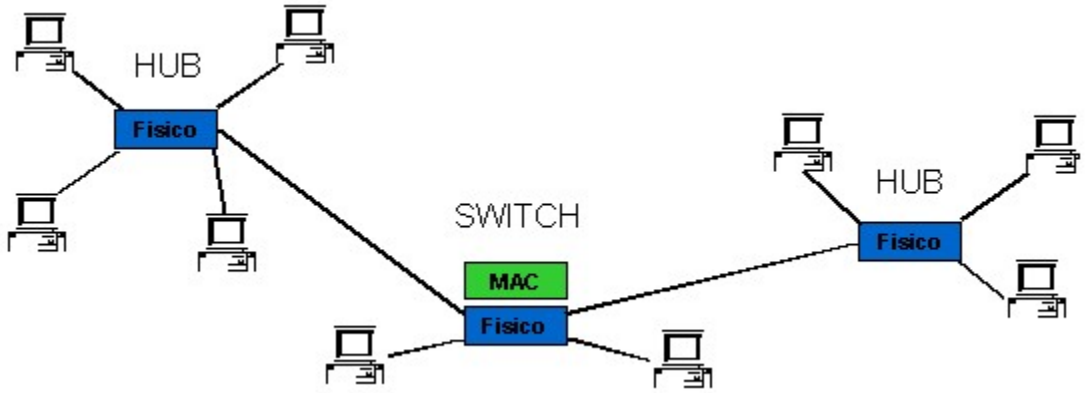


Fattori come la coesistenza di tecnologie diverse, le prestazione limitate in caso di molti utenti e/o di elevato traffico, la ridotta estensione geografica specialmente nel caso di **LAN** ad alte velocità, hanno comportato la scelta di suddividere una LAN in più parti e interconnetterla con i dispositivi 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.

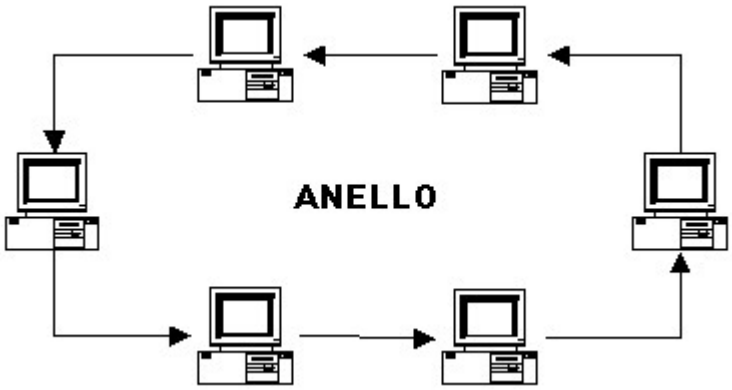
Domini di collisione

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.

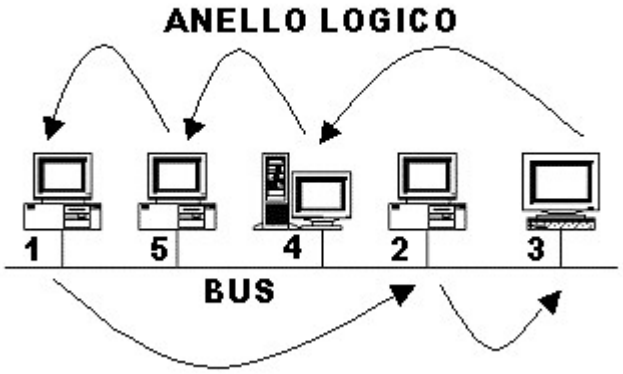
Il protocollo *Token Ring* è del tipo ad accesso controllato, in cui il trasmettitore deve acquisire il controllo del **canale** prima di poter inviare il messaggio. Il controllo del canale viene realizzato attraverso il possesso di un ***token*** (gettone), che è un particolare **pacchetto** che ciascuna **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.

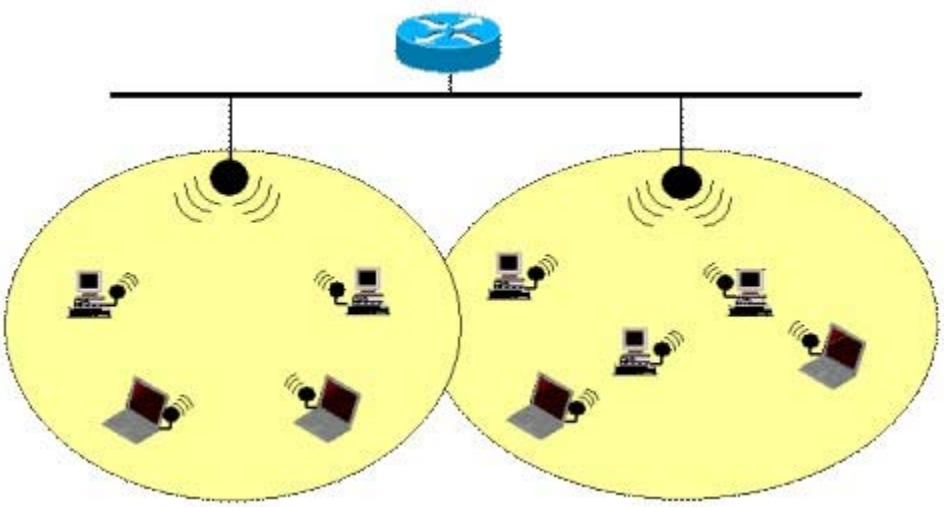


Il funzionamento del protocollo di accesso è simile a quello del ***Token Ring*** : un ***token*** , che rappresenta il completo possesso del **canale** e quindi la possibilità di trasmettere senza collisioni, viene trasmesso da una stazione alla successiva rispettando l'ordine dell'anello logico. Anche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

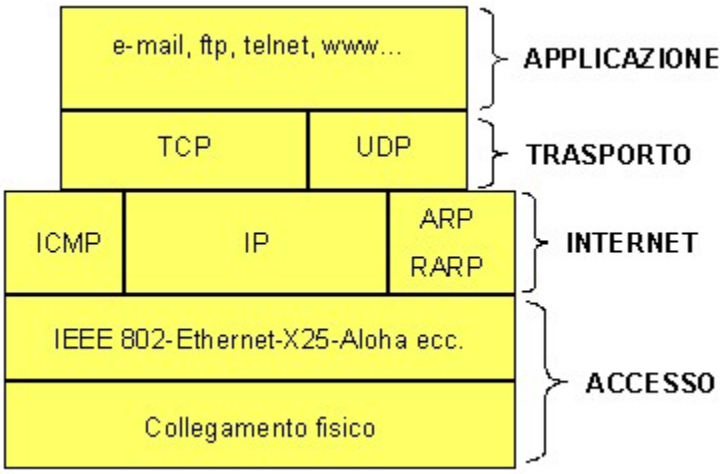
Per la definizione delle problematiche di accesso al mezzo il MAC 802.11 propone due soluzioni possibili:

- 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.

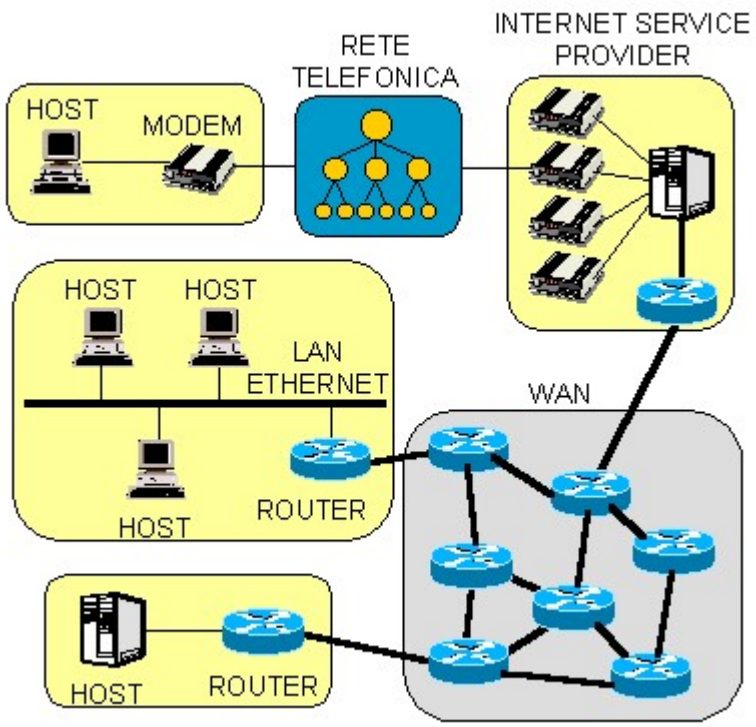
La versione distribuita dimostra particolare efficienza nella gestione di stazioni che colloquiano direttamente oppure in presenza di traffico con caratteristiche impulsive. Un protocollo di tipo centralizzato, invece, si applica tipicamente quando le stazioni *wireless* comunicano fra loro tramite una 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.

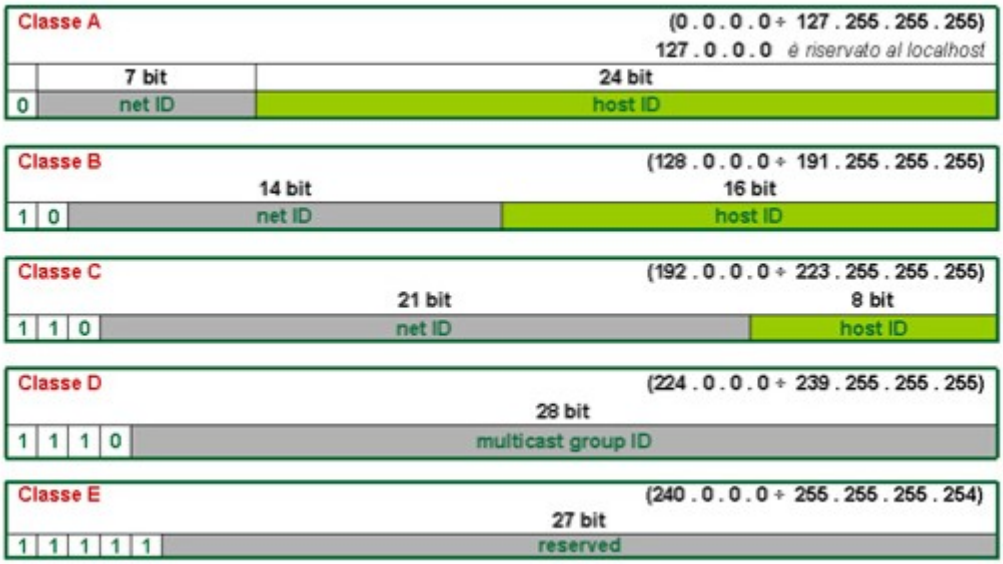
Non sono i nodi ad avere un indirizzo IP, bensì le interfacce. Quindi se un **nodo** ha tre interfacce (ad esempio un ***router***), esso ha tre indirizzi IP. Gli indirizzi IP sono univoci a livello mondiale e sono assegnati da un'unica autorità (in realtà l'autorità assegna al gestore di una rete un 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*.

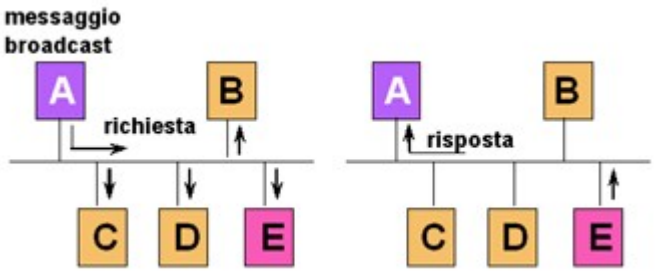


Corrispondenza tra indirizzi IP e indirizzi MAC

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.

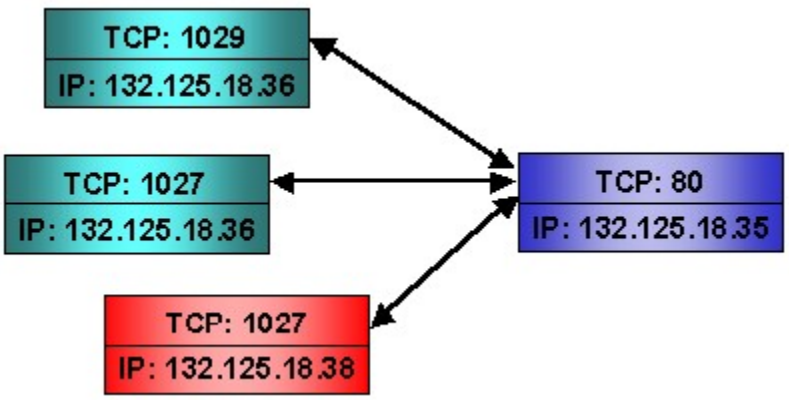
Poiché TCP è un protocollo che opera in modalità orientata alla connessione, ogni trasmissione di dati deve essere preceduta da una fase di attivazione della connessione e seguita da una fase di rilascio.

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

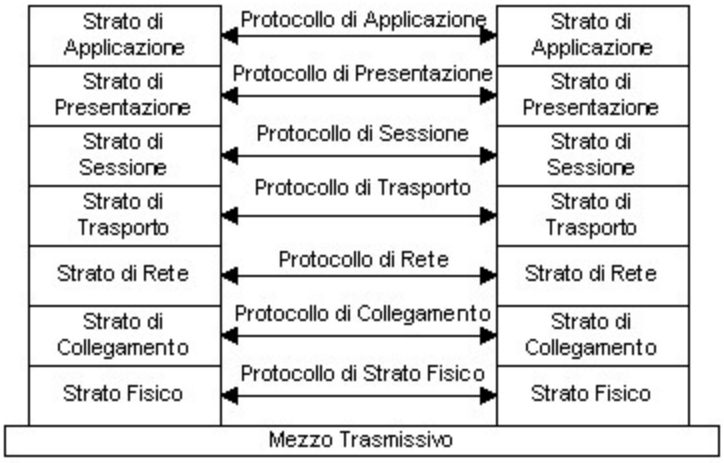
Approfondimenti

Modello di riferimento ISO-OSI

Prof. Franco Callegati
5.2.1 (Elencare e definire gli strati dei protocolli di rete TCP/IP e OSI)

L'architettura

Come già visto nell'introduzione, il **modello ISO-OSI** (***Open System Interconnection***) prevede una architettura a strati. Nel modello di riferimento OSI gli strati sono 7, organizzati come mostrato nella figura seguente.

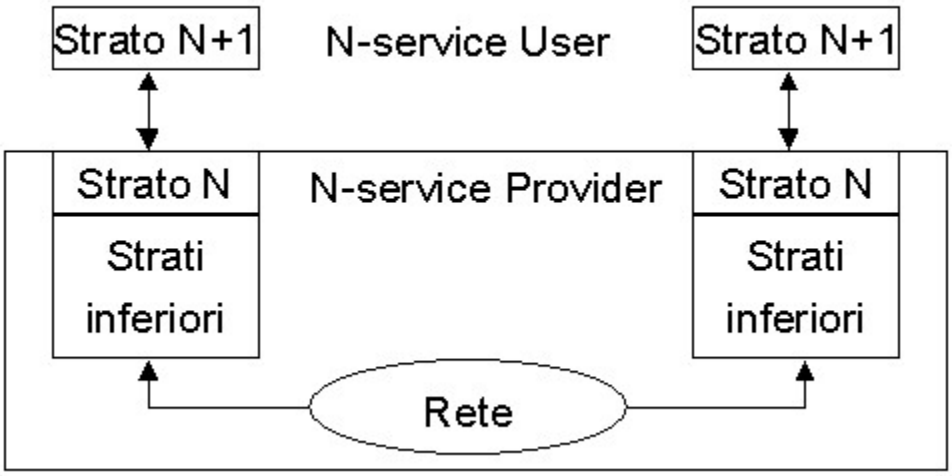


Secondo il modello di riferimento OSI il risultato dell'interazione verticale fra i livelli è un **servizio** (***service***). Un servizio viene definito sulla base delle relative interazioni e dei parametri scambiati.

Secondo la terminologia OSI si dice:

- *N-service provider*
  - Il fornitore di servizio a livello N comprende il livello N e tutti i livelli inferiori di cui il livello N fa uso.
- *N-service user*
  - L'utilizzatore di servizio di livello N è l' **entità** di livello N+1 che fa uso dei servizi del livello N.

Come già detto, il generico strato N, nel fornire il servizio al relativo strato N+1 maschera a questo l'esistenza degli strati inferiori.



Un servizio può essere di tipo ***Connection Oriented*** o ***Connectionless***.

Una modalità di fornire un servizio si dice *Connection Oriented* quando si stabilisce una connessione:

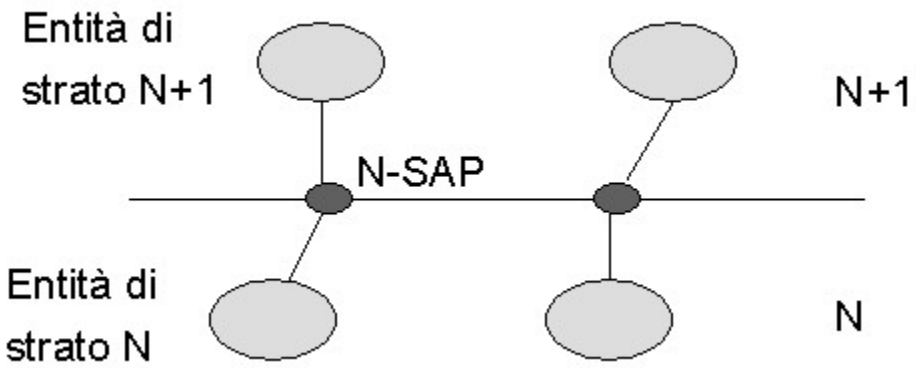
- la connessione associa due o più sistemi al fine di trasferire dati;
- il processo di comunicazione si compone normalmente di tre fasi;

- instaurazione della connessione, tramite lo scambio di opportune informazioni iniziali;
- trasferimento dei dati veri e propri;
- chiusura della connessione.

Qualora i dati vengano trasferiti senza prima stabilire una connessione si parla si servizio *Connectionless*.

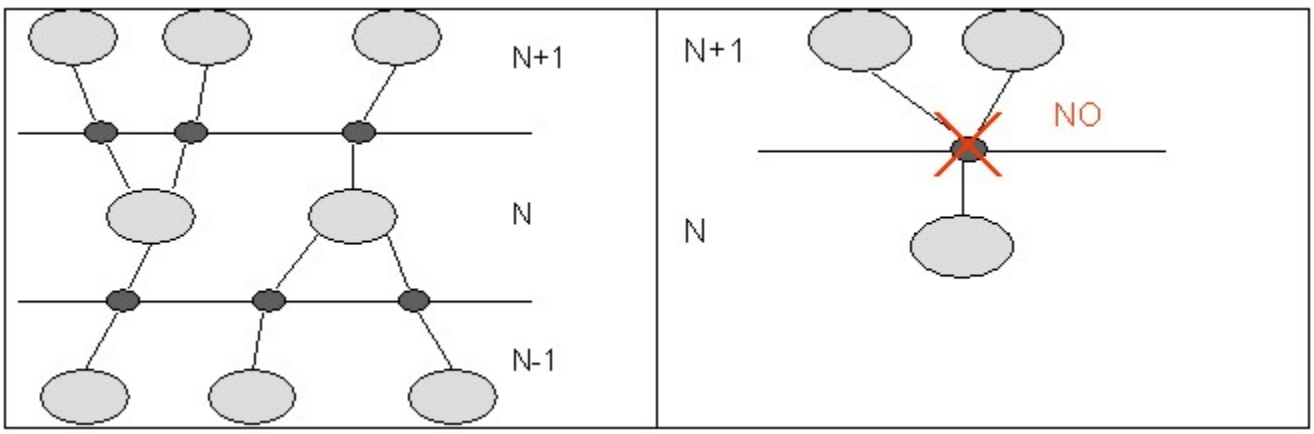
- Per ogni accesso al servizio vengono fornite tutte le informazioni necessarie per il trasferimento dei dati.
- Ogni unità di dati viene trasferita in modo indipendente dalle altre.

Ogni elemento attivo in uno strato viene detto entità. Ciascuno strato comprende una o più entità.



Il ***Service Access Point*** (**SAP**) è l'interfaccia logica fra un'entità di livello N+1 e una di livello N, attraverso la quale viene fornito un servizio:

- ogni N-SAP ha un **indirizzo** (*address*) unico.
- Un'entità di livello N può servire più N-SAP contemporaneamente.
- Un utilizzatore di livello N può servirsi di più N-SAP contemporaneamente.
- Non è permesso connettere più N-*user* allo stesso N-SAP:
    - si genererebbe ambiguità sulla provenienza/destinazione dei dati.

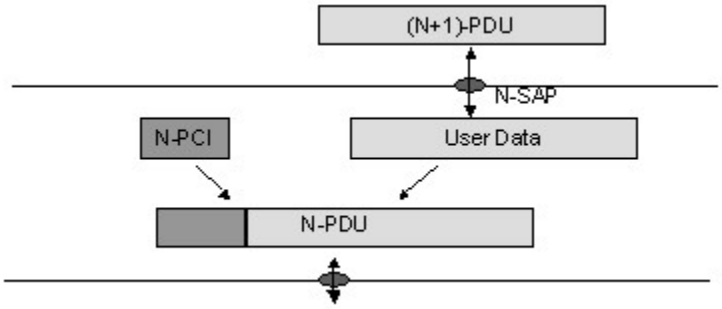


Ciascuno strato deve gestire i dati che gli provengono dallo strato superiore e aggiungere a questo quelle informazioni che servano per la realizzazione delle funzioni proprie dello strato in oggetto.

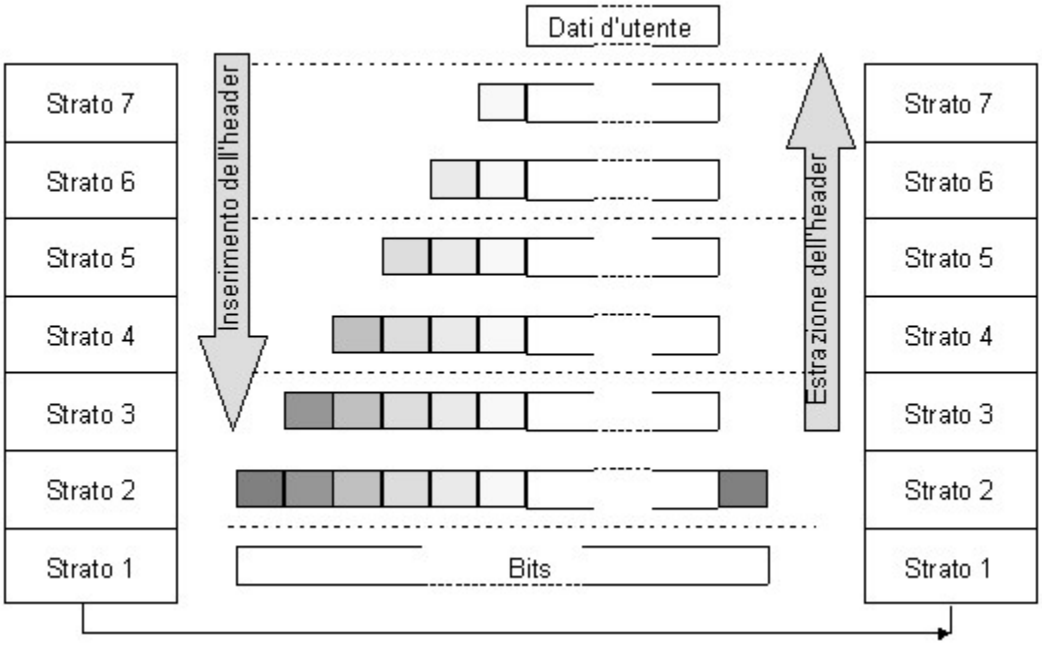
Si possono quindi evidenziare tre tipologie di dati:

- *User Data*:
  - I dati passati al livello N attraverso un N-SAP.
- *Protocol Control Information* (PCI):
  - Informazioni di controllo aggiunte dal livello N.
- ***Protocol Data Unit*** (**PDU**):
  - I dati trasferiti fra entità dello stesso livello.

Come mostrato in figura la PDU altro non è che l'unione di PCI e *User Data*. Le PCI sono anche dette **intestazione** o ***header*** della PDU.



Il trasferimento dei dati fra due applicazioni avviene quindi tramite un progressivo imbustamento di questi con PCI dei vari livelli, fino ad arrivare allo strato fisico che si limita alla trasmissione dei bit.



L'insieme della regole utilizzate dal generico strato N per il trasferimento dei dati, comprendente la specifica del formato e del significato delle PCI utilizzate si dice **protocollo** utilizzato dallo strato N.

Vedremo con maggiore dettaglio le funzioni che il modello di riferimento demanda a ciascuno strato.

Strato 1 - Fisico

Lo strato **fisico** è strutturato per regolamentare tutto ciò che riguarda le caratteristiche dell'interconnessione fisica fra due nodi della rete.

Per fare questo deve specificare le caratteristiche:

- meccaniche:
  - forma di prese e spine, numero di contatti;
- elettriche:
  - voltaggio e caratteristiche elettriche dei segnali associati all'interfaccia;
- funzionali:
  - significato dei vari segnali;
- procedurali:
  - combinazioni e sequenze dei segnali all'interfaccia necessarie al fine di regolarne il funzionamento;

Uno degli esempi più diffusi di standard di strato 1 è l'interfaccia di comunicazione seriale RS-232, emanato dall'EIA. Esistono anche standard per comunicazione parallela quali IEEE 488 e, più recenti standard per la comunicazione veloce fra calcolatori e periferiche quali l'*Universal Serial Bus* (USB).

Inoltre tutti gli standard per reti locali prevedono specifiche per l'interconnessione fisica del calcolatore al mezzo trasmissivo.

Nel caso in cui il calcolatore debba essere connesso ad una rete geografica, generalmente di tipo pubblico, solitamente ci si rifà ad uno schema di collegamento fisico in cui il calcolatore, denominato anche **DTE** (***Data Terminal Equipment***), utilizza per l'interconnessione alla rete un apparato di interfaccia denominato **DCE** (***Data Communication Equipment***). Lo standard di strato 1 in questo caso si prende carico di specificare solamente le caratteristiche che deve avere il collegamento fra DTE e DCE, mentre non dice nulla relativamente alle modalità di connessione del DCE alla rete. Questo tipo di approccio ha il notevole vantaggio di rendere trasparente al terminale di utente (calcolatore) il tipo di tecnologia e di interfaccia di accesso utilizzata per l'interconnessione alla rete pubblica. Infatti le modalità di connessione alla rete possono essere cambiate, modificando il DCE. Se si mantiene costante l'interfaccia del DCE verso il calcolatore queste modifiche sono del tutto invisibili all'utente del calcolatore stesso.

Un esempio di questo approccio è il collegamento ad **Internet** tramite **modem** . Il calcolatore (DTE) si collega alla rete pubblica tramite un apparato detto modem (DCE) utilizzando una certa interfaccia di strato 1 (RS-232, USB, *wireless* ...). Qualora si decida di modificare il tipo di accesso alla rete pubblica, per esempio passando da un normale accesso di tipo telefonico all'accesso di tipo ADSL, è sufficiente cambiare il modem esistente con uno nuovo avente la medesima interfaccia verso il calcolatore di quello precedente, con il risultato che il collegamento alla rete viene modificato senza modificare il calcolatore.

Strato 2 - Data Link

Il livello ***data link*** è il secondo livello partendo dal basso nella pila di strati. Si occupa delle procedure di colloquio necessarie per un trasferimento di informazioni sufficientemente affidabile ed efficiente attraverso ogni linea di collegamento fra nodi di rete adiacenti e nodi di rete e terminali di utente. Nel caso delle reti locali, questo livello gestisce anche le procedure per l'accesso condiviso al mezzo trasmissivo.

Il livello *data link* fornisce servizi di :

- controllo e recupero di errore/perdita/duplicazione di dati;
- controllo e recupero di sequenza dei dati; i bit del livello fisico sono organizzati in trame (***frame***) cioè vengono raggruppati in pacchetti;

- **controllo di flusso** .

I servizi offerti da questo livello sono :

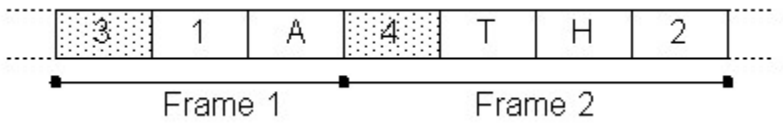
- senza connessione e senza riscontro; vengono inviati dei *frame* indipendenti e non vengono confermati dal destinatario quando questi vengono ricevuti, non viene instaurata una connessione diretta tra i 2 sistemi in comunicazione. Può capitare che alcuni *frame* non vengano ricevuti, e con questa strategia viene ignorato (a livello *data link*) il mancato recupero. è un servizio appropriato per reti con basso tasso di errore, con traffico che richiede una elevata trasparenza temporale (ad esempio per traffico vocale), in particolare viene usato nelle reti locali quando si preferisce la velocità all'integrità dei dati;
- senza connessione e con riscontro; caso analogo al precedente, solo che al momento della ricezione viene inviato dal destinatario un messaggio che conferma la corretta ricezione (***acknowledge - ack***) del *frame*. Il mancato ricevimento dalla sorgente del segnale *ack* comporta la **ritrasmissione** del *frame* non confermato. Questo servizio è utile per reti non affidabili, ad esempio connessioni *wireless*. È possibile che un *frame* non riscontrato sia spedito più volte, inoltre questo meccanismo di riscontro è utile ma non necessario, infatti è possibile implementarlo a livelli superiori;
- con connessione e con riscontro; è il servizio più sofisticato, prevede tre fasi, instaurazione della connessione, invio dei dati e chiusura connessione. In questo modo è possibile garantire che ogni *frame* sia consegnato correttamente e nell'ordine giusto. Viene fornito al livello di rete un flusso di bit affidabile.

Un tipico esempio di funzionamento del livello *data link* è il seguente:

- in trasmissione:
  - segmenta il flusso di bit proveniente dal livello di rete in *frame*;
  - calcola un'apposita funzione, detta ***checksum*** per ogni *frame*, e la inserisce nel *frame* stesso;
  - consegna il *frame* come flusso di bit al livello fisico;
- in ricezione:
  - ricostruisce una serie di *frame* partendo dal flusso di bit fornito dal livello fisico;
  - per ogni *frame* ricalcola il *checksum*, se il *checksum* incapsulato nel *frame* corrisponde con quello appena calcolato, allora il *frame* è considerato esente da errori e viene accettato, altrimenti viene scartato.

Per delimitare i *frame* possono essere usate diverse strategie:

- conteggio dei caratteri; si utilizza un campo all'inizio del *frame* (*header*) per indicare di quanti caratteri è composto il *frame* stesso. Il problema di questo approccio è che se si dovesse rovinare il campo che contiene il conteggio dei caratteri allora il messaggio sarebbe completamente errato in quanto sarebbe impossibile arrivare all'inizio del *frame* successivo.



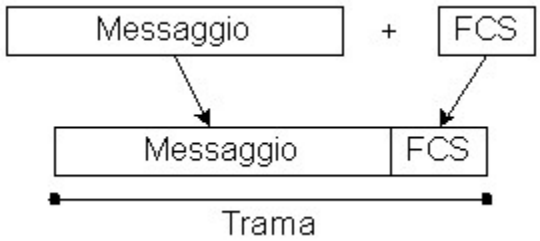
- Caratteri di inizio e fine, con *character stuffing*; viene usato un particolare carattere **ASCII** per delimitare l'inizio del *frame* ed un altro per la fine. In questo modo se la destinazione perde traccia dei confini di un *frame*, la ricezione del carattere di inizio permette il riallineamento. Sorge però un problema, ossia i *byte* che rappresentano i caratteri utilizzati per delimitare i *frame* possono essere contenuti all'interno del messaggio stesso. Per evitare questo inconveniente, quando si presenta un tale *byte* all'interno del *frame*, il livello ne aggiunge un altro subito dopo, in modo che solo i *byte* che rappresentano l'inizio e la fine sono contenuti una volta sola nel flusso, quando se ne presentano due il secondo viene rimosso prima di essere trasferito al livello superiore. Questa tecnica viene detta di *character stuffing*.
- *Bit pattern* di inizio e fine con ***bit stuffing*** ; la tecnica precedente è legata all'utilizzo di codifica ASCII, e può non andare bene per codifiche piu moderne. Per evitare questo problema viene utilizzata una particolare sequenza di bit (*bit pattern*) che indicano l'inizio e la fine del *frame*, ad esempio la sequenza 01111110. Anche

in questo caso può presentarsi questa sequenza all'interno dei bit da trasmettere, perciò se si presentano 5 bit pari a 1 consecutivamente da trasmettere, il livello *data link* inserisce uno 0 successivamente a questa serie di 1. In ricezione se si presentano una serie di 5 1 consecutivi, viene rimosso lo 0 che segue. Pertanto la sequenza 01111110 può apparire solo all'inizio e alla fine dei *frame*. Questa tecnica viene detta *bit stuffing*.
- Violazione della codifica; in molte reti, soprattutto nelle **LAN** , si codificano i bit al livello fisico con ridondanza, ossia gli 1 vengono trasmessi con una coppia alto/basso di tensione, mentre gli 0 con una coppia basso/alto. In questo modo non si incontrano coppie del tipo alto/alto e basso/basso. Queste due coppie possono essere utilizzate per delimitare i *frame*.

L'altro importante compito dello strato di linea è quello di controllare gli errori di trasmissione sui bit, che possono verificarsi con modalità diverse a seconda del mezzo utilizzato. Gli errori sono dovuti in genere a rumori di fondo, disturbi improvvisi e interferenze. Gli approcci al problema sono due:

- possiamo includere una quantità di informazione aggiuntiva in modo da poter ricostruire il messaggio, ossia una strategia di correzione dell'errore;
- includiamo una quantità minore di informazione aggiuntiva solo per permettere il riconoscimento dell'errore in fase di trasmissione, ossia riconoscimento dell'errore.

La parte che viene aggiunta si chiama *Frame Sequence Check* (FCS) e dipende dal tipo di codice utilizzato. I codici di *Hamming* permettono la correzione dell'errore e sono adatti quando il tasso di errori è così alto che si impiega meno tempo a mandare un messaggio più lungo (con più bit di ridondanza) piuttosto che ad aspettare la ritrasmissione. I codici polinomiali o **Codici a Ridondanza Ciclica** (**CRC**) permettono solo il rilevamento dell'errore, ma richiedono meno bit di ridondanza rispetto ai codici di *Hamming*.



Strato 3 - Rete

Il livello di **rete** ha come compito quello di instradare i pacchetti dalla sorgente fino al destinatario, attraversando i nodi intermedi (***router***) che uniscono le varie *subnet*. La differenza tra il livello di rete ed il livello ***data link*** è che il livello *data link* deve solo trasferire i pacchetti da un capo all'altro del ramo, mentre il livello di rete deve effettuare una vera e propria funzione di instradamento.

I compiti di questo livello sono di conoscere la topologia della rete, di scelta di percorso, di gestire il flusso dei dati e le eventuali congestioni, di gestire la presenza di più reti differenti.

I servizi offerti dal livello di rete possono essere sia con connessione che senza:

- con connessione; le **entità** coinvolte nella comunicazione stabiliscono una connessione, negoziando i vari parametri, e a questa connessione viene associato un identificatore. Questo identificatore viene inserito in ogni **pacchetto** inviato dalle due entità, la comunicazione è bidirezionale e i pacchetti viaggiano in sequenza lungo il percorso prestabilito in fase di negoziazione. Con questa strategia il **controllo di flusso** è operato automaticamente grazie ai parametri prestabiliti all'inizio. In questo modo si opera in modo da fornire un servizio di tipo affidabile;
- senza connessione; la sottorete viene considerata inaffidabile, pertanto sono il sorgente e il destinatario del flusso informativo che devono preoccuparsi di gestire sia gli errori che il controllo di flusso, in pratica è il livello di trasporto che si deve occupare di queste cose. Il servizio offerto è di tipo **datagramma** , cioè i pacchetti

viaggiano indipendentemente l'uno dall'altro e devono contenere tutti un **indirizzo** di destinazione.

Per realizzare correttamente la principale funzione del livello di rete, ossia l'instradamento o ***routing*** , sono necessari opportuni algoritmi. L'algoritmo di *routing* deve calcolare su quale uscita di un commutatore instradare il flusso dati in ingresso. Se il servizio è con connessione, questo algoritmo si applica solo in fase di *setup* della connessione, se invece è senza connessione allora si applica su ogni pacchetto.

I requisiti per un algoritmo di *routing* sono:

- semplicità, al fine di non richiedere ai nodi grandi sforzi di elaborazione;
- robustezza, per garantire buone funzionalità anche in presenza di malfunzionamenti della rete;
- stabilità, per non creare inconsistenze che possano rendere inefficace l'intradamento dei dati;
- equità al fine di fornire la stessa qualità di servizio a tutte le connessioni;
- ottimalità nelle scelte di percorso.

Gli algoritmi di *routing* possono essere statici e adattivi. Gli algoritmi statici sono eseguiti solamente all'avvio della rete, e le decisioni prese non vengono più modificate. Rientrano in questa classe gli algoritmi:

- *shortest path routing*; ogni ***router*** viene considerato come un **nodo** , e una connessione punto punto come un ramo. Vengono calcolati i cammini minimi tra ogni coppia di nodi e vengono inviati a ogni *router*. I cammini minimi vengono calcolati in base al numero di nodi che devono essere attraversati, alla lunghezza dei rami, tempo medio di immagazzinamento e rilancio;
- ***flooding*** ; il pacchetto viene rinviato su tutti i rami tranne quello da cui è arrivato. In questo modo però si potrebbe generare un numero infinito di pacchetti, quindi per ridurre il traffico generato si possono utilizzare alcuni stratagemmi. Uno di questi richiede l'inserimento nei pacchetti di un numero massimo di nodi da attraversare, dopodiché se questo numero viene superato allora il pacchetto viene scartato.Un altro richiede la verifica da parte di ogni *router* che quel pacchetto non sia già transitato, altrimenti lo scarta. Questò è l'algoritmo più robusto e affidabile anche se genera una quantità di dati tale da non essere usabile con efficacia;
- *flow-based routing*; questo algoritmo effettua una stima del traffico atteso su ogni ramo, poi calcola il tempo medio di attraversamento, quindi decide su quale ramo instradare.

Nelle reti moderne sono in uso algoritmi dinamici di *routing*, in grado di adattarsi ai cambiamenti della rete stessa. Questi algoritmi funzionano non solo all'avvio della rete, ma rimangono in esecuzione durante il normale funzionamento della rete stessa. Fanno parte degli algoritmi dinamici di *routing*:

- **distance vector** *routing*; ogni *router* mantiene al proprio interno una tabella in cui vengono indicizzati tutti gli altri *router* conosciuti fino a quel momento nella rete. In questa tabella viene memorizzato per ogni altro *router* la distanza e il ramo d'uscita per arrivarci. Il *router* a intervalli di tempo manda degli speciali pacchetti chiamati *echo* a tutti gli altri **nodi adiacenti** e misura il tempo di risposta. Appena completa la tabella la invia ai nodi adiacenti. In questo modo non viene a conoscenza del *router* la topologia totale della rete, ed inoltre la convergenza dell'algoritmo è piuttosto lenta quando si verificano eventi che modificano la topologia della rete;
- **link state** *routing*; ogni *router* controlla lo stato dei collegamenti con i *router* adiacenti, misurando i ritardi di attraversamento, e distribuisce queste informazioni agli altri nodi adiacenti. Considerando tutti i pacchetti arrivati, si costruisce un grafo della rete e si calcola il cammino minimo per ogni nodo della *subnet*. Questo algoritmo è molto usato, ad esempio una sua implementazione in **Internet** è piuttosto affermata, questa corrisponde al nome di **OSPF** - *open shortest path first*.

Quando la grandezza della rete diventa tale da non permettere un efficace utilizzo di questi algoritmi, viene utilizzato il metodo del ***routing*** **gerarchico** . La rete viene suddivisa in regioni, e gli algoritmi si applicano su due livelli, all'inizio si opera all'interno di una regione, successivamente si applica l'algoritmo una seconda volta su tutti i *router* che fanno parte del confine di una regione.

Strato 4 - Trasporto

Scopo dello strato di **trasporto** è fornire un **canale** sicuro *end-to-end*, svincolandoli da tutti i problemi di rete.

Si occupa tipicamente di adattare la dimensione dei frammenti forniti dagli strati superiori (*files*) a quella richiesta dalle reti (**pacchetto**):
funzione di Pacchettizzazione (*fragmenting*)

Può avere molte altre funzioni fra cui:

- **controllo dell'errore** ;
- **controllo di flusso** ;
- gestione di dati prioritari, eccetera...

Non tutti le applicazioni hanno bisogno delle stesse funzioni, per cui si possono definire diverse Classi di servizi di trasporto.

Ad esempio nel modello **Internet** lo strato di trasporto prevede diversi protocolli per la fornitura di diverse tipologie di servizio. I più usati fra questi protocolli sono:

- **TCP** per un trasferimento dati *end-to-end connection oriented* con recupero degli errori e controllo del flusso;
- **UDP** per un trasferimento dati *end-to-end connectionless*;
- RTP per un trasferimento dati *end-to-end* che rispetti il più possibile stretti requisiti di temporizzazione.

Ad esempio un'applicazione di trasferimento *file* tipicamente utilizzerà TCP, mentre l'applicazione di invio di un ***e-mail*** utilizzerà UDP ed un collegamento audio via Internet utilizzerà RTP.

Strato 5 - Sessione

Lo strato di **sessione** suddivide il dialogo fra le applicazioni in unità logiche (dette appunto sessioni), in modo tale che una sessione possa essere individuata, interrotta e ripresa, per fare fronte a vari eventi catastrofici: perdita di dati, caduta della linea, momentaneo *crash* di uno dei due interlocutori...

Permette la chiusura ordinata (*soft*) del dialogo, con la garanzia che tutti i dati trasmessi siano arrivati a destinazione.

Anche gli strati di sessione hanno molte funzionalità e possono essere più o meno completi a seconda delle richieste delle applicazioni.

Strato 6 - Presentazione

Lo strato di **presentazione** adatta il formato dei dati usato dai due interlocutori preservandone il significato.

La descrizione del tipo di dati usati per una applicazione e del loro formato si dice una sintassi. Ogni interlocutore ha una sua Sintassi locale e durante il dialogo bisogna concordare una Sintassi di trasferimento. È stato definito un linguaggio detto *Abstract Sintax Notation* 1 (ASN 1) per descrivere e negoziare le sintassi.

Nell'architettura dei protocolli di **Internet** non sono previsti strati di sessione e presentazione, per cui le relative funzioni sono demandate alle applicazioni. Per questa ragione, ad esempio, dobbiamo preoccuparci di specificare il tipo di codifica quando inviamo un allegato ad un ***e-mail*** , oppure dobbiamo ricominciare da capo una navigazione se per qualche ragione cade il collegamento. Se queste funzioni fossero previste in rete, la rete stessa si

preoccuperebbe di svolgerle, senza renderle visibili all'utente.

Strato 7 - Applicazione

Lo strato di **applicazione** è l'utente della rete di calcolatori.

Rappresenta il programma applicativo (o Applicazione) che per svolgere i suoi compiti ha bisogno di comunicare con altre applicazioni remote.

Sono applicazioni i programmi che utilizziamo normalmente per accedere a servizi di rete, quali il **browser** Internet, il programma di invio e ricezione dell' ***e-mail*** , i programmi di trasferimento *file* e condivisione delle risorse eccetera.

Secondo il modello di riferimento ISO- **OSI** l'applicazione dovrebbe occuparsi solamente dell'interazione con l'utente e della gestione dei dati relativi. Come già detto nel caso di **Internet** all'applicazione sono demandate anche funzioni di gestione della sessione e di presentazione dei dati.

Introduzione alle reti di calcolatori

Massimo Maresca
5.1.1 Illustrare vantaggi e svantaggi degli ambienti di rete e non di rete, 5.1.2 Descrivere ambienti di rete quali peer-to-peer e client/server

Rete di calcolatori 1

Buongiorno, io sono Massimo Maresca, sono un professore di "FONDAMENTI DI INFORMATICA" presso l'università di Padova e insegno anche "RETI DI CALCOLATORI" presso l'università di Genova. Cominciamo subito col primo di questi moduli che riguarda l'introduzione alle reti di calcolatori. Quindi ci riferiamo alle reti di calcolatori, che è qualcosa che oggi è presente nella vita di tutti i giorni. In particolare sappiamo che ci sono reti come internet che pervadono le case, i luoghi di lavoro, le fabbriche, tutti i posti in cui le persone in genere vivono. Sappiamo, inoltre, che all'interno degli stessi luoghi ci sono anche delle reti locali. Molti di noi sono dotati di calcolatori per uso personale interconnessi in rete. Vale quindi la pena, all'inizio, vedere cos'è una rete di calcolatori. Una rete di calcolatori è un sistema che consente a ciascun calcolatore (o nodo) l'invio (o la ricezione) di dati verso (o da) altri

nodi, identificati da appositi indirizzi. Questa è una definizione generale, se ne possono dare tantissime. Però bisogna cercare in qualche maniera di delimitare l'argomento, perché vedremo che effettivamente la definizione di rete è importante.

Rete di calcolatori 2

Qua parliamo essenzialmente di un sistema di interconnessione che consente a diversi calcolatori o nodi di scambiarsi dei dati, ma l'elemento importante è che ci sono degli indirizzi che identificano questi nodi. Gli indirizzi, in qualche maniera, sono quelli che consentono di parlare di una rete, la quale è associabile (o associata) ad un piano di indirizzamento. Perlomeno in questo corso assumiamo questa definizione. Quindi, quando parliamo di rete, e questo è il primo concetto di una cera rilevanza, intendiamo un piano di indirizzamento. Ad esempio quella telefonica è una rete: c'è un ente (un'istituzione) che gestisce il piano degli indirizzi, cioè dei numeri di telefono, per cui il fatto stesso che io abbia un telefono, con un numero che mi è stato rilasciato da qualcuno, mi inserisce automaticamente all'interno della rete telefonica. La stessa cosa può valere, per esempio, per internet: appartengo alla rete internet se ho un indirizzo che mi è stato assegnato da quell'ente che gestisce e assegna gli indirizzi per la rete internet. Altri esempi ancora: appartengo alla rete privata di quell'organizzazione se l'ente che amministra gli indirizzi delle macchine della rete di quell'organizzazione mi ha assegnato un indirizzo.

Argomenti della lezione

Descriviamo brevemente quali sono gli argomenti di questa lezione. Per prima cosa parleremo delle tipologie di reti, locali e geografiche. Parleremo poi della commutazione di circuito e di pacchetto, del routing, quindi delle tecniche di instradamento dei dati e vedremo il concetto di connessione, che è un concetto di base più per la telefonia che per le reti, ma viene utilizzato anche in questo settore. Infine daremo un cenno a quello che viene chiamato "internet working" e che quindi deriva essenzialmente dalla rete internet.

Reti locali 1

Iniziamo con le tipologie di reti. Una prima categoria di reti è costituita dalle cosiddette reti locali o LAN (Local Area Network). Queste vengono descritte tradizionalmente come reti che interconnettono più calcolatori, o nodi, o sistemi,

all'interno dello stesso edificio e che seguono un piano di indirizzi locali. Una rete locale rappresenta una tecnologia: possiamo dire che una rete Ethernet, tecnologia utilizzata nella maggior parte delle reti locali, di fatto non è associata ad un piano di indirizzi gestito da qualcuno. Si hanno diversi nodi interconnessi in rete, senza definire necessariamente alcun piano di indirizzamento, se non gli indirizzi dei nodi interconnessi che però, come vedremo tra poco, non sono indirizzi di rete. Abbiamo quindi un piano di indirizzi locali che si riferisce sostanzialmente alle schede che vengono utilizzate per l'interconnessione alla rete locale.

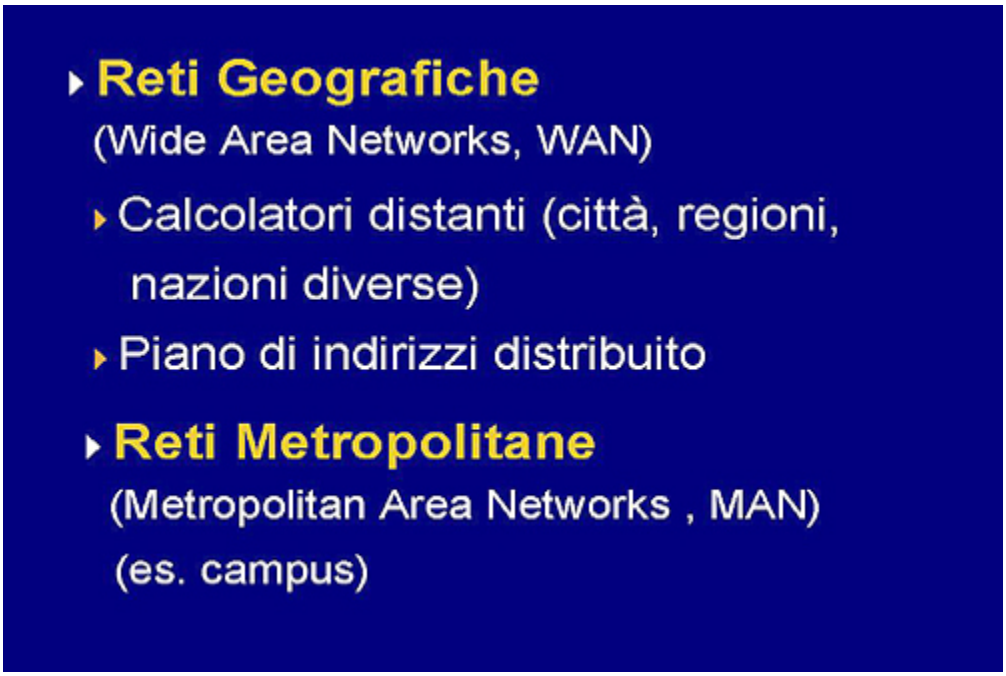
Reti locali 2

Una rete locale potrebbe essere parte di un'altra rete, nel senso in cui l'abbiamo definita. Le reti locali sono nate una ventina di anni fa con la nascita del meccanismo di interconnessione Ethernet, che si basava inizialmente sulla presenza di un cavo coassiale che connetteva tutti i sistemi interconnessi alla rete. Ci sono state poi delle evoluzioni, per esempio la IBM ha sempre spinto un'altra tecnologia per le reti locali chiamata "Token Ring"; di questa naturalmente non parliamo in un corso introduttivo come questo. Successivamente la diffusione del " Token Ring " è andata via via calando, mentre Ethernet è rimasta la rete di riferimento, che si è poi evoluta: oggi abbiamo Fast Ethernet, che è una rete basata sulla tecnologia Ethernet precedente, ma a più alta velocità. Si è passati, infatti, da una velocità di circa 10 Mbit/sec di Ethernet, ad una di 100 Mbit/sec. Si hanno poi altre tecnologie per la realizzazione di reti locali, in particolare basate su ATM, a velocità pari a 155 Mbit/sec o 622 Mbit/sec; abbiamo addirittura il Gigabit Ethernet, che va alla velocità di un Gbit/sec.

Reti geografiche

Vediamo ora l'altra categoria, quella delle reti geografiche, chiamate anche WAN (Wide Area Network). Mentre nel caso delle reti locali abbiamo parlato di calcolatori localizzati nello stesso edificio, o comunque situati in edifici vicini, quindi di reti che coprono più edifici appartenenti alla stessa area, nelle reti WAN invece, i calcolatori sono distanti l'uno dall'altro, quindi collocati in città e continenti diversi senza alcuna limitazione sulla distanza. In questo caso abbiamo un piano di indirizzi distribuiti perché viene tipicamente gestito da un fornitore esterno. Infatti, mentre la rete locale è sotto il dominio di chi la utilizza, la rete geografica è composta da nodi che vengono interconnessi attraverso l'utilizzazione di una infrastruttura di comunicazione gestita da uno o più fornitori di telecomunicazione esterni, come possono essere Telecom Italia, altre Telecom o operatori di questo tipo.

Reti metropolitane



Una terza categoria che viene spesso presentata tradizionalmente, quando si introducono le reti di calcolatori, sono le cosiddette reti metropolitane o MAN (Metropolitan Area Network), dette anche Campus Networks. Quindi, stando a questa classificazione, avremo le LAN, le WAN e le MAN. Nella realtà quest'ultima categoria di reti non viene quasi mai referenziata, di fatto è collassata all'interno delle LAN. Quindi, nel momento in cui deve essere realizzata una rete nell'ambito di uno stabilimento industriale o di un porto, quella viene chiamata tipicamente LAN, oppure rete a livello di Campus (utilizzando comunque le tecnologie delle LAN), perché si tratta di una rete che si trova all'interno di un'area completamente gestita dallo stesso ente. In questa area vengono stesi i cavi, vengono dislocati gli apparati e viene quindi realizzata questa LAN. Viceversa una rete geografica è costruita su distanze più elevate.

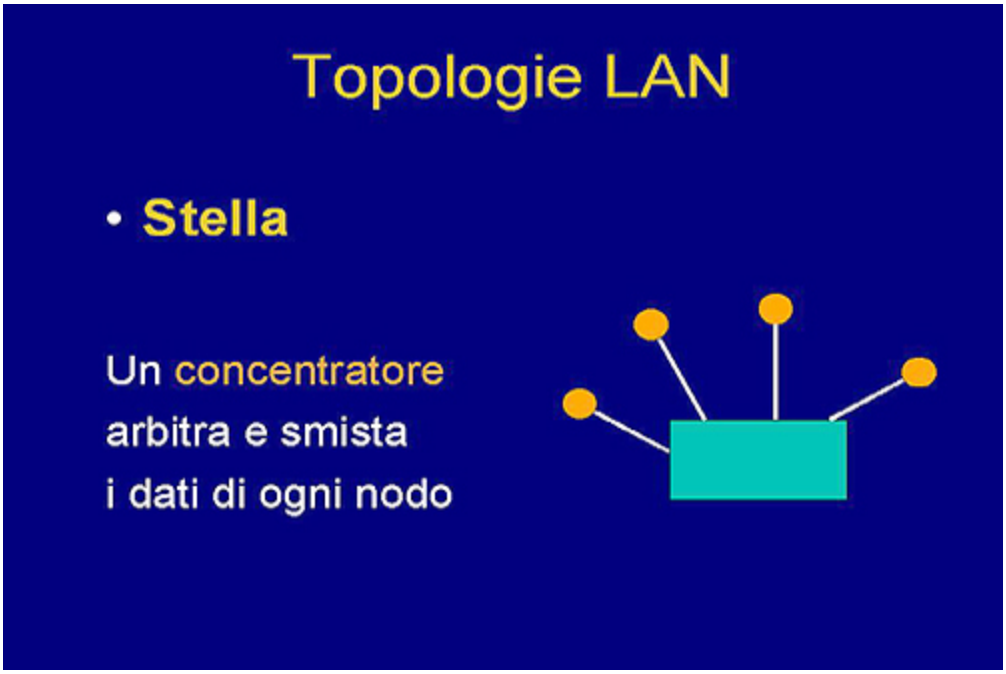
Caratteristiche delle reti locali

Le caratteristiche delle reti locali sono: l'elevata velocità di trasmissione dei dati e i bassi ritardi. Infatti, trasmettendo per esempio alla velocità di 100Mbit/sec si ha bisogno di poco tempo per trasmettere una quantità elevata di dati. Sono realizzate su supporto privato, quindi all'interno di aree gestite dagli utilizzatori. Gli elaboratori degli utenti, però, risultano spesso direttamente interconnessi l'uno all'altro (ci sono tecnologie dove ciò viene evitato) e la dimensione è limitata (l'ordine di grandezza è di qualche chilometro).

Caratteristiche delle reti geografiche

Passiamo ora alle caratteristiche delle reti geografiche: sono tradizionalmente di velocità medio-bassa, infatti fino a qualche tempo fa la velocità tipica di trasmissione delle reti geografiche era 9,6 Kbit/sec. Tuttavia attualmente si hanno dei collegamenti dedicati, a lunga distanza, che arrivano fino a qualche Mbit/sec, valore che rimane comunque molto inferiore alla velocità di trasmissione delle LAN. Se si devono coprire distanze dell'ordine di migliaia di chilometri, avrò dei ritardi che non posso effettivamente diminuire, dovuti all'effettiva velocità di propagazione dei bit sulle linee, che dipende a sua volta dalla velocità della luce. Come abbiamo già accennato, le reti geografiche sono realizzate su supporto pubblico, cioè da un operatore telefonico pubblico (tipicamente una Telecom) il quale costruisce una infrastruttura di elaboratori dedicati che sono dislocati nelle diverse aree dove la rete deve essere presente. A questi operatori pubblici si connettono i nodi, i sistemi che devono essere interconnessi in modo geografico. La distanza coperta da questo tipo di reti può essere molto elevata senza alcun limite effettivo.

Topologie LAN : Stella

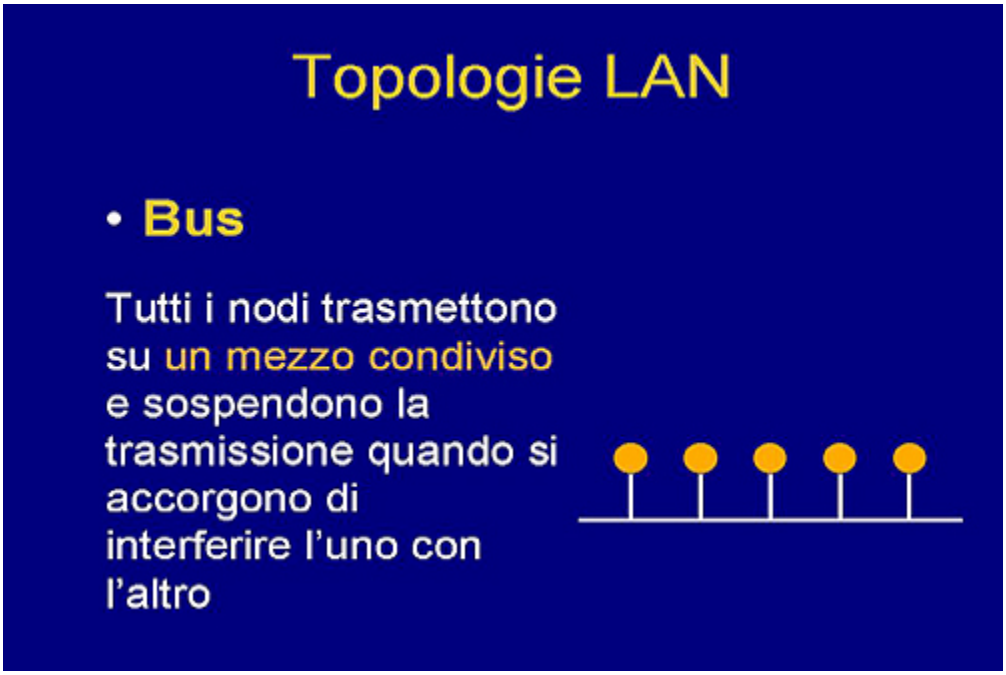


Ritorniamo alle LAN ed entriamo un po' più in dettaglio relativamente alle topologie. Una rete locale viene realizzata su una infrastruttura privata; i cavi della LAN vengono stesi fisicamente da coloro che devono realizzare la rete, per questo motivo ci interessa studiarne le topologie. Ce ne sono essenzialmente di tre tipi, la prima delle quali è la stella: si ha un nodo centrale, di solito chiamato hub, al quale vengono interconnessi tutti i nodi della rete. Il nodo centrale non deve necessariamente essere unico, ad esempio si può avere una rete locale dislocata in tre edifici, in ognuno dei quali è presente una hub, interconnessi tra loro. Abbiamo quindi diversi centri della stella. Se poi al centro dei tre c'è un quarto hub, si ottiene una stella di stelle: tale architettura è ricorsiva, può essere utilizzata in maniera gerarchica.

Topologie LAN : Anello

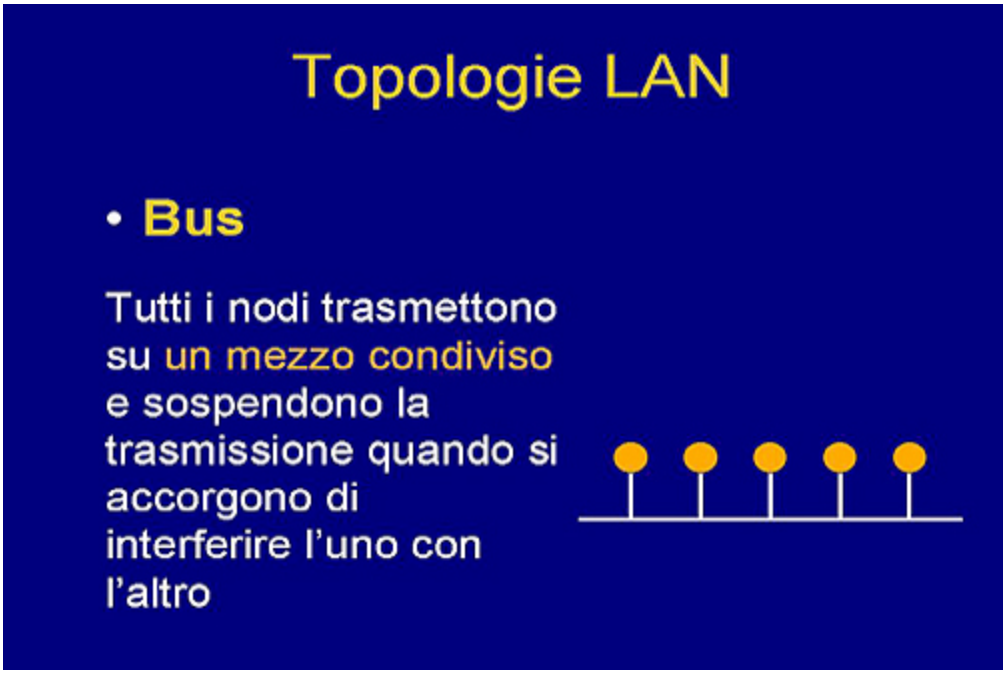
Un secondo tipo di LAN è quella ad anello, dove i nodi sono interconnessi tra di loro formando un anello e in modo tale che ogni nodo parla con il nodo adiacente. Come vedete nell'anello c'è anche una freccia, che indica il senso di rotazione. In una rete di questo tipo si assume di avere un "token", cioè un oggetto che costantemente percorre l'anello in senso orario ed ogni nodo della rete è abilitato ad immettere dati nell'anello soltanto quando questo token passa attraverso di lui.

Topologie LAN : Bus 1



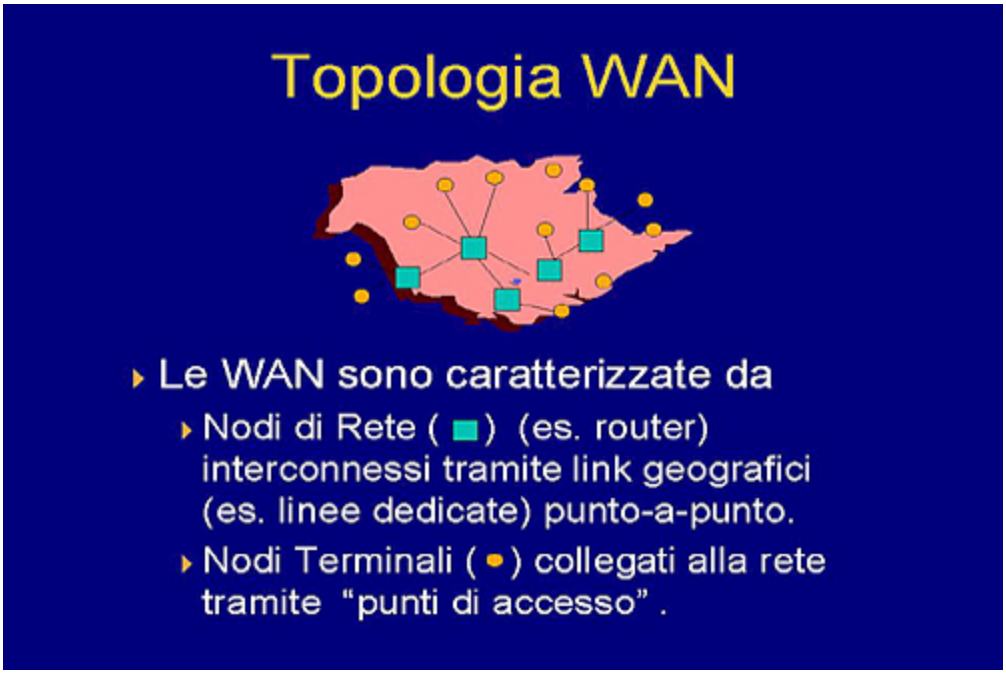
Vediamo ora la terza topologia, quella a bus, dove tutti i nodi trasmettono su un mezzo condiviso e sospendono la trasmissione quando si accorgono di interferire l'uno con l'altro. Questa topologia bus è alla base della rete Ethernet e ha dato luogo al fenomeno delle reti locali. Va sottolineata la presenza di questo mezzo condiviso perché poi lo incontreremo anche in altre reti; si ha un unico bus e tanti nodi che se lo contendono. Nasce quindi il problema dell'arbitraggio: quando più nodi desiderano immettere dei dati sulla rete, ci deve essere un meccanismo in base al quale uno dei nodi riesce, mentre l'altro fallisce. Sulla rete Ethernet è nato tutto il discorso, sviluppato poi negli anni, dell'arbitraggio della risorsa bus condivisa. Riassumendo abbiamo visto tre topologie: stella, anello e bus. Queste possono esser viste come vere e proprie topologie di cablaggio, ad esempio per quanto riguarda la stella, si avrà nella rete locale un centro e da tutti i punti in cui sono previsti dei nodi dovrà partire un cavo che raggiunge il centro-stella.

Topologie LAN : Bus 2



È chiaro che il costo di questi cavi può essere anche elevato. Se, ad esempio, si hanno due nodi tra loro molto vicini, ma lontani dal centro-stella, occorreranno due cavi di lunghezza quasi uguale da ciascuno dei due nodi fino al centro stella. In una topologia a bus, invece, si avrà un unico cavo, al quale tutti i nodi sono connessi, che passa prima attraverso uno dei due nodi e poi attraverso l'altro, risparmiando nel cablaggio. La stessa cosa si può dire della tipologia ad anello, dove può accadere che due nodi molto vicini risultino adiacenti anche dal punto di vista della rotazione dei dati. Quello che è importante sottolineare è che la tecnologia di accesso, quindi l'uso di un bus condiviso, deve essere separata dal cablaggio. Quindi se in una certa situazione può essere conveniente utilizzare un bus condiviso, ciò non implica necessariamente l'utilizzo di un cablaggio a bus. Attualmente il modo in cui vengono realizzate le reti locali prevede cablaggi esclusivamente a stella. Su un cablaggio a stella è possibile poi simulare una topologia a bus oppure ad anello. Per tale ragione oggi si realizzano retti locali esclusivamente a stella e gli standard di riferimento per la realizzazione di cablaggi strutturati prevedono essenzialmente il cablaggio a stella.

Topologie WAN

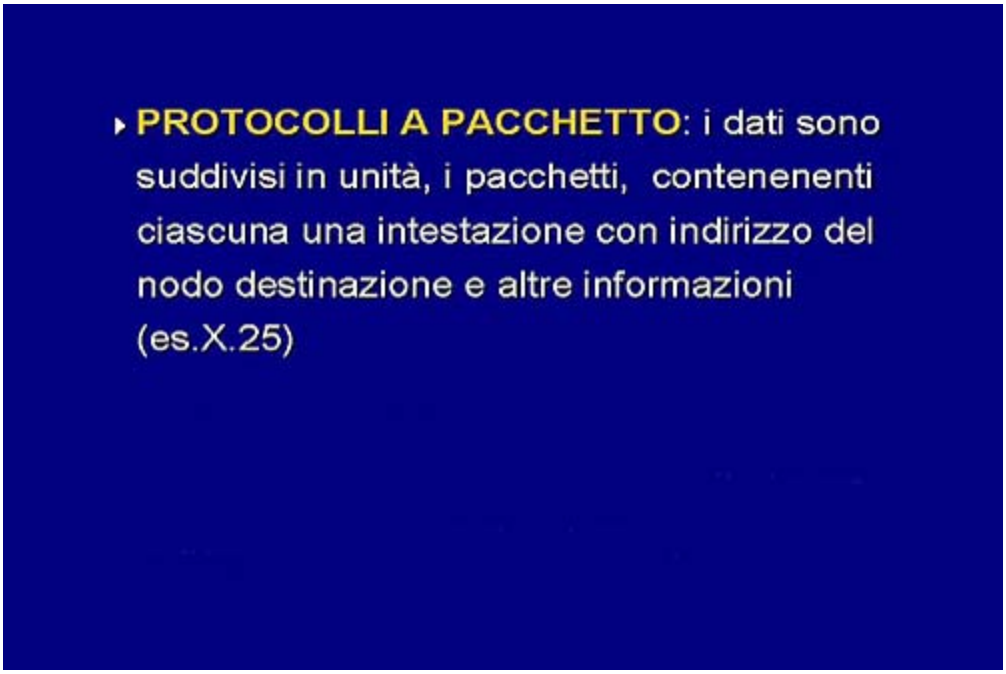


Per quanto riguarda le reti geografiche le topologie sono molto diverse, questo perché le WAN non seguono sostanzialmente alcuna topologia, ma sono delle maglie di nodi più o meno interconnessi tra loro e non è possibile definirne un tipo. Possiamo ad esempio avere una rete geografica realizzata con due nodi, o un nodo interconnesso ad una stella, cioè ad un nodo al quale sono interconnessi molti altri e così via. Ci si riferisce quindi alle reti geografiche come topologie a maglia, formate da nodi di rete (gli oggetti azzurri) interconnessi tramite link, cioè connessioni geografiche di tipo punto a punto (le linee) e infine dai nodi terminali (gli oggetti gialli), che sono interconnessi ai nodi di rete attraverso dei punti di accesso. Su questa interconnessione tra nodo terminale e nodo di rete è localizzata quella che viene chiamata interfaccia tra utente e rete: detta più propriamente la UNI (User-to-Network Interface). Ci si riferisce spesso a questa UNI, lo vedremo nelle lezioni successive, come a quell'insieme di standard e tecnologie che supportano l'interconnessione del nodo terminale con il nodo di rete.

Trasmissione dei dati nella rete

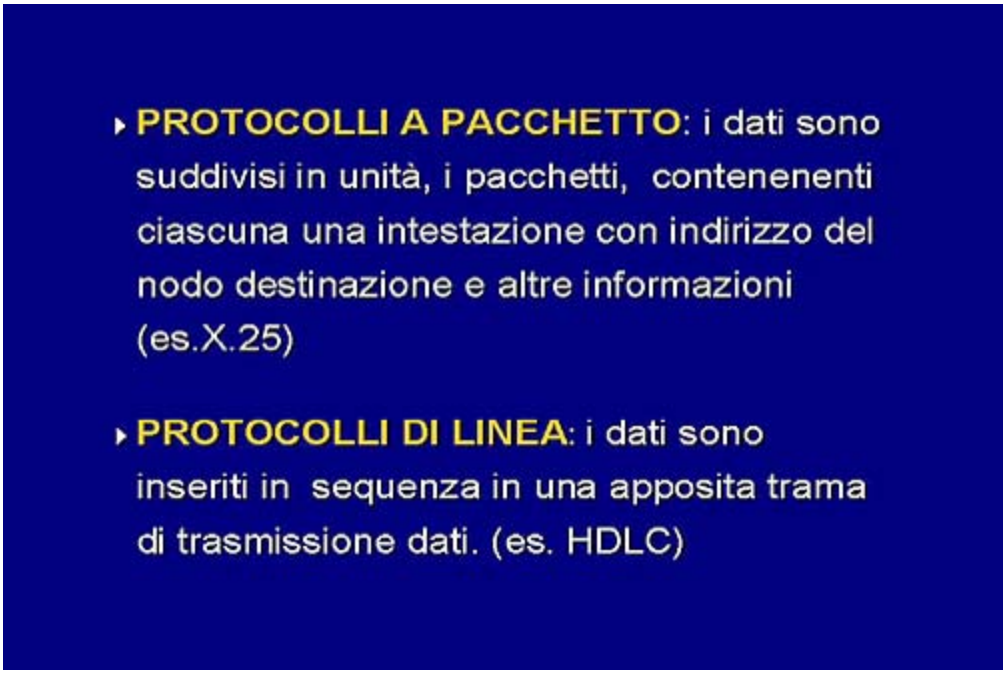
La trasmissione dei dati nella rete avviene rispettando determinati protocolli e cioè formati di dati più regole di trasmissione. È molto importante definire il concetto di protocollo: non è altro che un insieme di regole. Nel momento in cui io devo parlare con un altro, decido come devono essere strutturati i messaggi che ci scambiamo. Per esempio la grammatica della lingua italiana è un protocollo, infatti rispettando le regole di tale grammatica posso essere capito da un'altra persona che conosce queste regole. L'insieme delle regole con cui i dati vengono scambiati e organizzati viene detta sintassi del protocollo. Ci sono poi delle regole di trasmissione, per esempio è previsto che nel momento in cui io voglio approcciare un altro sistema, debba fare richiesta, ricevere l'autorizzazione e solo in quel momento possa iniziare ad inviare dei dati. Questo insieme di scambi informativi è anch'esso parte del protocollo: ogni singolo scambio informativo è organizzato seguendo un formato e delle regole particolari, come ad esempio la stessa sintassi della lingua italiana.

Protocolli a pacchetto



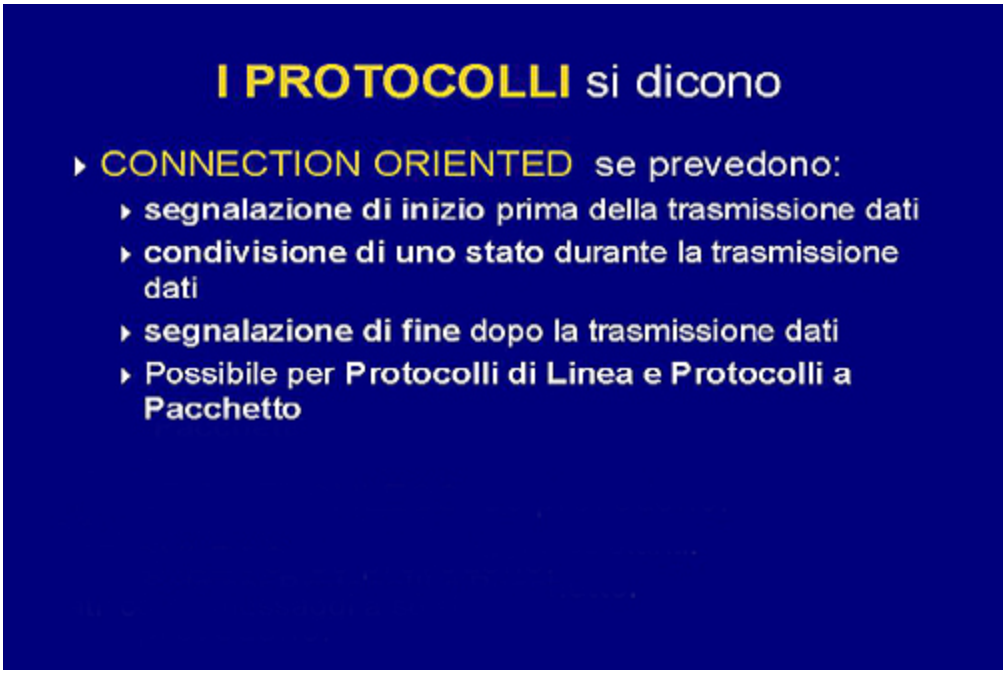
Abbiamo protocolli a pacchetto che sono quelli che vengono utilizzati nelle reti di calcolatori. In tali protocolli i dati sono suddivisi in unità, cioè in blocchi, che vengono appunto chiamati pacchetti, ciascuno dei quali contiene una intestazione con un indirizzo del nodo destinazione e altre informazioni (esempio l'X.25). Questa affermazione è generale e non del tutto vera. Quando un nodo terminale deve comunicare con un altro nodo terminale manda l'informazione in forma "pacchettizzata". Invia quindi dei pacchetti, in ognuno dei quali devono essere indicati oltre ai dati da trasferire anche il destinatario. Ci sono quindi informazioni di controllo: mittente, destinatario, se hanno una particolare priorità ecc. e informazioni vere e proprie (es: payload). Ci sono protocolli di rete, come ad esempio l'X.25, che non necessitano di avere il nodo destinazione, ma semplicemente ,come vedremo, un identificatore. In altri protocolli invece ogni singolo pacchetto contiene l'indirizzo del nodo destinazione ed eventualmente anche del nodo sorgente; in tal caso la rete viene associata ad un piano di indirizzi.

Protocolli di linea



Abbiamo poi i protocolli di linea. In tali protocolli i dati sono inseriti in sequenza in un'apposita trama di trasmissione dati. I protocolli di linea sono quelli che vengono utilizzati ai capi di una linea. Per esempio, se nell'ambito di una rete geografica due nodi sono direttamente interconnessi da una linea, su quella avremo un protocollo di linea. Un protocollo a pacchetto viene invece utilizzato per scambiare dati tra due nodi che non sono direttamente interconnessi, ma che sono invece interconnessi ad una rete. Nell'ambito di un protocollo di linea l'indirizzamento di fatto è inutile, dato che, se un nodo invia i dati su una linea, il destinatario sarà sicuramente il nodo che si trova all'altro capo della linea. Nel caso in cui la linea non sia del tipo punto a punto ma sia un bus, come nel caso Ethernet, dovrà essere indicato anche l'indirizzo del nodo ricevente. Qui abbiamo due esempi l'X25 e HDLC, quest'ultimo è uno dei più noti protocolli di linea.

Protocolli connection oriented 1



Vediamo di fare un'altra distinzione. Abbiamo protocolli (o comunicazioni) " connection oriented ", si prevedono: una segnalazione d'inizio prima, una condivisione di uno stato durante e una segnalazione di fine al termine della trasmissione dati e questo ovviamente è possibile sia per protocolli in linea che per quelli a pacchetto. Vediamo cosa vogliamo dire: nella trasmissione " connection oriented ", come si può vedere, esiste una fase di inizio durante la quale il nodo che vuole iniziare la trasmissione dati segnala (parola usata tipicamente in ambito telefonico) al suo interlocutore (che potrebbe essere un nodo interconnesso o un nodo che si trova chissà dove) che intende interconnettersi e iniziare uno scambio informativo. Questa segnalazione di inizio prima della trasmissione comprende oltre alla fase di richiesta anche, ovviamente, una fase di risposta in cui il nodo destinatario,

Protocolli connection oriented 2

quello che viene interessato dalla trasmissione, dichiara al nodo trasmittente di essere disposto ad effettuare lo scambio dei dati. Allora, se vogliamo andare più nel dettaglio senza entrare nel tecnico, avremo che il nodo trasmittente effettua una segnalazione di richiesta, cioè chiede a quell'altro di iniziare. L'altro, ovviamente, quando riceve questa richiesta viene risvegliato ("mi stanno facendo una richiesta"). Questo fatto viene chiamato nella terminologia telefonica "indication", cioè mi viene segnalato che c'è qualcuno che sta chiamando. A questo punto lui può accettare oppure no, cioè da una risposta positiva o negativa e quando perviene al trasmettitore, cioè a quello che aveva iniziato la richiesta, diventa una conferma. Queste transazioni: richiesta, risveglio del ricevitore, risposta e conferma, chiudono la fase di stabilimento della connessione. Al termine di questa esiste una connessione: il trasmettitore e il ricevitore sanno di essere interconnessi, condividono uno stato. A ciascun dei due potremmo andare a chiedere: "tu ora sei interconnesso a qualcuno?". "Sì io ho una connessione in corso con quell'altro". Il quale sa di avere una connessione in corso con il primo. Quindi condividono uno stato durante la trasmissione dati. Ad esempio il trasmettitore dice: "sono connesso con il sistema B e gli ho già mandato 2500 byte gliene devo mandare ancora 3000".

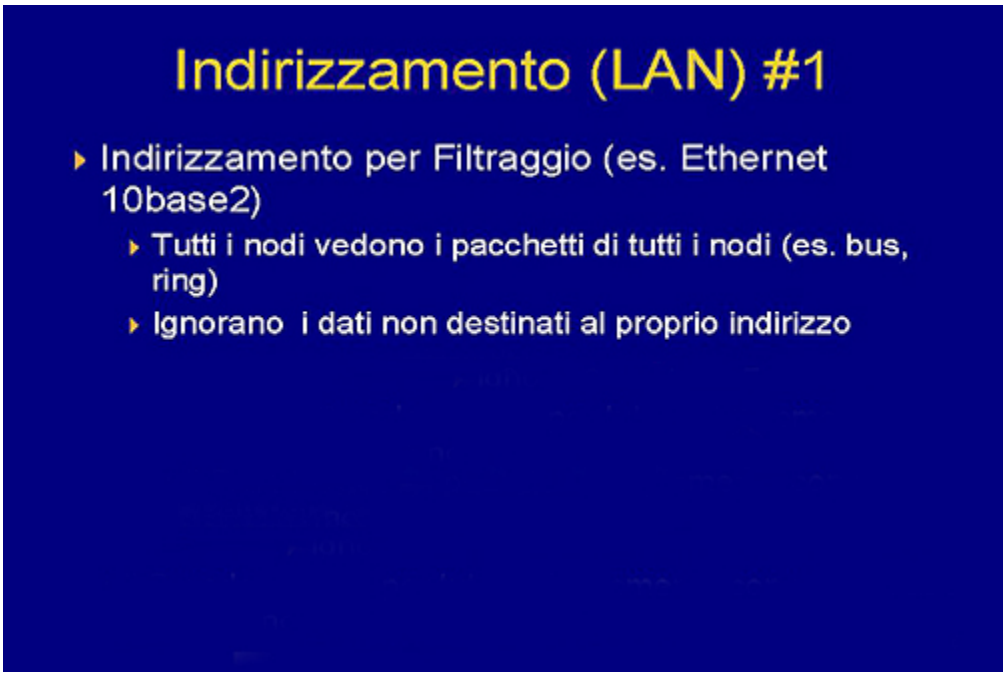
Protocolli connection oriented 3

E l'altro è connesso con il sistema A, ha già ricevuto 2500 byte e ne aspetta degli altri. Una volta terminata la trasmissione dati, il trasmettitore, quello che aveva iniziato la connessione con la richiesta, attiva di nuovo una fase di segnalazione nella quale dichiara di aver finito. Manda una segnalazione di fine che arriva al ricevitore il quale accetta la terminazione. In questo modo avviene la terminazione della connessione che a questo punto non c'è più. Va ricordato che questi protocolli "connection oriented" hanno 3 fasi: lo stabilimento della connessione, lo scambio dati durante l'esistenza della connessione e la terminazione. I protocolli "connection oriented" esistono sia all'interno di protocolli di linea (due sistemi interconnessi da un canale) che a livello di protocolli a pacchetto, come quelli che abbiamo visto prima.

Protocolli connectionless

L'altro tipo di protocolli è quello identificato dalla parola connectionless, cioè senza connessione. Questi prevedono l'invio di dati come messaggi a sé stanti ed esistono solo per protocolli a pacchetti. Sono più semplici degli altri perché, in questo caso, non abbiamo stabilimento di una connessione: non viene prima messa in piedi una connessione. Quindi il sistema trasmittente non deve segnalare a quell'altro che vuole ricevere un'autorizzazione e soltanto in seguito inviare dei dati, segnalare la fine, richiedere la terminazione e ricevere una conferma di terminazione. In questo caso semplicemente mando dei dati e ogni pacchetto che io invio è un messaggio a sé stante. Ovviamente, in questo caso, i messaggi raggiungono il ricevitore ciascuno per conto proprio; sarà il ricevitore che, se necessario, dovrà rimetterli assieme per costruire l'intero messaggio.

Indirizzamento LAN 1



Vediamo rapidamente l'indirizzamento per le Lan. Allora, all'interno delle Lan abbiamo un indirizzamento per filtraggio: vuol dire essenzialmente che tutti i nodi vedono i pacchetti di tutti i nodi, ma ignorano i dati non destinati al proprio indirizzo. Cosa vuol dire? Significa che se ho un unico bus è chiaro che tutti i nodi sono in ascolto su quel bus. Quindi, ogni messaggio o pacchetto che viene indirizzato ad uno di questi nodi interconnessi viene visto da tutti, ma soltanto quello che risponde a quell'indirizzo ne aspetta effettivamente la ricezione. Abbiamo qui l'esempio di Ethernet 10base2, che è un particolare modo di realizzazione della rete Ethernet basato su un bus, cioè un cavo coassiale, che percorre un intero edificio, come descrivevo all'inizio. Quindi, nel momento in cui la rete Ethernet (vi dicevo anche che oggi non è pratica comune realizzare reti Ethernet in questa maniera ma ce ne sono ancora) è realizzata con una topologia a bus, quindi col 10base2 che è un particolare standard, effettivamente tutti i nodi vedono tutto ciò che passa sul bus.

Indirizzamento LAN 2

Per commutazione. Lo standard è il 10baseT. Nel momento in cui oggi devo realizzare una rete locale basata su standard Ethernet, o fast Ethernet, uso il cablaggio tipicamente 10baseT, che è quello stellato. Vi avevo detto all'inizio che oggi le reti vengono realizzate essenzialmente su topologia a stella. In questo caso ogni nodo è interconnesso ad un concentratore o Switch.

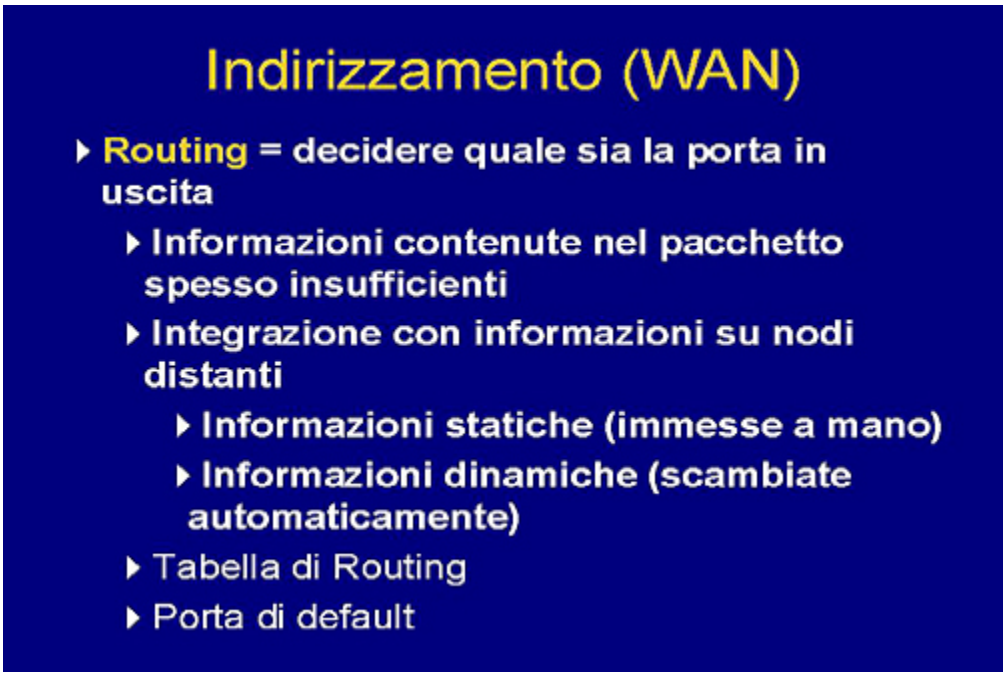
Indirizzamento LAN 3

In realtà bisogna essere un po' più precisi, perché il nostro concentratore può essere uno Switch, notate che la traduzione della parola vuol dire commutatore, che riceve da una linea, guarda l'indirizzo e trasmette ciò che ha ricevuto sulla linea opportuna. Quindi, nel momento in cui un "frame" viene trasmesso dal sistema numero 1 e raggiunge il nostro commutatore (Switch) per il sistema numero 4, ovviamente gli altri sistemi non vedono questi dati. Questo è quello che succede se il concentratore è uno Switch; ci sono però anche dei casi in cui il concentratore è semplicemente una realizzazione in forma centralizzata di un bus di comunicazione. In questi casi, anche con il cablaggio 10baseT, si ha effettivamente un indirizzamento per filtraggio.

Indirizzamento WAN 1

Nel caso delle reti geografiche abbiamo sempre la commutazione, cioè i nostri nodi, che sono magliati cioè realizzati attraverso interconnessioni punto a punto di vario tipo, effettuano sempre una commutazione. Ricevono i dati sempre da una particolare linea, guardano a chi sono diretti e li mettono su un'altra porta di uscita, in maniera del tutto analoga ai dispositivi per LAN commutate, quelle che abbiamo visto.

Indirizzamento WAN 2



Che cosa devono fare questi nodi delle reti geografiche? Devono effettuare il cosiddetto routing e cioè decidere qual è la porta verso la quale devono scrivere. Nel momento in cui abbiamo un nodo di rete che riceve dei dati da una certa port,a deve guardare all'interno di questo pacchetto che ha ricevuto e decidere dove mandarlo. Questo è quello che si chiama routing. Molto spesso le informazioni che sono contenute nel pacchetto sono insufficienti e di conseguenza il nostro nodo di rete si trova a dover decidere dove mandare i pacchetti senza le informazioni necessarie. Deve pertanto utilizzare altre informazioni, sui nodi distanti, che possono essere: statiche e dinamiche. Che cosa vuol dire? Vediamo di spiegare questo aspetto. Io ho la mia rete magliata e dei pacchetti che l'attraversano. A un certo punto uno di questi nodi di rete, o router, riceve un pacchetto, guarda a chi è indirizzato e si domanda: "per raggiungere questo indirizzo di destinazione da che parte devo andare?" Allora, o al suo interno ha una tabella che per ogni possibile indirizzo di destinazione gli dice su quale porta deve mandarlo e questa si chiama tabella di routing. Oppure lui sa che per raggiungere tutti i nodi terminali che non conosce si deve andare in quella che viene chiamata una porta di default. Sostanzialmente il nostro nodo dice: "per alcuni indirizzi di destinazione so dove devo inviare i dati, per altri non la so per cui li mando tutti in una cosiddetta porta di default". Il modo in cui queste tabelle vengono configurate può essere statico, cioè fatto da una persona che inserisce fisicamente queste informazioni nelle tabelle, oppure automatico, quindi dinamico, nel senso che i nostri nodi di rete si parlano tra loro e si scambiano le informazioni per aggiornarsi l'un l'altro le tabelle di routing.

Commutazione di pacchetto

Sempre come terminologia di base, i tipi di commutazione che possiamo esaminare sono: la commutazione di pacchetto e quella che viene utilizzata sostanzialmente in tutte le reti di calcolatori, cioè la copiatura di ciascun pacchetto da una porta d'ingresso ad una porta d'uscita, decisa sulla base dell'indirizzo di destinazione del pacchetto. Un esempio è IP, quello che abbiamo descritto fino ad ora. Sostanzialmente un nodo di rete non fa altro che eseguire la commutazione di pacchetto.

Commutazione di circuito

C'è anche la commutazione di circuito in cui abbiamo una copiatura di un flusso di bit da una porta di ingresso ad una di uscita, decisa sulla base di un identificazione del flusso, per esempio la PSTN che è la rete telefonica. Nel caso

di commutazione di circuito non abbiamo la suddivisione dei dati in pacchetti ma abbiamo delle connessioni a livello di circuito, quindi a livello di flussi di bit tra una sorgente e una destinazione. Nel momento in cui una sorgente ed una destinazione devono scambiarsi dei dati attraverso la commutazione di circuito, viene stabilito effettivamente un circuito tra loro e su questo viene trasmetto il flusso di bit.

Circuito virtuale

Una modalità simile che possiamo provare a mettere in alternativa alle tre è quella del circuito virtuale. Lo utilizzo quando voglio realizzare un circuito tra due interlocutori, quindi tra due sistemi, usando una commutazione di pacchetto. In questo caso realizzo il circuito non attraverso un circuito fisico, ma attraverso un meccanismo di trasporto a pacchetto.

Vantaggi e svantaggi della commutazione di pacchetto

Vediamo rapidamente i vantaggi e gli svantaggi della commutazione di pacchetto. Ovviamente tra i vantaggi c'è la concorrenza di più connessioni: nella commutazione di pacchetto ho la possibilità di avere più scambi dati simultanei tra due nodi sulla rete, perché non utilizzo in maniera statica le risorse. La possibilità di fare il cosiddetto rerouting: cioè di utilizzare percorsi alternativi in caso di guasto anche durante la connessione. Nel momento in cui due nodi sono interconnessi tra loro e a un certo punto per qualche ragione si verifica un guasto si può fare il rerouting della connessione. Ovviamente abbiamo un costo basso della comunicazione per il semplice fatto che, grazie alla condivisione delle risorse, più utenti ne dividono il costo. Tra gli svantaggi della comunicazione di pacchetto, in particolare c'è l'impossibilità di garantire la capacità, cioè la velocità di trasmissione di ciascuna connessione non soltanto in termini di banda ma anche in termini, vedremo poi, di ritardo. La possibilità di avere congestione del canale: nel momento in cui troppi dati rispetto alla quantità prevista affluiscono ad un nodo di rete, questo può essere incapace di gestirli e di effettuare la commutazione in tempi rapidi. Poi ci possono essere problemi di sicurezza dovuti alla condivisione del mezzo nel senso che, nella commutazione di pacchetti, più connessioni di rete condividono lo stesso mezzo. I primi due svantaggi sono quelli che hanno sconsigliato fino ad oggi, ma le cose stanno cambiando, l'uso della commutazione di pacchetto per la trasmissione di segnali come la voce.

Vantaggi e svantaggi della commutazione di circuito 1

Per quanto riguarda i vantaggi e gli svantaggi della commutazione di circuito, parliamo della capacità del canale. Nel momento in cui stabilisco un circuito tra me e un mio interlocutore, mi viene allocata, quindi garantita, una determinata capacità. La tariffazione della commutazione di circuito è dipendete dal tempo: più a lungo tengo il circuito occupato e più ho una tariffa elevata, sia che usi sia che non usi il circuito. È il solo fatto di tenere occupata la risorsa che costituisce un costo per chi mi fornisce il circuito. Ovviamente è più facile controllare la sicurezza (questo era uno svantaggio del caso precedente). Non esiste overhead, cioè un sovraccarico di interpretazione dell'indirizzo: perché nel momento in cui esiste un circuito fisico realizzato tra me e un interlocutore, tutti i bit che io trasmetto su questo circuito sono per definizione destinati all'interlocutore e non c'è bisogno che lo divida in pacchetti specificando per ognuno di essi a chi è destinato. Gli svantaggi sono: il costo elevato a causa della allocazione privata del canale, perché nel momento in cui questo viene realizzato esclusivamente per me il costo diventa molto elevato non essendo condiviso con altri utenti. È più difficile effettuare il rerouting se c'è un guasto perché bisogna rieffettuare la connessione e quindi ristabilire il nostro circuito. Questo chiude il discorso sulla parte introduttiva reti di calcolatori. Vorrei quindi semplicemente sintetizzare alcuni elementi che penso possano rimanere come traccia, anche per una discussione successiva. In particolare il discorso che abbiamo fatto all'inizio che una rete corrisponde ad un piano di indirizzamento; credo che questo sia una cosa importante perché per lo meno da un riferimento preciso.

Vantaggi e svantaggi della commutazione di circuito 2

La rete locale, per esempio una rete Ethernet, in questo senso non è una rete, lo è nel momento in cui sopra una infrastruttura Ethernet sovrappongo un piano di indirizzamento che mi viene dato da un amministratore di rete locale. Nel caso di una rete geografica tipicamente questo piano di indirizzamento invece è amministrato dal fornitore di rete geografica. Questo è il discorso sul significato di rete Abbiamo visto poi rapidamente le tre categorie: Lan, Wan e Man. Di fatto le Man, altra informazione che può rimanere, oggi come oggi non esistono: nel passato erano associate ad una particolare tecnologia, ormai abbastanza abbandonata, per lo scambio dei dati su area campus. Oggi si parla quasi esclusivamente di Lan, o di Lan estese a livello di campus, e di reti geografiche. Sono le due categorie principali, esempio tipico delle reti geografiche può essere internet.

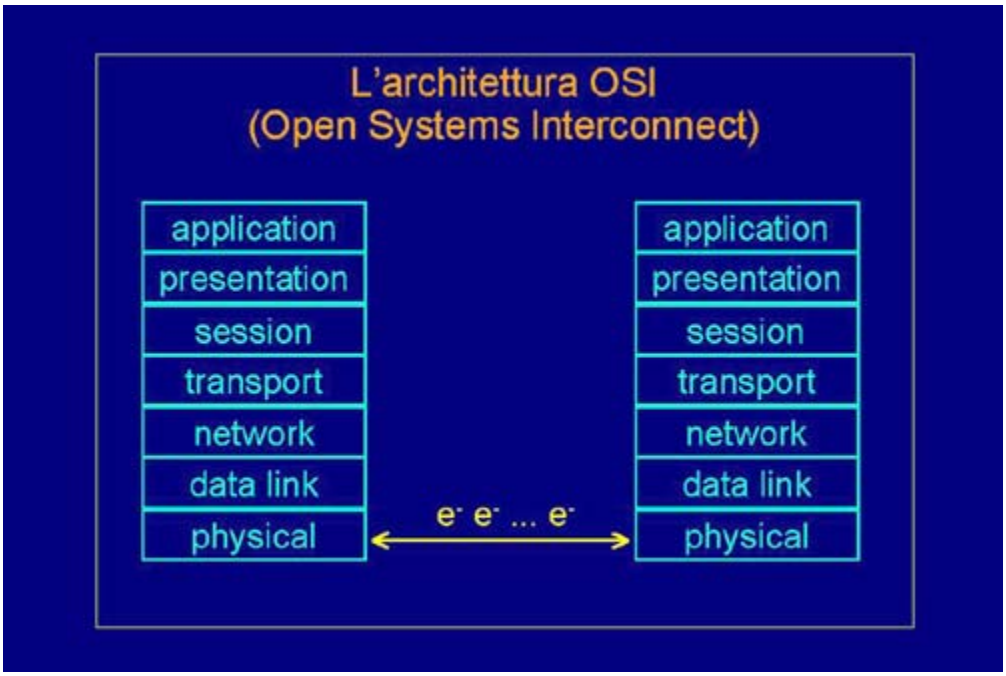
Vantaggi e svantaggi della commutazione di circuito 3

L'altra cosa che ritengo importante venga sottolineata è il discorso delle topologie. Le topologie del cablaggio sono una cosa, i meccanismi di allocazione dei canali sono un'altra cosa. Quindi posso avere una rete cablata a stella, che è quello che oggi gli standard di cablaggio strutturato prevedono, e su di essa posso avere reti a bus, a ring o a stella. Nel caso tipico delle reti a bus, realizzate su topologia a stella, vengono proposte anche delle variazioni, per cui gli standard tipici delle reti a bus così come sono nati, in particolari mi riferisco ad Ethernet, evolvono verso reti stellate. È chiaro che non è certo questa presentazione la sede in cui discutere questo discorso, però bisogna tener presente che effettivamente esiste questa evoluzione in senso opposto al passato. Una volta, prima di Ethernet, esistevano le reti a stella, poi è arrivato Ethernet che ha proposto le reti a bus e adesso sta ridiventando a stella. Questi sono gli elementi principale che possiamo proporre come discussione alla fine di quest'ora.

L'architettura di rete TCP/IP

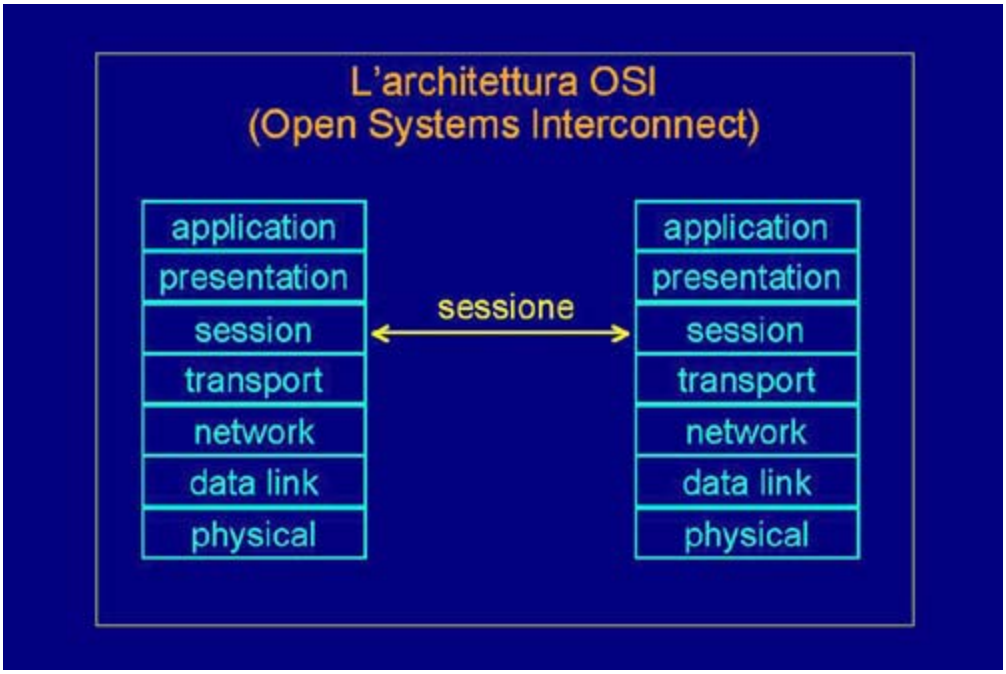
Antonio Lioy

OSI: Fisico - Data link



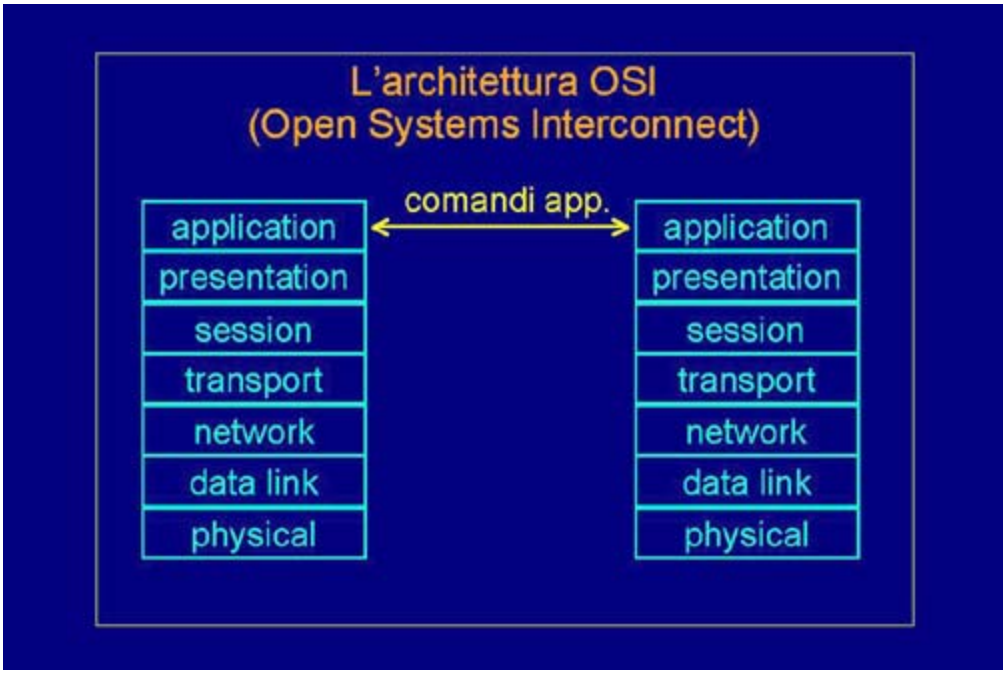
Per poter rendere sicura una rete bisogna prima aver capito molto bene in quale modo funziona. Ecco quindi che in questa breve lezione parleremo dei meccanismi di funzionamento delle reti, concentrandoci in particolare sulle reti TCP/IP che oggigiorno sono quelle più utilizzate. In generale il modello a cui obbedisce il funzionamento di una rete di calcolatori è quello definito dall'architettura OSI, che significa interconnessione di sistemi aperti. OSI è un modello che descrive quali sono i vari livelli di astrazione e a volte anche di implementazione in cui due calcolatori colloquiano. Il primo è il cosiddetto "livello fisico". A questo livello due calcolatori sono in comunicazione scambiandosi dati secondo un contenuto fisico appropriato. Ad esempio due calcolatori, collegati tramite una rete Ethernet o ISDN, possono trasmettersi dati scambiandosi in realtà degli elettroni, ossia delle correnti o delle tensioni. Il "livello fisico" serve per trasmettere fisicamente i dati forniti dal livello 2, detto "data link", di trasmissione dei dati. A livello "data link" noi non trattiamo più col formato fisico dei dati inteso come elettroni o fotoni, ma con bit logici, quindi zeri e uni.

OSI: Network - Trasporto - Sessione



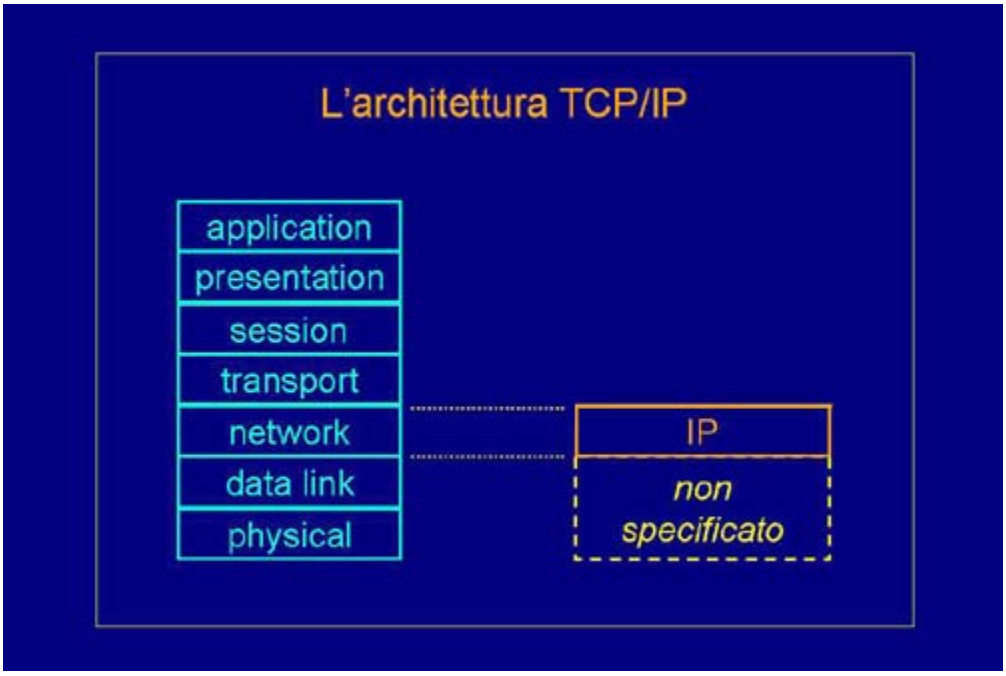
Questi bit logici a loro volta vengono utilizzati per formare i cosiddetti pacchetti di rete. Infatti il livello 3 di trasmissione è chiamato il "livello rete" ed è il primo in cui ci si rende completamente indipendenti dal substrato di trasmissione. È detto "end to end": dall'indirizzo del mittente a quello del destinatario ignorando quale sia il cammino intermedio. Ci penserà l'infrastruttura di rete a trasmettere i dati, sottoforma di pacchetti, dalla macchina che ha indirizzo numero uno alla macchina che ha indirizzo numero due. I pacchetti di rete servono a creare dei canali logici che appaiono a livello 4, il cosiddetto "livello di trasporto", in cui due calcolatori sono collegati da un canale virtuale o da una comunicazione logica di tipo messaggio. I canali logici sono delle sorti di oleodotti dentro cui transitano i bit invece che il petrolio. Bisogna però decidere quali sono le regole per costruire un oleodotto; questo in termini di calcolatori viene deciso a livello 5 ossia: il "livello di sessione".

OSI: Presentazione - Applicazione



Sopra la sessione esistono ancora altri due livelli. Il "livello presentazione" è quello che effettua la trasformazione del formato dei dati, per adattarli al tipo di codifica che viene utilizzato tra due diversi sistemi che comunicano. Infine, a livello 7, si parla di "applicazioni": ossia tutti i dati che sono stati trasportati attraverso la rete sono serviti a creare dei comandi applicativi, a svolgere una qualche funzione. Dal punto di vista dell'utente questo è l'unico livello che interessa: tutti gli altri sono semplicemente ausiliari che servono a trasportare queste informazioni e a far funzionare una applicazione via rete. Questo è un modello teorico.

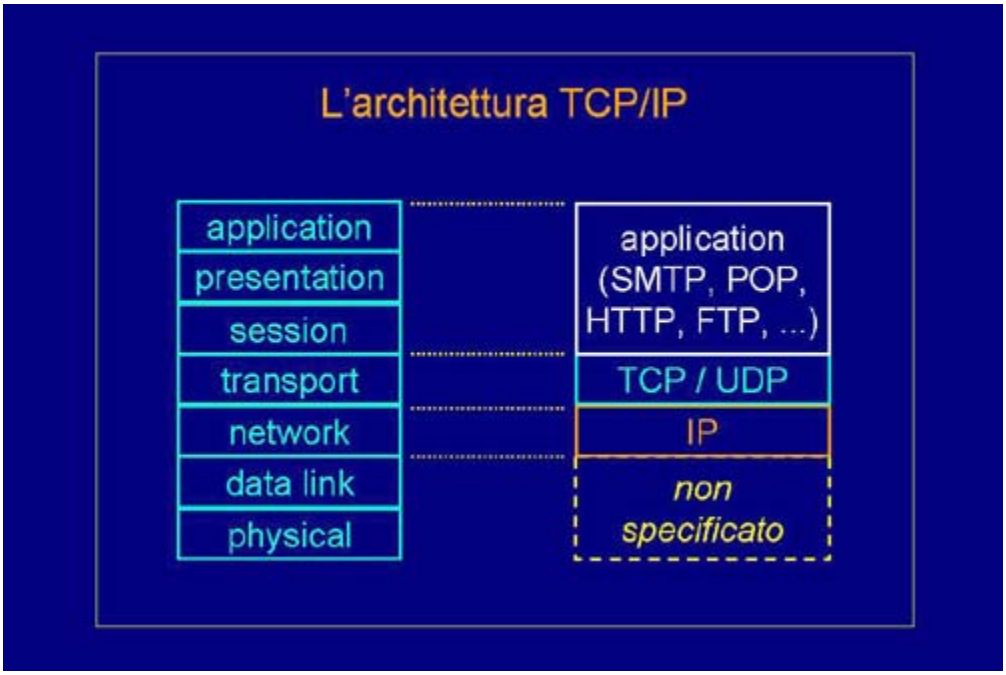
L'architettura TCP/IP 1



Vediamo adesso come nella realtà questo modello venga implementato dalla rete oggigiorno più utilizzata: la rete

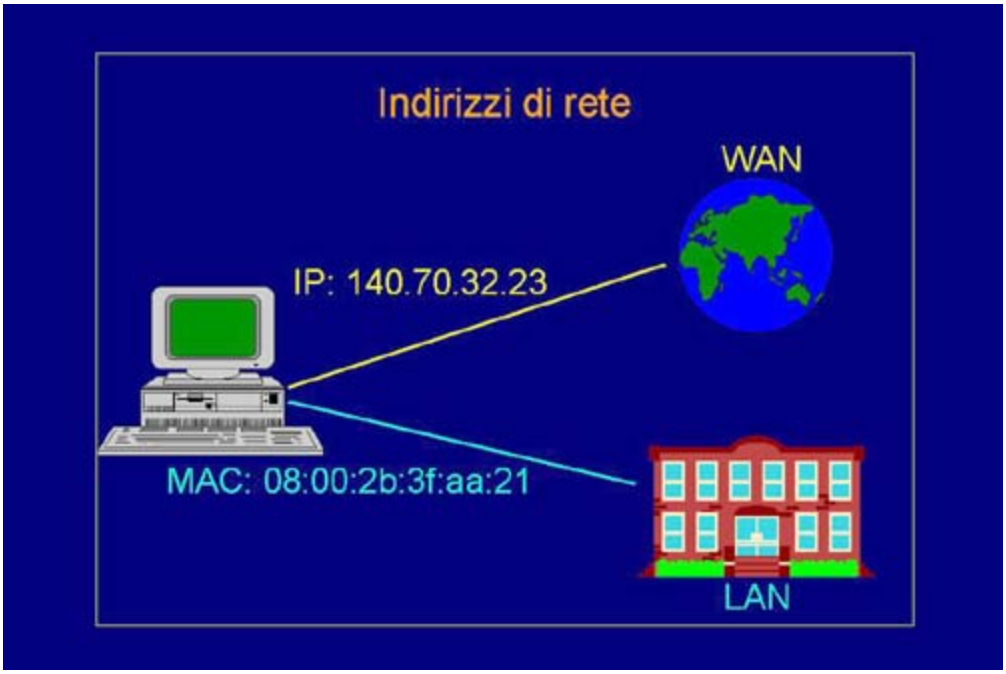
TCP/IP. Confronteremo tale architettura rispetto al modello logico OSI. La prima cosa, per cominciare, è che TCP/IP non specifica assolutamente alcun tipo di formato, protocollo o codifica per quanto riguarda i livelli bassi, ossia il livello fisico e il livello 2. Questo significa che qualunque sistema che sia in grado di implementare i livelli 1 e 2, in modo conforme a quello che i livelli superiori di TCP/IP si aspettano, può benissimo funzionare con tutti gli altri protocolli dello stack di rete. Il primo livello in cui TCP/IP è presente è il terzo, il livello rete. Questo è implementato dal protocollo IP (Internet Protocol): originariamente l'architettura TCP/IP è stata concepita per effettuare l'interconnessione di reti locali e solo recentemente è stata utilizzata anche come protocollo al loro interno.

L'architettura TCP/IP 2



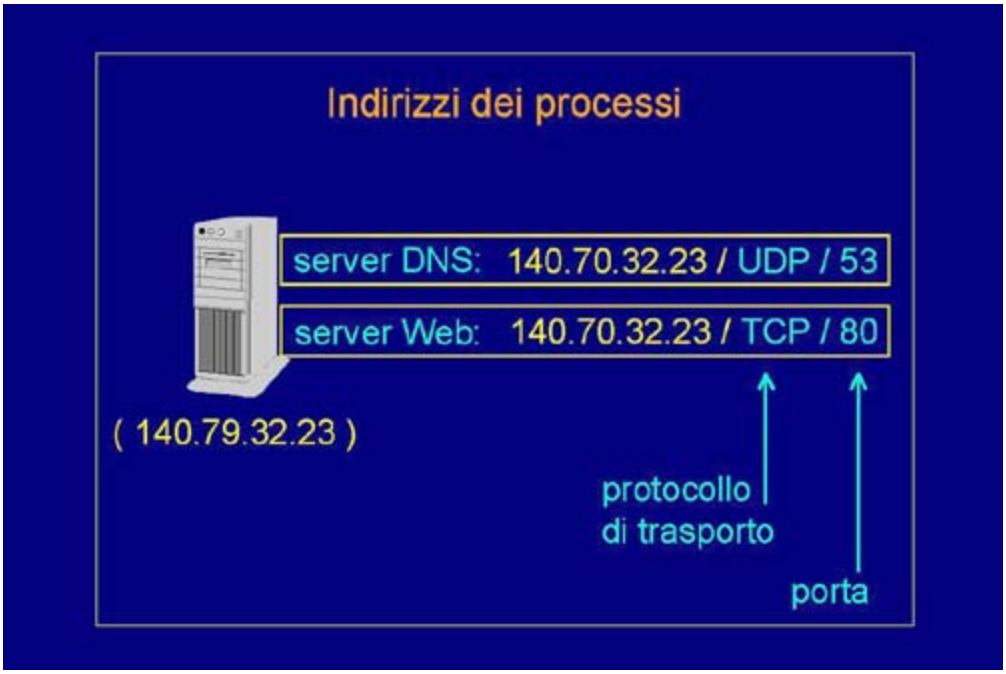
TCP/IP ha anche specificato dei protocolli per quanto riguarda il livello di trasporto. In particolare due sono i principali protocolli a livello 4: il TCP, che offre un canale logico virtuale appoggiato sopra IP, e il protocollo UDP, che utilizza invece dei messaggi di tipo datagram per consegnare messaggi "end to end" all'interno della rete. TCP/IP non frammenta ulteriormente la trasmissione ai livelli superiori ma ingloba tutto quanto in un unico livello applicativo. Questo significa che ciascuna applicazione deciderà autonomamente quali tipi di sessione, di formato dati e di comandi applicativi utilizzare. Quindi, in questo senso, esistono dei protocolli unici che specificano insieme tutti e tre i livelli. Ad esempio, il protocollo SMTP è quello utilizzato per la trasmissione dei messaggi di posta elettronica, il POP è quello utilizzato per trasmettere i messaggi che sono depositati nella casella postale fino alla postazione di lavoro dell'utente e così via. Quindi diciamo che, in generale, TCP/IP è un insieme di protocolli più semplificato rispetto al modello teorico OSI, avendo in questo modo il vantaggio di risultare più veloce, più leggero e più facilmente gestibile nelle reti reali.

Indirizzi di rete



Affinché due calcolatori possano funzionare e comunicare attraverso una rete, a ciascuno di essi deve essere dato un indirizzo. Esistono però svariati tipi di indirizzi: in particolare se il nostro calcolatore è collegato all'interno di una rete locale, quella che normalmente si chiama una Lan, dovrà avere un indirizzo che lo contraddistingue nei confronti delle apparecchiature che costituiscono tale la rete. Ad esempio qui vedete indicato un indirizzo su 48 bit tipico delle reti Ethernet. Se però il nostro calcolatore desidera anche comunicare attraverso una rete geografica, quale ad esempio la rete internet, avrà bisogno anche di un indirizzo univoco a livello mondiale. Siccome non è certo che il nostro destinatario utilizzi il medesimo tipo di tecnologia che utilizziamo noi, e soprattutto perché la tecnologia delle reti locali non può essere utilizzata anche per coprire distanze geografiche, bisognerà fornire un altro tipo di tecnologia di interconnessione e anche un altro tipo di indirizzo. Ecco quindi che per i collegamenti in rete geografica il medesimo nodo di elaborazione verrà identificato con un altro indirizzo. All'interno della rete TCP/IP si usano gli indirizzi IP che sono indicati con quattro gruppi numerici ognuno dei quali può variare da 0 a 255, perché in realtà sono indirizzi su 32 bit e quindi ognuno di questi gruppi, separati da punti, corrisponde a 8 bit.

Indirizzi dei processi

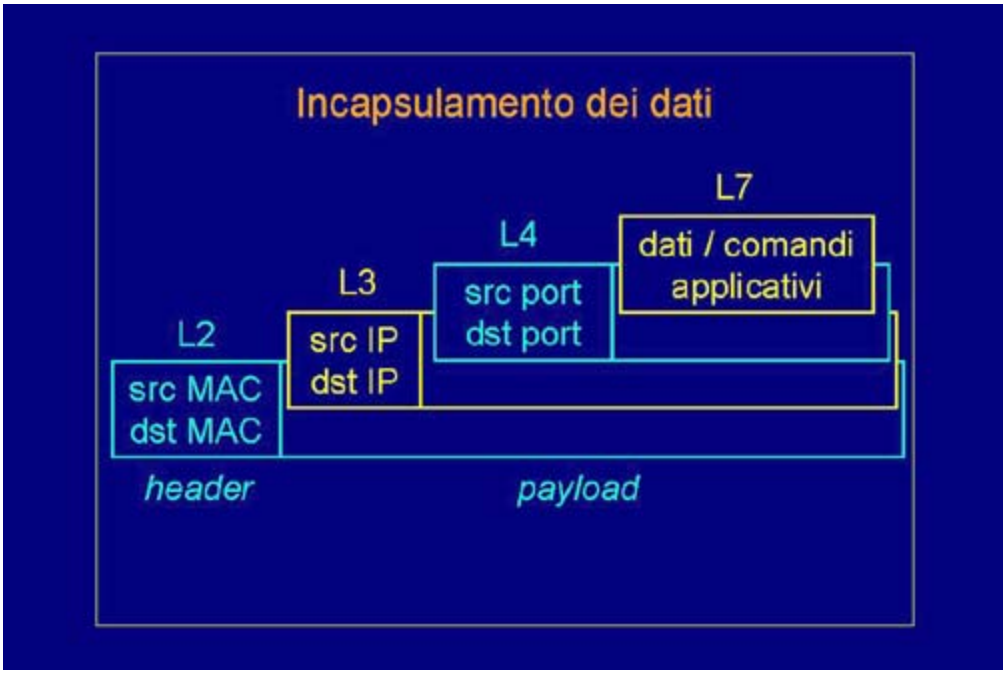


Ma all'interno di un unico nodo di elaborazione possono essere presenti più processi applicativi, tipicamente più servizi: i cosiddetti "server". Quando un'applicazione deve accedere ad uno di questi sevizi ha bisogno di venire a conoscenza, non soltanto dell'indirizzo di rete del nodo di elaborazione da cui il servizio è offerto, ma anche di indirizzare lo specifico processo. Ecco quindi che si parla anche di indirizzi dei processi. Ad esempio su questo nodo di elaborazione, che ha indirizzo IP 140.70.32.23, girano due processi: un server web e uno DNS. Per riuscire a distinguere questi server bisogna dare delle informazioni aggiuntive: il protocollo di trasporto con cui i dati verranno veicolati verso il nostro server e la particolare porta. La porta è una distinzione ulteriore che permette di riconoscere i vari processi attivi su un unico nodo di rete. Ecco allora che il nostro server web potrà essere identificato in base al suo indirizzo IP, al fatto che dialoga tramite il protocollo di trasporto TCP e alla porta 80, quella su cui tutti i server web normalmente sono in ascolto. Ovviamente un server diverso dovrebbe avere un indirizzo diverso. Infatti, il server DNS ospitato sulla medesima macchina (lo si nota perché ha lo stesso indirizzo IP), utilizzerà il protocollo di trasporto UDP, quindi un protocollo diverso da TCP, e una porta diversa, ad esempio la 53.

Incapsulamento dei dati 1

Quando si trasmettono dei dati, ogni livello di rete richiede che siano messi in un formato peculiare di quel livello. Questo vuol dire che i dati a livello applicativo vengono incapsulati in una serie di buste di livello successivo. Quindi, in realtà, i dati che sono trasmessi in rete sono soltanto in minima parte dati applicativi e per la maggior parte sono dovuti al meccanismo di trasporto. In particolare i dati, ad ogni livello, sono trasportati all'interno del cosiddetto "payload" (carico pagante), il quale è preceduto dall'"header" (intestazione), che dice, per quel particolare livello, chi sono il mittente e il destinatario. Ad esempio, a livello 2 l'header conterrà fra gli altri dati anche l'indirizzo di livello 2, il cosiddetto "MAC", del sorgente e quello del destinatario. Ma se questo pacchetto di livello due è stato originato fuori dalla nostra rete locale, vorrà dire che è stato generato da un pacchetto di livello 3. Ed ecco che a livello 3 il payload di livello 2 sarà in realtà scomposto in due parti: un payload di livello tre preceduto da un intestazione di livello 3, che fra gli altri dati conterrà anche gli indirizzi IP del mittente e del destinatario.

Incapsulamento dei dati 2



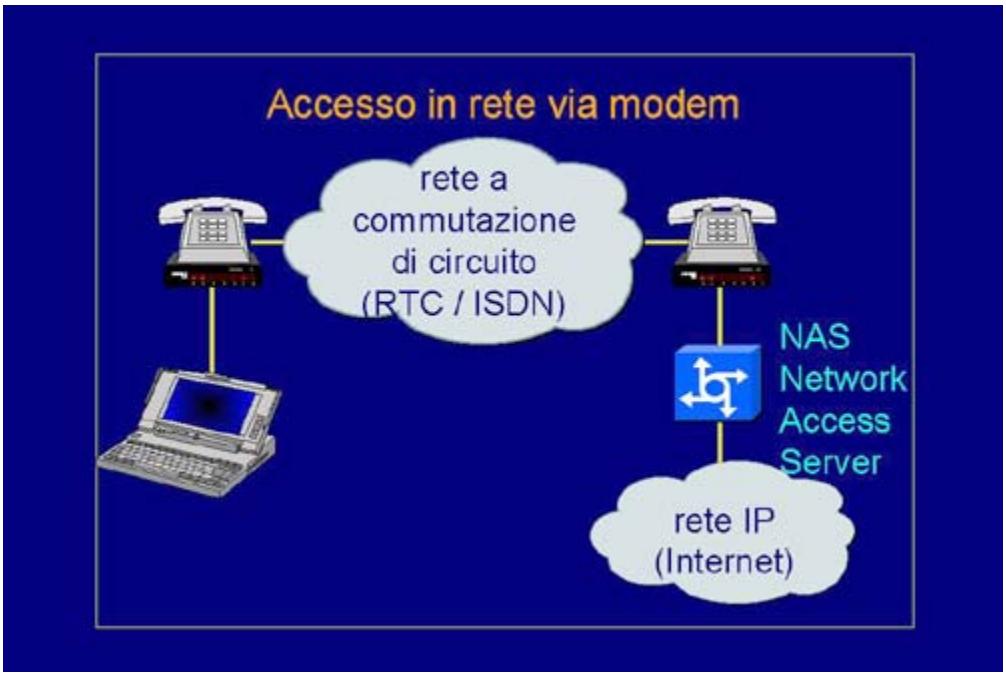
Questo gioco di scatole cinesi prosegue e, ad esempio, il livello 4 specifica che il mittente che aveva questi indirizzi "MAC" e IP era un processo situato in una certa porta. Analogamente il livello 4 specificherà qual è la porta del destinatario. A livello di payload utilizza direttamente i dati o i comandi applicativi che sono stati forniti dal livello 7.

Accesso in rete via modem 1

A questo punto consideriamo quali sono le possibili modalità per accedere in rete. Se una persona dispone di un personal computer a casa, o un portatile, tipicamente non è attaccato direttamente ad una rete locale. Per accedere alla rete geografica, quindi, utilizzerà un modem: una apparecchiatura di telecomunicazione che serve a trasformare i bit forniti dal computer in un segnale adatto alla trasmissione su una rete a commutazione di circuito. Per esempio: la

normale rete telefonica commutata, su cui tutti facciamo le nostre normali telefonate, o la rete ISDN, che è la rete numerica integrata nei dati e nei servizi.

Accesso in rete via modem 2

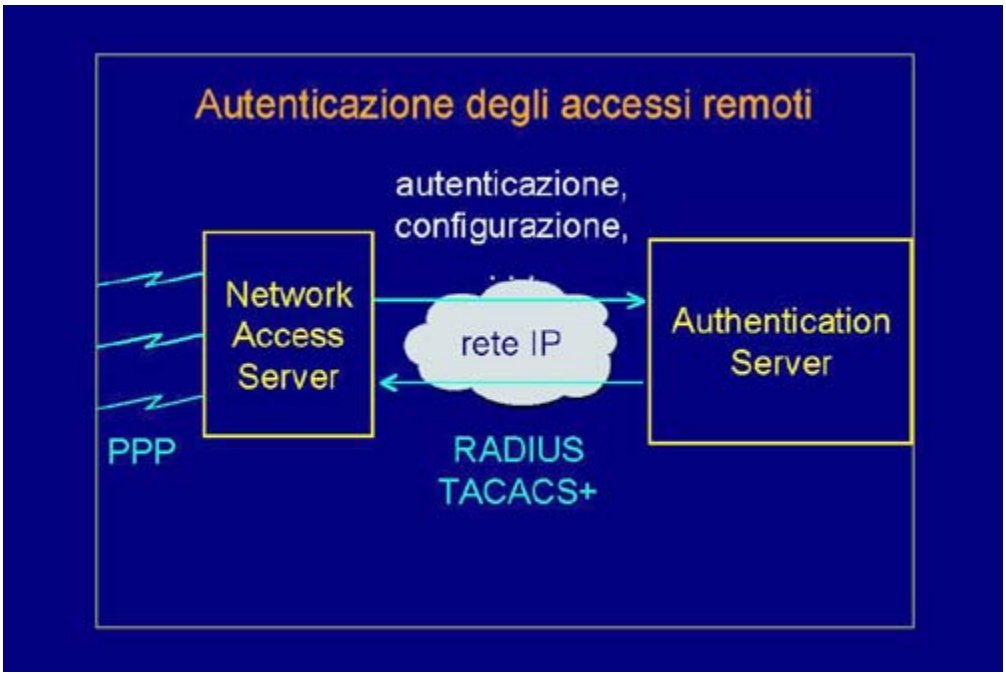


Dall'altra parte ci sarà un'apparecchiatura analoga: ossia un altro modem in grado di decodificare i segnali telefonici e trasformarli in binari. Questi segnali binari verranno forniti a quello che si chiama un NAS (Network Access Server) ossia un nodo che ha proprio il compito di decidere se, in quale misura e come, i dati che arrivano dalla rete telefonica possono essere trasformati in dati appartenenti a una rete di tipo IP. Quindi, per collegarsi tramite un normale computer portatile o un computer casalingo a una rete geografica, occorre disporre a casa nostra di un modem che effettuerà la traduzione da bit ad impulsi fonici. Da parte del ricevente ci dovrà essere, oltre a un modem che effettuerà la demodulazione da impulsi fonici a bit, anche un'apparecchiatura che sarà attaccata in modo permanente alla rete geografica a cui vogliamo collegarci.

Autenticazione degli accessi remoti 1

Ovviamente bisogna evitare che delle persone non autorizzate possano collegarsi alla rete geografica. Per questo motivo, normalmente, il nostro Network Access Server dispone di un elenco di persone abilitate ad utilizzare la rete. Questo tipo di identificazione viene normalmente veicolato tramite un canale cosiddetto PPP. Il "Point to Point Protocol" è un protocollo standard di livello 2, da utilizzarsi su reti commutate, che serve a veicolare protocolli di livello superiore.

Autenticazione degli accessi remoti 2



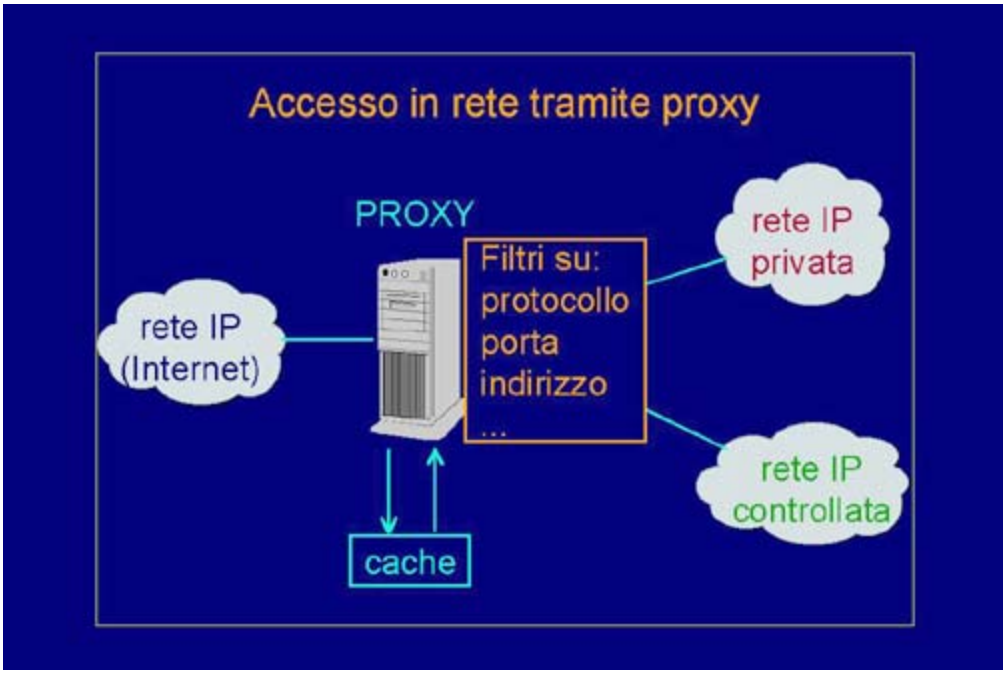
Il NAS può decidere lui stesso di concedere al chiamante l'accesso alla rete, ma solitamente dialoga, tramite una rete IP locale, con un server che fornisce i servizi di autenticazione, di configurazione e per esempio di logging, per più

NAS. Il NAS dialoga con l'authentication server tramite dei protocolli specifici. Il protocollo RADIUS, il TACACS o TACACS PLUS sono attualmente quelli più utilizzati per effettuare l'autenticazione degli accessi remoti, ossia verificare se un utente che sta chiamando un certo numero telefonico ha diritto oppure no a collegarsi alla rete geografica.

Autenticazione dei canali PPP

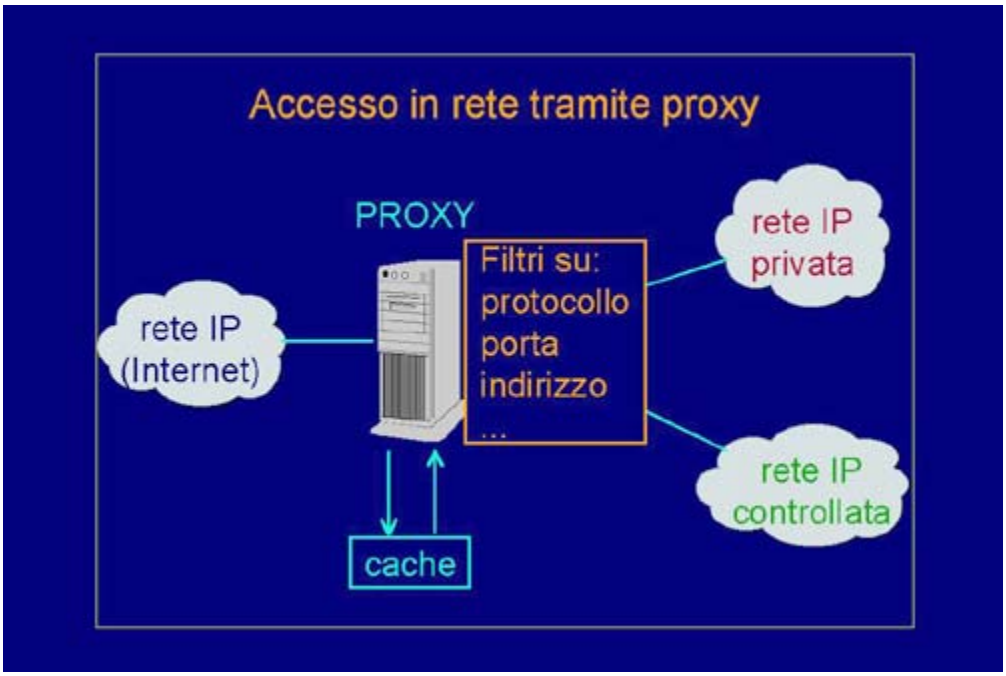
Esistono due modalità base con cui l'utente può veicolare la propria autenticazione all'interno di un canale di tipo PPP. La prima modalità è quella chiamata PAP (protocollo di accesso tramite password). Il sistema PAP invia lo "user name" e la "password" dell'utente, in chiaro, sul canale. È quindi intuibile che è un sistema fortemente sconsigliabile se qualcuno può avere accesso alla linea telefonica. Ad esempio, un fasullo operaio dei telefoni che finge di correggere un guasto nella centralina o comunque qualcuno che possa attaccarsi alla rete telefonica. Per evitare questo genere di attacchi è consigliabile non usare gli stessi "user name" e "password" che già sfruttati per l'accesso ad altri tipi di sistemi, ma usarne uno specifico solo per l'accesso alla rete. Cosa ancora migliore sarebbe evitare il protocollo PAP utilizzando quello alternativo che si chiama CHAP: è un protocollo che si basa su una sfida (challenge) simmetrica basata sulla "password". Quindi, l'utente ha sempre assegnato uno "user name" e una "password" per entrare in rete, ma la seconda non viene visualizzata e non viene trasmessa attraverso la linea telefonica. Di per se è un protocollo che sarebbe altamente preferibile ma purtroppo la maggior parte degli Internet Service Provider non lo implementano quasi mai e quindi permettono che esista questa debolezza che potrebbe essere facilmente cancellata.

Accesso in rete tramite proxy 1



Nel caso, invece, che il nostro nodo di elaborazione sia già collegato ad una rete locale, tutta questa parte non ha bisogno di essere effettuata, perché normalmente significa che la nostra macchina è autorizzata a collegarsi a tale rete. In questo caso, spesso, per vari motivi viene istituito un filtro di controllo in uscita, quando i nostri dati devono uscire dalla rete locale e navigare all'interno della rete geografica. Questo normalmente viene fatto con quello che si chiama un PROXY. Questo è lo schema di un PROXY. Supponiamo di avere una rete IP esterna e delle reti IP interne. Noi potremmo avere una rete IP privata, in cui non vogliamo che i nostri utenti escano né che siano raggiunti dalla rete internet, oppure una rete IP interna di tipo controllato, in cui vorremmo sottoporre a controllo le azioni che i nostri utenti fanno.

Accesso in rete tramite proxy 2



In entrambi i casi queste reti non escono, non sono collegate direttamente in internet ma sono collegate tramite un PROXY, il quale svolge varie funzionalità. Ad esempio, è in grado di effettuare dei filtri in base al protocollo, alla porta o all'indirizzo sia del mittente che del destinatario dei pacchetti. Inoltre, nel caso che la linea che collega le nostre reti locali con la rete esterna sia a bassa prestazione, per esempio una linea ISDN a 64Kbit al secondo, per motivi di prestazioni molto spesso il PROXY ha anche funzioni di cache. Una volta che ha trasferito dei dati per conto di un utente, se ne fa anche una copia all'interno di una cache locale (dischi locali). Se per caso lo stesso utente o un altro utente della rete interna richiederà gli stessi dati, lui non andrà più a riprenderseli sulla rete geografica ma li estrarrà dalla cache e li fornirà a chi li ha richiesti, ottimizzando in questo modo anche le prestazioni Quindi un PROXI è un sistema che ha una doppia funzionalità: da una parte può essere utilizzato per migliorare le prestazioni di una rete tramite il meccanismo di caching, dall'altra parte può avere una funzionalità di controllo sugli utenti, sui nodi e sui protocolli che possono collegarsi tra la rete interna e la rete geografica.

Mezzi trasmissivi e cablaggio

Paolo Zaffoni

5.2.2 (Identificare e descrivere i più importanti standard di rete IEEE), 5.4.2 (Descrivere protocolli software per LAN come TCP/IP)

Mezzi trasmissivi

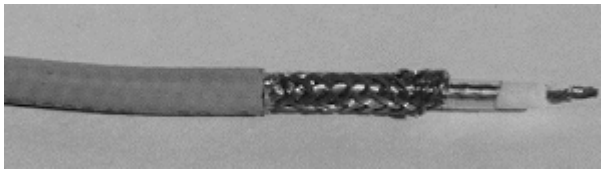
I mezzi fisici tipicamente utilizzati per connettere i calcolatori in una LAN sono:

- mezzo elettrico;
- onde elettromagnetiche;
- mezzo ottico.

In realtà quello utilizzato nella maggior parte dei casi è il mezzo elettrico, nella fattispecie sotto forma di coassiale grosso e sottile, o doppino. Le onde elettromagnetiche sono utilizzate in situazioni particolari, ad esempio per permettere ad un utente di potersi spostare liberamente con il suo elaboratore all'interno della struttura che ospita la **LAN** , senza però perdere o sospendere la sua connessione. I mezzi ottici, ossia fibre ottiche e laser, hanno la proprietà di permettere collegamenti alle velocità di trasferimento più elevate, e di essere relativamente insensibili ai disturbi elettromagnetici. Per questo motivo sono utilizzate per cablare delle parti di **LAN** che sono sottoposte a inquinamento elettromagnetico notevole.

Cavo coassiale

Esistono due tipi di cavo coassiale:



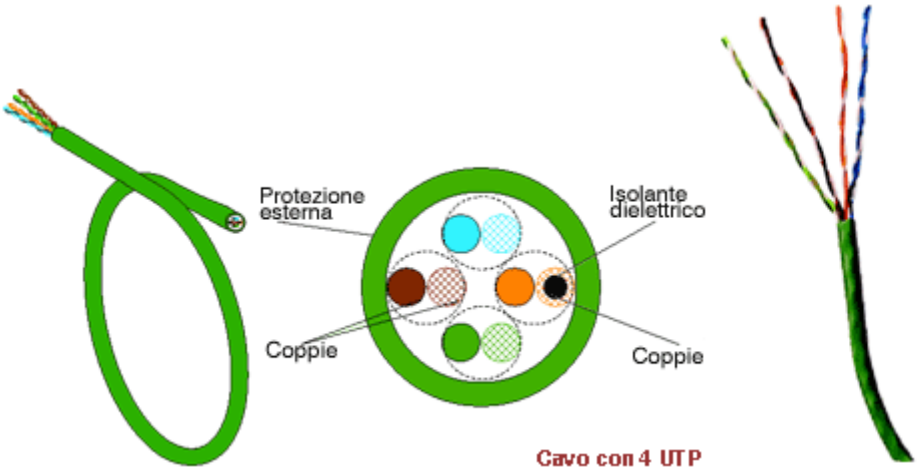
- *cavo coassiale spesso* (*thick ethernet*); è stato il primo mezzo trasmissivo utilizzato. Il segnale trasmesso è di tipo sbilanciato, con la maglia esterna a massa. Le caratteristiche principali sono il costo elevato, la difficoltà di posare il cavo con raggi di curvatura maggiori di 50 centimetri, un buon isolamento dal mondo esterno e dal rumore elettromagnetico, e una bassa attenuazione. Il cavo viene posato senza interruzioni, il collegamento tra il cavo e l'elaboratore è fatto con costosi *transceiver*. Questi si agganciano al cavo, e sono dotati a loro volta di un cavo di lunghezza massima pari a 50 metri che termina collegandosi con l'elaboratore. Un vantaggio di questo mezzo trasmissivo è che l'utente non è in grado di vedere il cavo, perciò è una soluzione affidabile. La lunghezza massima del cavo coassiale è di 500 metri, mentre la distanza minima tra due *transceiver* è di 2.5 metri. Il cavo coassiale spesso è poco usato a causa delle difficoltà di cablaggio.

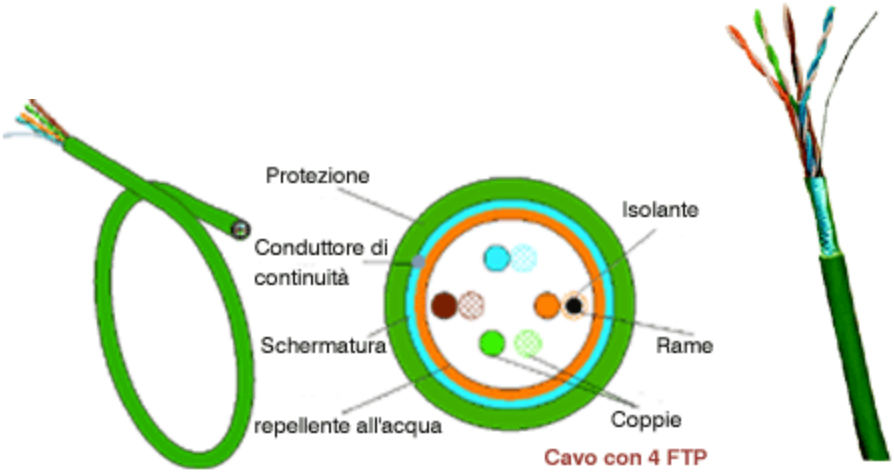
- *cavo coassiale sottile* (*thin ethernet*);

è un cavo coassiale con segnale trasmesso di tipo sbilanciato e maglia esterna a massa. Le sue principali caratteristiche sono flessibilità, quindi facilità di posa, ma un isolamento inferiore al coassiale grosso. I *transceiver* vengono connessi tagliando il cavo e connettendo i due spezzoni con una T, creando una struttura con ponticelli; l'attenuazione è maggiore del *thick ethernet* e comporta una lunghezza massima del cavo pari a circa 200 metri, compresi i cavi di attacco alla macchina, con distanza minima tra le stazioni 0.5 metri. In questo caso invece l'utente può facilmente arrivare ai ponticelli aprendo il circuito e compromettendone il funzionamento, con problemi di affidabilità.

Doppino ritorto

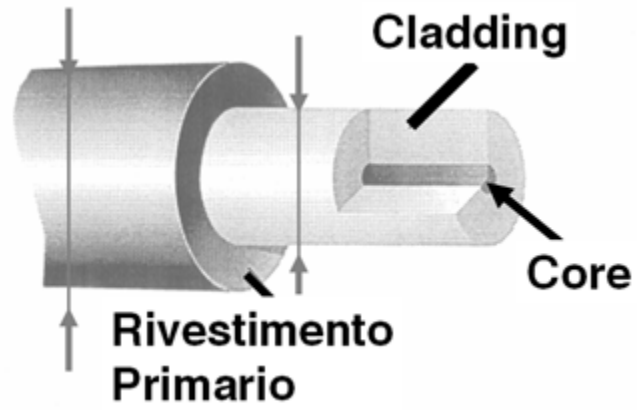
Il doppino viene utilizzato come mezzo trasmissivo in cavi formati da più doppini, chiamati coppie simmetriche. Il segnale in questo caso è trasmesso in maniera bilanciata. Le sue caratteristiche principali sono sia il basso costo che la facilità di posatura; ciò lo rende adatto ai cablaggi strutturati, che hanno avuto enorme diffusione recentemente perchè migliorano i processi di produzione, con migliore difesa dal rumore, migliore qualità dell'isolante, codifiche più efficienti. Necessita di amplificatori che possano lavorare ad alte frequenze e rendere la trasmissione poco sensibile al rumore elettromagnetico. Sono presenti problemi di diafonia tra le coppie di doppini all'interno del cavo, questo problema però può essere risolto con schermature coppia per coppia. Le possibili varianti per il doppino sono: UTP (*Unshielded Twisted Pair*) ossia non schermato, **STP** (*Shielded Twisted Pair*) schermato coppia per coppia, e **FTP** (*Foiled Twisted Pair*), un solo schermo per tutto il cavetto.





Fibra ottica

Le fibre ottiche presentano una notevole insensibilità al rumore elettromagnetico, una mancanza di emissioni, una bassa attenuazione, una banda passante teoricamente illimitata (questo nel caso delle più costose fibre monomodali), un basso costo di produzione, un alto costo per le interfacce e i connettori.



Tuttavia l'utilizzo di fibra ottica è limitato, e i campi di impiego sono caratterizzati da altissime velocità (>150 Mbit/s), lunghe distanze di interconnessione ed infine ambienti con problemi di compatibilità elettromagnetica.

Si distinguono in fibre *monomodali* e fibre *multimodali*. Se la luce ha un solo modo di propagazione allora la fibra è monomodale, se invece ha più modi allora il tempo di arrivo dello stesso raggio luminoso in partenza non è lo stesso, e la fibra è multimodale. Per le **LAN** si usano le fibre multimodali perchè anche se presentano un'attenuazione maggiore, costano meno le interfacce.

La fibra ottica è realizzata in materiale trasparente, tipicamente vetro, ma anche plastica nelle fibre più economiche. La fibra è una struttura a sezione cilindrica, costituita da materiali con diverso indice di rifrazione. La parte più interna del cilindro, detta *core* o nucleo, ha indici di rifrazione maggiore, mentre la parte esterna, detta *cladding* o mantello, ha indice di rifrazione minore. Questa differenza fra gli indici di rifrazione permette di piegare il raggio luminoso mantenendolo all'interno della fibra con minima dispersione di luce verso l'esterno.
L'indice di rifrazione del nucleo può essere costante (fibre a salto d'indice) o variabile con continuità fra il suo valore massimo, verso il centro e il valore di quello del rivestimento verso l'esterno (fibre a indice graduale).

Cablaggi strutturati

Per cablaggio si intende l'insieme di componenti passivi come cavi, prese, connettori, permutatori, eccetera, installati e predisposti per poter interconnettere i componenti attivi dei sistemi di elaborazione. La progettazione razionale di sistemi di cablaggio prende il nome di *cablaggio strutturato*. Le normative sui sistemi di cablaggio definiscono metodi per cablare un gruppo di edifici costruiti su un comprensorio, cioè su un singolo appezzamento di suolo privato o su un insieme di appezzamenti vicini collegati da opere edilizie permanenti, come sovrappassi o sottopassi.

Le normative descrivono :

- le caratteristiche dei mezzi trasmissivi e dei componenti passivi, in relazione alle velocità trasmissive desiderate;
- le topologie di cablaggio ammesse (stella, anello, *bus*, maglia) e le caratteristiche ad esse riferite quali, ad esempio, eventuali livelli di gerarchia, distanze massime, adattamenti tra diverse topologie;
- le regole di installazione e le indicazioni sulla documentazione di progetto.

I sistemi di cablaggio sono sia di tipo proprietario, ad esempio il *Cabling System* IBM o il *DECconnect digital*, che standard internazionali, che di solito sono o americani o della **ISO** .

Standard internazionali

Esistono oggi i seguenti standard per i sistemi di cablaggio:

- EIA/TIA 568: è uno standard americano per il cablaggio di edifici commerciali; è stato approvato nel luglio 1991 ed è attualmente quello più applicato e diffuso in tutto il mondo;
- EIA/TIA 570: è uno standard americano per il cablaggio di edifici residenziali, occupati da una singola famiglia o più occupanti, che possono avere un numero ridotto di uffici commerciali. In questo caso è preponderante l'aspetto della distribuzione delle linee telefoniche esterne;
- ISO/IEC DIS 11801 è una proposta di standard internazionale per i cablaggi di edifici commerciali che è stata votata ed approvata nel luglio 1994. I paesi europei sono particolarmente interessati a questa normativa che viene sempre più richiesta come requisito base per la realizzazione di cablaggi strutturati;
- SP-2840-A è una proposta di revisione dello standard EIA/TIA 568 per far fronte alle esigenze di maggiori velocità trasmissive sui cablaggi;
- prEN 50173 è una proposta di standard europeo che non è ancora stata approvata ed è molto simile ad ISO/IEC DIS 11801.

I cablaggi devono essere certificati con appositi strumenti di misura per garantire determinate prestazioni. Inoltre per poter realizzare correttamente un sistema di cablaggio è necessario che tutte le infrastrutture di tipo meccanico ed edile rispondano a determinati requisiti. Questi aspetti sono trattati dallo standard americano EIA/TIA 569. Infine, lo standard TIA/EIA 607 tratta il problema della realizzazione di un impianto di messa a terra adeguato ad un cablaggio strutturato.

IEEE 802.3

Dott. Paolo Zaffoni

5.2.2 (Identificare e descrivere i più importanti standard di rete IEEE), 5.4.1 (Descrivere le principali funzioni di protocolli hardware per LAN), 5.4.2 (Descrivere protocolli software per LAN come TCP/IP)

Introduzione

Lo standard IEEE 802.3 si richiama alla rete locale ***Ethernet*** , originalmente sviluppata da *Xerox*. Lo standard IEEE 802.3 definisce sia le specifiche del livello **MAC** sia quelle del livello fisico. In questa sezione approfondiremo lo

studio del livello MAC per tale standard. Il protocollo MAC per IEEE 802.3 è di tipo ***Carrier Sense Multiple Access with Collision Detection*** (**CSMA/CD**).

MAC Protocol - 802.3

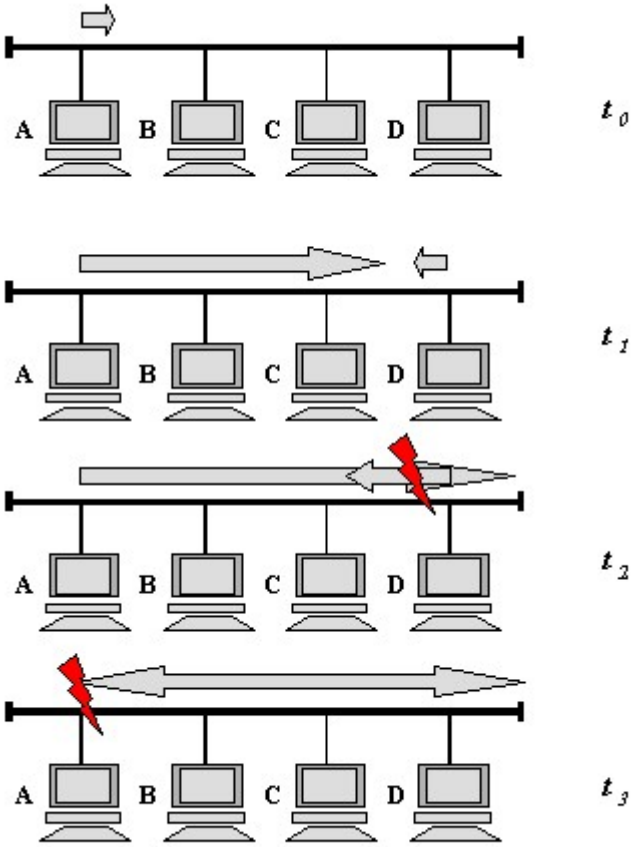
Con il protocollo **CSMA/CD** , la **stazione** che desidera trasmettere, si pone prima di tutto in ascolto sul mezzo trasmissivo al fine di verificare se è già in corso un'altra operazione di trasmissione (*carrier sensing*). Se il mezzo trasmissivo si trova in uno stato di *idle*, ossia non è al momento interessato da una trasmissione, la stazione può trasmettere. Se il segnale elettromagnetico si propagasse in modo istantaneo a tutte le altre stazioni della rete, questo meccanismo garantirebbe l'assenza di collisioni. Purtroppo questo non è vero, poiché il segnale trasmesso da una stazione impiega un tempo non nullo a raggiungere le altre. Sia T il tempo di propagazione del segnale fra due stazioni qualunque A e B. Se A inizia a trasmettere all'istante t0, qualora B inizi anch'essa a trasmettere fra t0-T e t0+T (intervallo di durata 2T) non è assicurata l'assenza di collisione. Si chiama intervallo di vulnerabilità il doppio del tempo di propagazione fra le due stazioni più distanti sul *bus*, corrispondente al caso peggiore dell'esempio precedente. Può quindi accadere che due stazioni effettuino il *carrier sensing* all'interno di un intervallo di vulnerabilità e facciano entrambi partire una trasmissione. In tal caso, si verificherà una **collisione** e di conseguenza i dati verranno alterati da tale evento e non potranno essere ricevuti correttamente.

La procedura di accesso può essere descritta in modo dettagliato attraverso una sequenza di passi fondamentali, come segue:

- Se il mezzo trasmissivo si trova in uno stato di *idle*, è lecito trasmettere; in caso contrario si vada al passo 2.
- Se il mezzo trasmissivo è occupato, porsi in ascolto dello stesso fino a che sul **canale** non viene ripristinato lo stato di *idle*. Rilevato tale stato, trasmettere immediatamente.
- Se viene rilevato un evento di collisione durante la trasmissione, si trasmette un particolare segnale denominato *jamming*, in modo tale che tutte le stazioni vengano messe a conoscenza dell'avvenuta collisione e cessino conseguentemente la loro trasmissione.
- Dopo aver trasmesso il segnale di *jamming* è necessario attendere un intervallo di tempo di durata casuale dopo il quale è possibile ritentare la trasmissione. (si torna al passo 1)

Esempio

La figura sottostante descrive il funzionamento di questa tecnica applicata su di un ***bus*** in **banda** base, prendendo come esempio il caso peggiore in cui le due stazioni che trasmettono sono quelle con la maggiore distanza reciproca.



All'istante t0, la **stazione** A inizia a trasmettere dei dati indirizzati alla stazione D e, all'istante t1, la stessa stazione D inizia una propria trasmissione, dato che il fronte iniziale della trasmissione di A non è ancora arrivato. Ovviamente all'istante t1, anche B e C sarebbero pronte a trasmettere, ma entrambe eseguendo il *carrier sensing* si accorgono che il mezzo è occupato da un'altra trasmissione e rimandano la propria. All'istante t2 la trasmissione di A arriva alla stazione D la quale rileva la **collisione** e cessa immediatamente la propria trasmissione. L'effetto della collisione si propaga su tutto il *bus* giungendo fino alla stazione A, dove viene rilevato solamente nell'istante t3.

Specifiche del protocollo CSMA/CD

Utilizzando il protocollo **CSMA/CD** , l'ammontare di **banda** sprecata si riduce al tempo necessario per rilevare la **collisione** . Se si fa riferimento all'esempio appena descritto, relativo ad un ***bus*** in banda base ed alla coppia di stazioni più distanti, si può affermare che il tempo necessario a rilevare una collisione non è mai superiore al doppio del ritardo di propagazione più lungo.

Tipicamente in molti sistemi CSMA/CD, incluso IEEE 802.3, si impone che le trame siano sufficientemente lunghe da consentire di rilevare la collisione prima della fine della loro trasmissione.

La durata del ritardo introdotto nel punto 4 della procedura viene determinata con una tecnica denominata *binary exponential backoff* (*attesa esponenziale binaria*). Si supponga che a causa di ripetute collisioni, ogni **stazione** tenti di trasmettere ripetutamente. Al verificarsi di ogni evento di collisione il valor medio del ritardo viene raddoppiato e, dopo 16 tentativi falliti, la stazione rinuncia a trasmettere e riporta un errore. Tale tecnica consente alle stazioni di ritardare sempre più la **ritrasmissione** quando la congestione aumenta, riducendo così la probabilità di collisione.

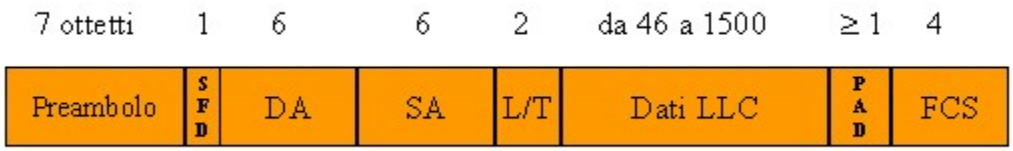
In presenza di un *bus* in banda basa l'evento di collisione produce delle oscillazione di tensione che sono tipicamente più alte di quelle prodotto da una normale trasmissione. Lo standard **IEEE** stabilisce dunque che si è in presenza di

una collisione quando il livello di tensione nel punto di contatto del trasmettitore col cavo è superiore al massimo che si potrebbe raggiungere i presenza di un singolo trasmettitore. Il problema che potrebbe verificarsi utilizzando questa tecnica è legato al fatto che in presenza di due stazioni trasmittenti fisicamente lontane, la potenza di segnale potrebbe attenuarsi ad un punto tale che i due segnali combinati potrebbero non superare la soglia di rilevazione della collisione. Per questa ragione e per limitare l'intervallo di vulnerabilità lo standard deve impone dei limiti ben precisi alle dimensioni della rete.

La trama MAC

La figura sottostante rappresenta il formato della **trama** del protocollo IEEE 802.3. Esso è caratterizzato dai seguenti campi:

- **Preambolo** : è costituito da una sequenza di 0 ed 1 alternati lunga 7 ottetti, usata dal ricevitore per stabilire la sincronizzazione di bit.
- ***Start Frame Delimiter*** **(SFD - delimitatore di inizio trama)**: è rappresentato dalla sequenza 10101011, che indica il reale inizio della trama e consente al ricevitore di localizzare il primo bit di inizio trama.
- ***Destination Address*** **(DA - indirizzo di destinazione)**: indica la **stazione** /i alla quale è indirizzata la trama. Può essere un unico indirizzo fisico, un indirizzo di gruppo oppure uno globale.
- ***Source Address*** **(SA - indirizzo di provenienza)**: specifica la stazione che ha inviato la trama.
- ***Length/Type***: indica la lunghezza del campo dati in ottetti o campo *Type* in ***Ethernet*** , a seconda che la trama sia relativa allo standard IEEE 802.3 o alle specifiche *Ethernet*. In entrambi i casi la dimensione massima della trama, se si esclude il preambolo e l'SFD è di 1518 ottetti.
- **Dati LLC**: unità dati fornita dal **LLC** .
- **PAD**: ottetti aggiuntivi per garantire una sufficiente lunghezza della trama al fine di rilevare la collisione.
- ***Frame Check Sequence*** **(FCS - sequenza di verifica di correttezza della trama)**: rappresenta un codice a controllo ciclico a 32 bit, calcolato su tutti i campi eccetto il preambolo, l'SFD e il FCS stesso.



Strato fisico dell'802.3: mezzi trasmessivi

Il protocollo IEEE 802.3 e le sue evoluzioni utilizzano diversi tipi di mezzi trasmessivi, specificati nella parte di strato fisico dello standard:

- ***Thick ethernet*** - Descritto nello standard **10Base5** , storicamente è stato il primo mezzo trasmissivo utilizzato da ***Ethernet*** per realizzare il ***bus*** condiviso. Consiste in un **cavo coassiale** spesso, la cui lunghezza massima è di 500 metri. La velocità di trasmissione è di 10 Mb/s e su uno stesso segmento (*bus*) possono essere installate fino a 100 macchine. Ogni **stazione** contiene un'interfaccia di rete (detta anche scheda *ethernet*), a cui viene collegata una estremità di un cavo lungo pochi metri, detto *transceiver drop cable*; all'altra estremità del cavo è connesso un ***transceiver*** che si aggancia, con una presa detta *a vampiro*, al cavo coassiale spesso, che di conseguenza non viene mai interrotto. In questa implementazione è il *transceiver* che contiene la circuiteria analogica per l'ascolto del **canale** e la rilevazione delle collisioni.
- ***Thin ethernet*** - Descritto nello standard **10Base2** , si tratta di un cavo coassiale sottile, più robusto del coassiale spesso e quindi più maneggevole e facile da piegare. Le sue caratteristiche sono velocità di trasferimento di 10 Mb/s, 200 metri di lunghezza massima per un singolo segmento e al più 30 macchine installate su un segmento. Di norma l'interfaccia di rete installata sulla macchina contiene anche il *transceiver*, mentre l'allaccio di una stazione alla rete avviene con una giunzione a T, alla quale sono collegati il cavo che

porta alla stazione e due cavi thin, che costituiscono una porzione del segmento. Le varie stazioni sono collegate in cascata sul segmento.

- ***Twisted Pair*** - È il tradizionale **doppino** di rame intrecciato, utilizzato anche nella rete telefonica. Ne esistono diverse categorie, con cavi schermati o meno, e viene utilizzato per realizzare i collegamenti punto-punto tra stazioni e **hub** nella topologia a stella. Lo standard **10BaseT** prevede una lunghezza massima di 100 metri e una velocità di 10 Mb/s. Nel caso della *Fast Ethernet* e della *Gigabit Ethernet*, invece, si utilizzano il **100BaseTX** e il **1000BaseTX**, che funzionano a 100 Mb/s e 1Gb/s rispettivamente.
- **Fibra Ottica** - È un mezzo a **banda** molto larga e bassa **attenuazione** , che permette quindi velocità elevate e lunghe distanze di collegamento. Nelle reti locali di tipo *Fast Ethernet* e *Gigabit Ethernet*, si utilizzano gli standard **100BaseF** e **1000BaseF** rispettivamente, che prevedono una lunghezza massima di 2000 metri, rendendo adatte le fibre al collegamento di edifici.

IEEE 802.5

Dott. Paolo Zaffoni

5.2.2 (Identificare e descrivere i più importanti standard di rete IEEE), 5.4.1 (Descrivere le principali funzioni di protocolli hardware per LAN), 5.4.2 (Descrivere protocolli software per LAN come TCP/IP)

Introduzione

Il ***Token Ring*** , definito nello standard IEEE 802.5, si utilizza per la gestione dell'accesso al mezzo in una rete caratterizzata da una topologia ad anello.

L'elemento fondamentale del protocollo *Token Ring* è rappresentato da una particolare **trama** , il ***token*** (gettone). Si tratta di una trama di dimensioni ridotte di cui le **stazioni** presenti sull'anello si devono impossessare per acquisire il diritto di trasmettere. Se tutte le stazioni si trovano in uno stato di inattività il *token* circola liberamente lungo l'anello; nel momento in cui una stazione si impossessa del *token* ed inizia la propria trasmissione, sull'anello non sarà presente nessuna altra trama di *token*, costringendo le altre stazioni ad attendere per poter trasmettere a loro volta.

La stazione che acquisisce il *token* opera su di esso un'operazione di trasformazione modificando un bit e convertendolo di fatto in una sequenza di inizio di una trama dati, che è ovviamente seguita dai dati che la stazione desidera trasmettere.

Il *token*, una volta utilizzato, va rilasciato. Questo può essere fatto:

- dalla stazione trasmittente (modalità diffusiva);
- dalla stazione ricevente (modalità parzialmente diffusiva).

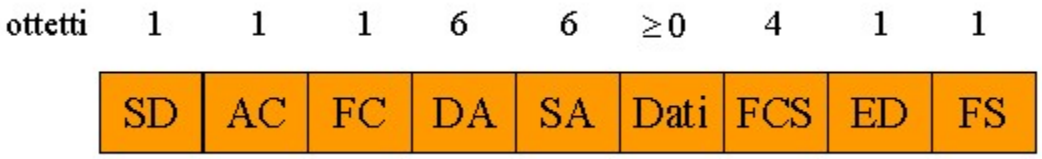
La modalità diffusiva risulta meno efficiente (la trama deve effettuare un intero giro dell'anello prima che sia rilasciato il *token*), ma garantisce la sequenzialità della ricezione del *token*. La soluzione parzialmente diffusiva risulta più efficiente, in quanto la trama deve percorrere solamente una parte dell'anello prima che sia rilasciato nuovamente il *token*, ma non mantiene la sequenzialità della ricezione del *token* e può quindi dare vita a fenomeni di non equità. Inoltre la modalità diffusiva ha il vantaggio di permettere automaticamente la verifica della correttezza della trasmissione in quanto, se la trama ritorna correttamente alla stazione trasmittente sarà sicuramente stata ricevuta anche dalla stazione ricevente. Il protocollo IEEE 802.5 utilizza la modalità diffusiva.

Il protocollo *Token Ring* realizza una gestione equa dell'accesso al mezzo condiviso. Lo svantaggio principale di questo **protocollo** si concretizza nella necessità di gestire la trama *token*: la perdita o un'eventuale duplicazione del *token* rende di fatto inutilizzabile l'anello. A questo scopo è prevista una stazione detta monitor che controllo il normale flusso del *token* e, in presenza di malfunzionamenti, interviene per ripristinarlo.

La trama MAC

La figura sottostante rappresenta il formato della **trama** del protocollo IEEE 802.5. Esso è caratterizzato dai seguenti campi:

- ***Starting Delimiter*** **(SD - delimitatore di inizio trama)**: indica l'inizio della trama ed è caratterizzato dalla seguente sequenza distinguibile dai dati: JK0JK00.
- ***Access Control*** **(AC - controllo d'accesso)**: ha il formato PPPTMRRR, dove **PPP** e RRR indicano la priorità e la prenotazione a 3 bit; M è il bit di monitoraggio, T indica se si tratta di una trama dati o di un ***token*** . In quest'ultimo caso si ha solo un campo successivo che l'ED.
- ***Frame Control*** **(FC - controllo di trama)**: indica se si tratta di una trama dati **LLC** ; in caso contrario i bit di FC controllano le funzioni **MAC** del ***Token Ring*** .
- ***Destination Address*** **(DA - indirizzo di destinazione)**: indica la **stazione** /i alla quale è indirizzata la trama. Può essere un unico **indirizzo** fisico, un indirizzo di gruppo oppure uno globale.
- ***Source Address*** **(SA - indirizzo di provenienza)**: specifica la stazione che ha inviato la trama.
- **Dati LLC**: unità dati fornita dal **LLC**
- ***End Delimiter*** **(ED - delimitatore di fine trama)**: contiene un bit di errore rilevato (E), posto ad 1 in presenza di errore ed un bit intermedio (I) per indicare se ritratta di una trama intermedia durante la trasmissione di più trame.
- ***Frame Check Sequence*** **(FCS - sequenza di verifica di correttezza della trama)**: rappresenta un codice a controllo ciclico a 32 bit, calcolato su tutti i campi eccetto il **preambolo** , l'SFD e il FCS stesso.
- ***Frame Status*** **(FS - stato della trama)**: contiene il bit di indirizzo riconosciuto e di trame copiata (rispettivamente A e C). Tali bit sono al di fuori della parte coperta dal FCS, quindi possono essere duplicati per fornire ridondanza e rilevare gli errori. La configurazione dei bit A e C permette alla stazione che trasmesso di verificare il risultato della propria trasmissione che si concretizza in tre possibili situazioni:
  - La stazione di destinazione non esiste o non è attiva.
  - La stazione di destinazione esiste, ma la trama non è stata ricevuta: A=0; C=1.
  - La trama è stata ricevuta: A=1; C=1.



Meccanismo di priorità nel Token Ring

Il protocollo ***Token Ring*** definisce un meccanismo opzionale per la gestione delle priorità. I livelli di priorità sono definiti attraverso 3 bit e sono quindi otto. L'algoritmo di gestione delle priorità può essere descritto nel modo seguente. Se una **stazione** desidera trasmettere una **trama** a priorità più alta della trama attuale, può prenotare il ***token*** successivo modificando, mentre la trama sta passando, i bit di priorità al livello che desidera imporre. Questi bit vengono copiati nel *token* successivo che quindi conterrà i bit di priorità al livello più elevato fra quelli prenotati. Le stazioni caratterizzate da un livello inferiore di priorità non possono impossessarsi di tale *token* che viene invece acquisito dalla stazione che ha richiesto la maggiore priorità.

Se una stazione aggiorna il livello di priorità, innalzandolo, ha il dovere di abbassarlo al livello precedente quando tutte le stazioni con priorità alta hanno terminato la trasmissione. In effetti, se tale stazione, dopo aver trasmesso, rileva un *token* con priorità pari a quella da lei utilizzata, significa che non è più presente traffico con priorità alta che deve essere trasmesso ed abbassa conseguentemente il livello del *token* prima di ritrasmetterlo.

Emissione anticipata del token

L'emissione anticipata del ***token*** è una specifica evolutiva che è stata aggiunta allo standard 802.5 che consente un utilizzo più efficiente dell'anello. Tale procedura è denominata ***Early Token Release*** (**ETR**) e permette ad una **stazione** trasmittente di emettere un *token* non appena si è conclusa la propria trasmissione, senza attendere necessariamente che l'intestazione della **trama** trasmessa sia ritornata alla stazione stessa. Il *token* emesso prima della ricezione dell'intestazione sarà caratterizzato da un livello di priorità identico a quello dell'ultima trama ricevuta.

L'immediata conseguenza dell'implementazione di tale procedura è che il ritardo di accesso per il traffico ad elevata priorità può subire un incremento in condizioni di carico elevato caratterizzato da trame brevi. Le stazioni che sfruttano la procedura ETR e quelle che non la usano sono ovviamente compatibili e interoperabili fra loro.

Il livello fisico IEEE 802.5: specifiche

Tasso di trasmissione (Mbps)	Mezzo trasmissivo	Tecnica trasmissiva	Dimensione della trama (ottetti)	Controllo d'accesso
4	UTP o STP o fibra	*Manchester* Differenziale	4550	TP o DTR
16	UTP o STP o fibra	*Manchester* Differenziale	18200	TP o DTR
100	UTP o STP o fibra	MLT-3 o 4B5B/NRZI	18200	TP o DTR

- **UTP** : doppino non schermato;
- **STP** : doppino schermato;
- **TP**: controllo d'accesso a passaggio di ***token*** ;
- DTR: ***Token Ring*** dedicato

IEEE 802.11

Dott. Paolo Zaffoni

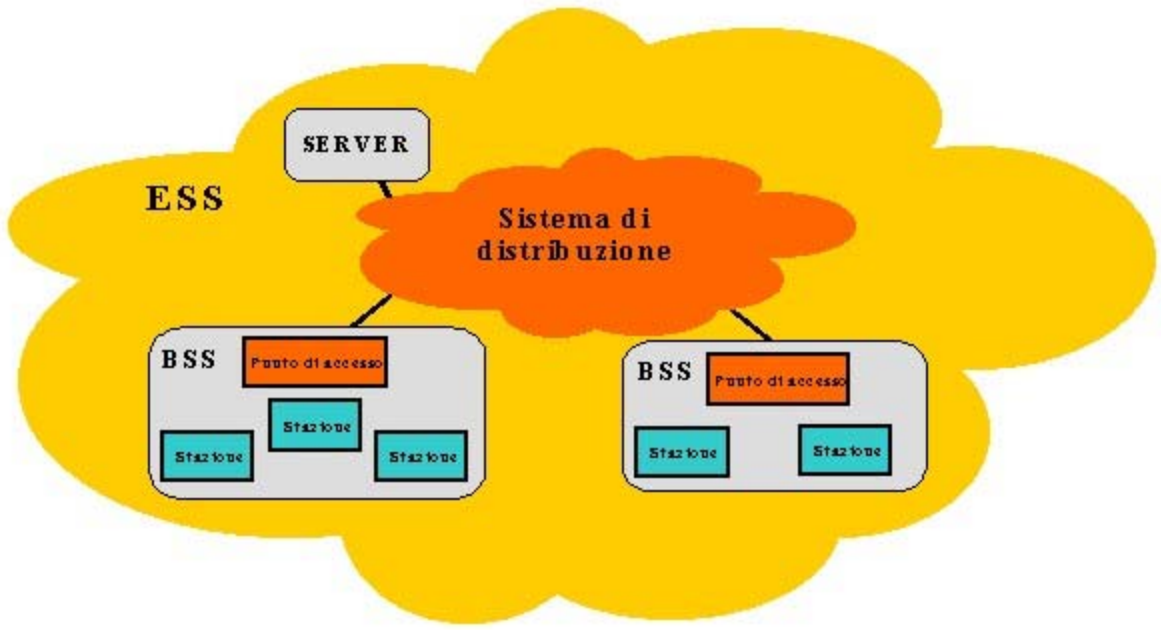
5.2.2 (Identificare e descrivere i più importanti standard di rete IEEE), 5.4.1 (Descrivere le principali funzioni di protocolli hardware per LAN), 5.4.2 (Descrivere protocolli software per LAN come TCP/IP)

Introduzione

Lo standard IEEE 802.11 contiene le specifiche per le **LAN** senza fili. Le terminologie introdotte, unitamente ad alcune caratteristiche specifiche, sono proprie dello standard e non si estendono a tutti i prodotti commerciali. In ogni caso, è di fondamentale importanza la conoscenza di tale standard in quanto esso detta le specifiche fondamentali richieste ad una *wireless* LAN.

L'architettura del modello IEEE 802.11 è rappresentabile come nella figura che segue. L'elemento fondamentale di una *wireless* LAN è costituito dal *Basic Service Set* (BSS) che caratterizza l'insieme dei servizi di base e che corrisponde ad una cella. Esso consiste in diverse stazioni che utilizzano lo stesso protocollo **MAC** per effettuare a procedura di accesso al mezzo condiviso. Il protocollo MAC può essere completamente distribuito oppure effettuare la gestione dell'accesso in modo centralizzato. Il BSS può essere isolato oppure connesso ad un sistema dorsale di distribuzione attraverso un punto di accesso che opera da ***bridge*** .

L'insieme dei servizi estesi, *Extended Service Set* (ESS) è costituito da due o più BSS interconnessi tipicamente attraverso una LAN cablata ed è configurato in modo analogo ad una LAN logica a livello **LLC** .



Lo standard IEEE 802.11 prevede l'esistenza di tre tipologie di stazioni che si differenziano sulla base delle loro caratteristiche di mobilità:

- **Nessuna transizione**: si tratta di stazioni caratterizzate da assenza di mobilità oppure che si muovono solo all'interno dell'area di comunicazione diretta associata ad un singolo BSS.
- **Transizione BSS**: sono stazioni che hanno la possibilità di spostarsi fra diversi BSS interni ad uno stesso ESS. Si rende necessaria la presenza di uno schema di indirizzamento che permette di stabilire la nuova posizione della **stazione** .
- **Transizione ESS**: questo tipo di stazioni hanno la possibilità di muoversi fra BSS appartenenti ad ESS diversi. La gestione delle connessioni a livelli più alti è supportata dall'IEEE 802.11 ma non può essere garantita dato che esiste una probabilità non trascurabile di interruzione del servizio.

Il livello fisico IEEE 802.11: specifiche

Gli schemi di trasmissione previsti dal modello IEE 802.11 sono attualmente tre:

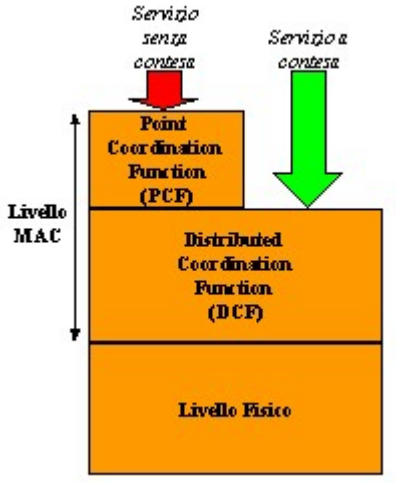
- **Infrarosso**: prevede una trasmissione a 1 Mbps ed a 2 Mbps su una lunghezza d'onda tra gli 850 ed i 950 nm.
- ***Spread Spectrum Direct Sequence***: opera nella **banda** ISM a 2,4 GHz e sfrutta 7 canali ognuno caratterizzato da una frequenza di trasmissione dati di 1 Mbps o 2Mbps.
- ***Spread Spectrum Frequency Hoppimg***: opera nella banda ISM a 2,4 GHz, con una frequenza di trasmissione dati di 1 Mbps o 2Mbps.

Il protocollo MAC 802.11

Per la definizione delle problematiche di accesso al mezzo il gruppo di lavoro 802.11 ha studiato due soluzioni possibili. La prima basata su un meccanismo di controllo dell'accesso di tipo distribuito, similare al CSMA, il quale comunica alle stazioni la possibilità di trasmettere attraverso un sistema di rilevazione della portante e la seconda basata su di 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 si applica tipicamente quando le stazioni *wireless* sono interconnesse fra loro da una **stazione** base, a sua volta collegata ad una **LAN** di dorsale cablata.

Lo studio effettuato dal gruppo di lavoro IEEE 802.11 sulle problematiche di gestione dell'accesso ha portato alla definizione di una algoritmo **MAC** denominato *DFWMAC, Distributed Foundation Wireless MAC*. Tale algoritmo permette un meccanismo di controllo dell'accesso di tipo distribuito sul quale è implementato un controllo centralizzato a carattere opzionale. L'architettura può essere schematizzata come nella figura seguente.



Il livello MAC è caratterizzato da un primo strato più basso che offre la funzione di coordinamento distribuita (***Distribution Coordination Function* - DCF**) che si basa sull'utilizzo di un algoritmo a contesa. Il traffico asincrono ordinario sfrutta direttamente la DCF. La funzione di coordinamento del punto di accesso (***Point Coordination Function, PCF***) è un algoritmo MAC centralizzato che fornisce un servizio senza contesa. La PCF opera al di sopra della DCF e ne sfrutta le caratteristiche per assicurare un accesso privilegiato ai suoi utenti.

Distribution Coordination Function - DCF

La funzione di coordinamento distribuita si basa sull'uso di un semplice algoritmo CSMA. Quando una **stazione** deve trasmettere si pone in ascolto sul mezzo. La trasmissione è possibile solo se il mezzo è libero altrimenti si deve aspettare fino a che la trasmissione in corso si è conclusa.

Il DCF non prevede una procedura di rilevazione della **collisione** dato che in un contesto *wireless* tale funzione non può essere gestita in modo semplice. Infatti, risulta estremamente difficile per una stazione trasmittente distinguere fra segnale trasmesso, deboli segnali in arrivo e rumore.

Il corretto funzionamento di questo algoritmo si basa sulla definizione di uno schema di priorità, implementato introducendo una serie di ritardi. Il singolo ritardo è definito *InterFrame Space*, IFS. In presenza di un singolo ritardo (sono possibili fino a tre diversi ritardi) l'accesso segue le seguenti regole:

- La stazione che deve trasmettere ascolta il mezzo. Se il mezzo è libero la stazione verifica che lo rimanga per un tempo pari ad IFS. Se tale condizione è soddisfatta la stazione può trasmettere.
- Se il mezzo è occupato la stazione attende fino a che termina la trasmissione corrente.
- Quando la stazione a finito di trasmettere, la stazione ritarda di una altro IFS. Se il mezzo rimane libero per questo intervallo di tempo la stazione attende utilizzando uno schema di tipo *binary exponential backoff*. Se il mezzo è ancora libero dopo tale attesa la stazione può trasmettere.

Per introdurre uno schema di priorità si introducono tre diversi valori di IFS:

- **SIFS (*Short IFS*)**: usato per le azioni a risposta immediata. Si sfrutta come tempo da attendere prima di inviare un riscontro, quando la stazione trasmittente emette una **trama** del tipo *Request to Send* e si pone in attesa di una trama *Clear to Send*, nel caso di risposta ad un interrogazione.
- **PIFS (*Point Coordination Function IFS*)**: IFS di valore intermedio usato dal *controller* centralizzato nello schema PCF per la gestione dei permessi di trasmissione.
- **DIFS (*Distribution Coordination Function*)**: IFS di valore più elevato che viene usato nella funzione di coordinamento distribuito come ritardo minimo fra le trasmissioni asincrone.

Point Coordination Function - PCF

Le azioni svolte in tale punto funzionale consistono in un interrogazione effettuata dal controllore centrale, coordinatore dell'accesso. Tale **stazione** utilizza il PIFS per gestire le interrogazioni. Essendo il PIFS più corto del DIFS, tale stazione ha la possibilità di controllare il mezzo e bloccare il traffico asincrono quando invia le interrogazioni e si pone in attesa delle risposte.

Infine, per evitare che la stazione di coordinamento blocchi tutto il traffico asincrono emettendo ripetute interrogazioni viene introdotto un intervallo temporale denominato *supertrama*. Nella prima parte di tale intervallo la stazione di coordinamento emette interrogazioni in modo sequenziale, lasciando libero il resto dell'intervallo e permettendo la procedura di contesa per l'accesso asincrono.

Protocollo IP e collegati

Paolo Zaffoni

5.2.1 (Elencare e definire gli strati dei protocolli di rete TCP/IP e OSI), 5.4.1 (Descrivere le principali funzioni di protocolli hardware per LAN), 5.4.2 (Descrivere protocolli software per LAN come TCP/IP)

Introduzione

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* 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.

La comunicazione in Internet avviene nel seguente modo: il livello di trasporto gestisce le informazioni in forma di *data stream* che vengono frammentati in datagrammi a livello di rete. Risulta quindi fondamentale comprendere la modalità con cui viene costruito un pacchetto IP.

Tale sezione presenta i seguenti argomenti all'interno del capitolo relativo al pacchetti IP:

- **formato del pacchetto IP** ;
- **problemi di indirizzamento** ;
- **classi di indirizzi A, B, C, D** ;
- ***netmask* e valori possibili** ;
- **indirizzi privati e indirizzi pubblici** ;
- ***logical IP subnet*** .

La sicurezza delle connessioni ad Internet sta divenendo sempre più importante, in questa sezione vengono illustrate le principali tecniche che consentono di avere un accesso sicuro alla rete. Come noto, la *suite* di protocolli TCP/IP è in realtà un insieme abbastanza complesso di molteplici protocolli. Nella parte finale di questa sezione vengono

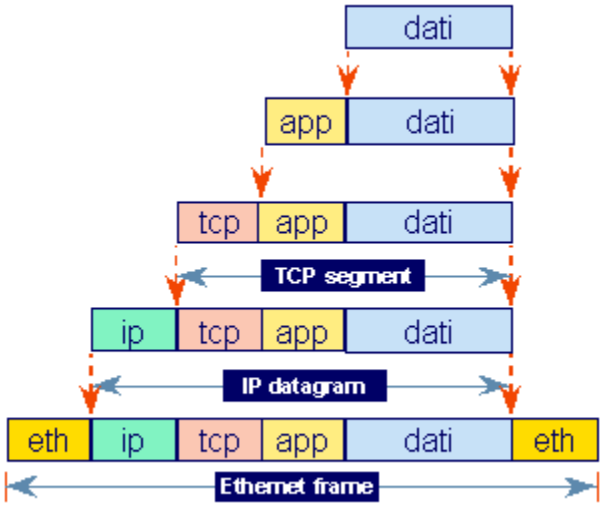
presentati alcuni protocolli, che insieme a più noti protocolli TCP e IP, giocano un ruolo fondamentale all'interno della rete Internet (per esempio i protocolli NAT e PAT, i quali tra l'altro consentono di risolvere il problema della carenza di indirizzi pubblici).

La sezione relativa alle soluzioni e ai protocolli correlati contiene le seguenti sezioni:

- **protocolli correlati a IP e loro impiego** ;
- **ICMP** ;
- **ARP/RARP** .

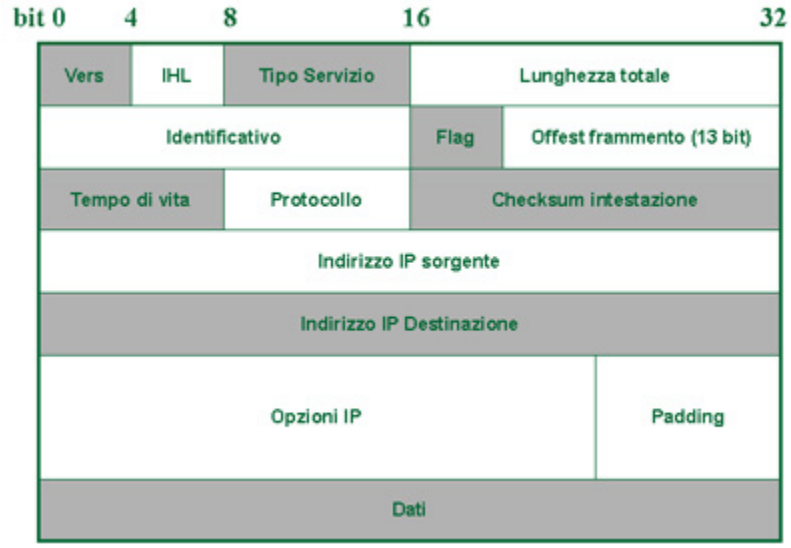
Formato del pacchetto IP

Il protocollo IP



Quando un'applicazione invia dei dati, utilizzando l'architettura **TCP** / **IP** , i dati vengono mandati verso il basso attraverso tutti i livelli della pila protocollare fino ad essere trasmessi dal livello fisico. Ogni livello aggiunge delle informazioni di controllo, preponendo degli ***header*** (ed a volte aggiungendo anche dei *trailer*) ai dati che riceve. I dati d'utente, ai quali viene preposta un'intestazione (*header*) dallo strato di applicazione, vengono passati al protocollo dello strato di trasporto (in questo caso si tratta del protocollo TCP, sebbene il funzionamento sia del tutto analogo nel caso si utilizzi **UDP**): quest'ultimo esegue varie operazioni e aggiunge un'intestazione alla **PDU** che gli è stata inviata. L'unità di dati prende ora il nome di segmento. Lo strato di trasporto fornisce quindi il segmento allo strato di rete, che presta anch'esso servizi specifici e aggiunge un'intestazione. Questa unità (che la terminologia di Internet definisce ora **datagramma**) viene passata ai livelli inferiori, dove lo strato di collegamento dati aggiunge la propria intestazione e una coda (*trailer*); l'unità di dati (che ora prende il nome di trama) viene poi trasmessa in rete dallo strato fisico. In figura è mostrato un esempio di imbustamento dei dati, nell'ipotesi che la sottorete sia una LAN di tipo *Ethernet*.

Il pacchetto IP



Il protocollo IP fornisce i seguenti servizi:

- trasmissione di un ***datagram*** *host-to-host* (indirizzamento);
- funzioni di ***routing*** ;
- frammentazione e riassemblaggio dei *datagram*.

Il protocollo non fornisce:

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

I *router* in rete elaborano il pacchetto fino a livello IP, per vedere quale sia l'indirizzo di destinazione; attraverso la tabella di instradamento viene deciso su quale interfaccia inviare il pacchetto. IP supporta le operazioni di frammentazione: il termine di frammentazione indica un'operazione in cui una PDU 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, un *router* sarebbe incaricato di gestire le incompatibilità tra le dimensioni delle PDU delle diverse reti. IP risolve il problema fissando regole di frammentazione per i *router* e regole di riassemblaggio nell'*host* ricevente.

I campi del pacchetto IP

Il campo versione identifica la versione del protocollo IP del pacchetto; quella oggi in uso prevalente è IPv4, sebbene ci si stia indirizzando verso l'uso della versione IPv6 (denominata anche IPng, IP *next generation*).

Il campo lunghezza dell'intestazione (IHL) contiene 4 bit impostati a un valore che indica la lunghezza dell'intestazione dei datagrammi. La lunghezza è misurata in parole di 32 bit; solitamente, un'intestazione senza opzioni di qualità del servizio (QoS) è costituita da 20 *byte* (quindi 20 * 8 = 160 bit, ovvero 5 raggruppamenti da 32); di conseguenza il valore del campo della lunghezza è di norma 5.

Il campo tipo di servizio (TOS) può essere utilizzato per classificare i pacchetti e offrire un servizio differenziato (QoS).

Il campo lunghezza totale specifica la lunghezza totale del datagramma IP. Si misura in *byte* e comprende la lunghezza dell'intestazione e dei dati. IP sottrae il campo lunghezza dell'intestazione dal campo lunghezza totale, per calcolare le dimensioni del campo dati. La lunghezza massima possibile per un datagramma è di 65.535 *byte*.

Il protocollo IP utilizza tre campi nell'intestazione per controllare la frammentazione e il riassemblaggio dei datagrammi. Questi sono il campo identificatore, *flag* e scostamento del frammento.

Il campo identificatore serve all'*host* ricevente per designare in modo univoco ciascun frammento di un datagramma proveniente dall'indirizzo di origine.

Il campo *flag* contiene i bit che determinano se il datagramma può essere frammentato: in caso affermativo, uno dei bit può essere impostato in modo tale da determinare se il frammento è l'ultimo del datagramma.

Il campo scostamento del frammento contiene un valore che specifica la posizione relativa del frammento nel datagramma originale; il valore si misura in unità di otto *byte*.

Il parametro tempo di durata (TTL, *Time To Live*) serve per misurare il tempo di presenza di un datagramma in rete. Ogni *router* quando riceve un pacchetto controlla questo campo, e lo scarta se il valore TTL è uguale a zero; prima di inoltrare nuovamente il pacchetto, il campo TTL viene diminuito di una unità. Il campo TTL indica quindi il numero di tratti che il pacchetto può attraversare, e può essere usato dai *router* per evitare che i pacchetti entrino in cicli infiniti, ma anche da un *host* per limitare la durata della presenza di segmenti in rete.

Il campo protocollo serve per identificare il protocollo dello strato immediatamente superiore a IP che deve ricevere il datagramma. È simile al campo tipo, presente nella trama ***Ethernet*** .

Il campo *checksum* dell'intestazione viene utilizzato per rilevare eventuali errori che possono essersi verificati nella sola intestazione. I controlli non vengono eseguiti sul flusso dei dati dell'utente. Se da un lato ciò consente di usare un algoritmo di *checksum* piuttosto semplice, in quanto non deve operare su molti *byte*, dall'altro richiede che un protocollo di livello superiore esegua un controllo degli errori sui dati dell'utente.

IP trasporta due indirizzi nel datagramma: l'indirizzo di origine e l'indirizzo di destinazione, che conservano lo stesso valore per tutto il trasferimento.

Il campo opzioni serve per identificare vari servizi supplementari.

Il campo riempimento può essere utilizzato per far sì che l'intestazione del datagramma sia allineata ad una delimitazione precisa di 32 bit.

Infine il campo dati contiene i dati dell'utente. La combinazione dei dati e dell'intestazione non può superare 65.535 *byte*.

Problemi di indirizzamento

Formato dell'indirizzo IP

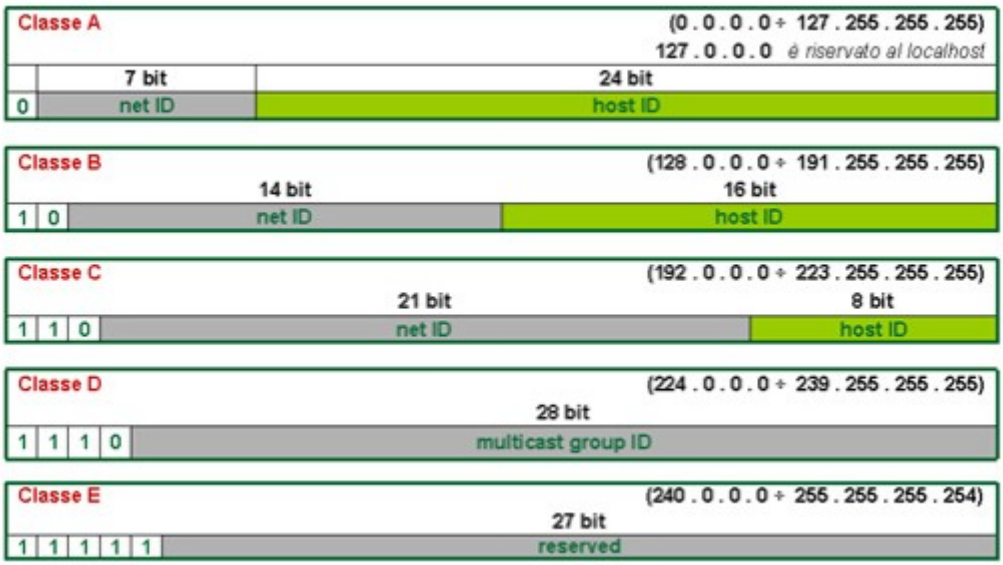
Le reti TCP/IP si avvalgono di un **indirizzo** di 32 bit (quattro *byte*); esso è espresso scrivendo i valori decimali di ciascun *byte*, separati dal carattere punto. Il suo formato è

Indirizzo IP = Indirizzo di rete (Net-Id)-Indirizzo di host (Host-Id)

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*.

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 dare 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. Per indicare non una macchina nella sottorete, ma la sottorete, si mettono a zero i bit della parte di indirizzo di *host*; per indicare tutte le macchine attestate sulla sottorete, cioè l'indirizzo di ***broadcast*** sulla sottorete, si mettono a uno i bit della parte di indirizzo di *host*. Quindi il numero di *host* possibili in una certa sottorete è pari alla dimensione dello spazio di indirizzamento della parte di *host-id* diminuita di 2.

Classi di indirizzi IP



Gli indirizzi IP sono suddivisi in cinque classi:

Classe A . Provvedono alle reti che hanno un numero cospicuo di *host*. Il campo dell'ID dell'*host* è di 24 bit, pertanto possono essere identificati circa 16 milioni di *host* per ogni rete di questo tipo. Sette bit sono dedicati all'ID di rete, per un massimo di 128 reti di classe A.
Classe B . Sono utilizzati per reti di dimensioni intermedie. Si possono avere al massimo circa 16000 reti di classe B, ciascuna con una dimensione massima di circa 64000 indirizzi.
Classe C . Sono utilizzati per numerose reti con pochi *host*. Le reti di classe C contengono meno di 256 *host* e sono individuate da 21 bit nell'ID di rete.
Classe D . Sono riservati al ***multicasting*** (RFC 1112).
Classe E. Sono riservati per usi futuri.

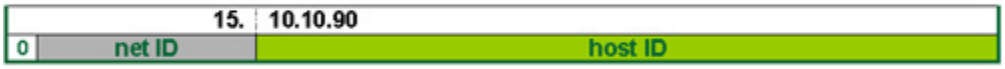
Lo spazio di indirizzamento va partizionato tra le varie classi di indirizzi, in modo che non vi siano sovrapposizioni tra classi diverse. Questo si ottiene fissando, per ogni classe, particolari configurazioni nel primo *byte*.

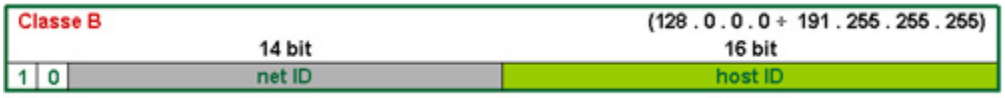
Classi di indirizzi A, B, C, D

classi A e B

Una rete di classe A è rappresentata dal primo bit (bit più significativo) a zero. I primi otto bit (0-7) identificano il numero della rete, e i rimanenti bit (8-31) identificano il numero dell'*host* all'interno della rete. Con questa rappresentazione si possono ottenere 128 (27) reti di classe A, ciascuna con un numero massimo di 16777216 (224) - 2 *host*. Gli indirizzi di classe A sono riconoscibili dal primo numero dell'indirizzo compreso tra 0 e 127.

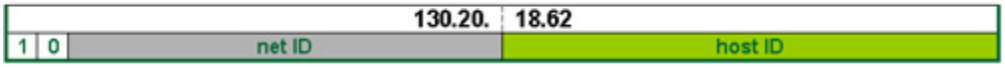
esempio





Una rete di classe B è rappresentata da un 1 ed uno 0 come primi due bit. I primi 16 bit (0-15) identificano il numero della rete, e gli ultimi 16 bit (16-31) identificano il numero dell'*host* all'interno della rete. Con questa rappresentazione si possono ottenere 16384 (214) reti di classe B, ciascuna con un numero massimo di 65536 (216) - 2 *host*. Gli indirizzi di classe B sono riconoscibili dal primo numero dell'indirizzo compreso tra 128 e 191.

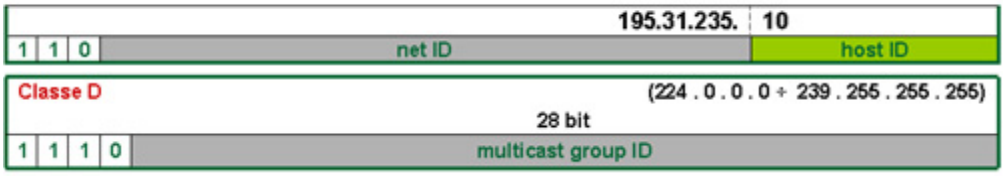
esempio



classi C e D

Una rete di classe C è rappresentata dai primi tre bit aventi valore rispettivamente 1,1, e 0. I primi 24 bit (0-23) identificano il numero della rete, e gli ultimi 8 bit (24-31) identificano il numero dell'*host* all'interno della rete. Con questa rappresentazione si possono ottenere 2097152 (221) reti di classe C, ciascuna con un numero massimo di 256 (28) - 2 *host*. Gli indirizzi di classe C sono riconoscibili dal primo numero dell'indirizzo, compreso tra 192 e 223.

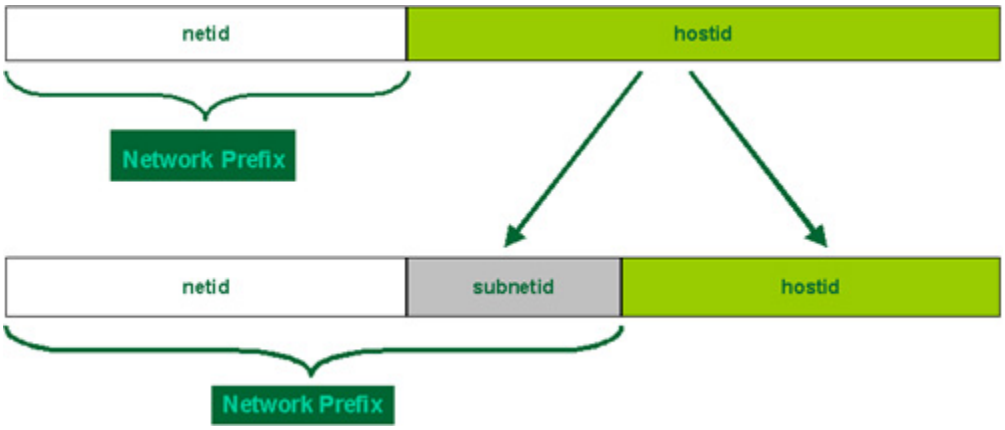
esempio



La classe D prevede che il primo *byte* contenga un valore compreso tra 224 e 239. Tale classe è riservata alla trasmissione di datagrammi IP in modalità **multicasting** .

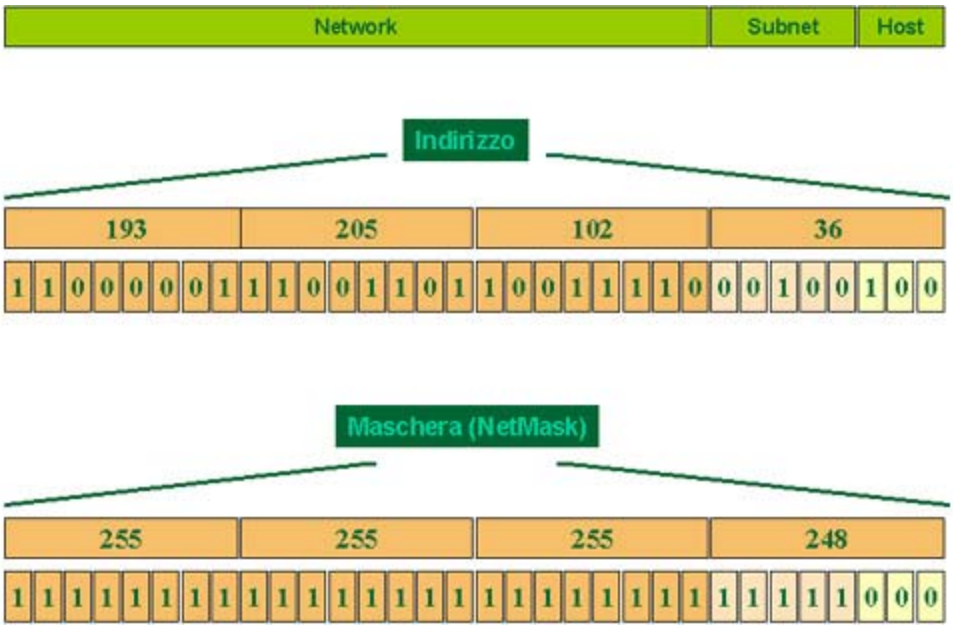
Netmask e valori possibili

***Subnet* ID**



Nel 1985, l'RFC 950 ha definito una procedura standard per supportare il *subnetting*, ovvero la divisione di una singola rete, di classe A, B o C, in sottoreti di dimensioni minori. Il *subnetting* è stato introdotto per superare alcuni dei problemi che Internet cominciava ad avere con la gerarchia di indirizzamento a due livelli (*netid* + *hostid*): la continua crescita delle tabelle di *routing*. Le organizzazioni dovevano richiedere un indirizzo di rete prima di poter installare una nuova LAN nella propria rete privata. Entrambi questi problemi sono stati affrontati aggiungendo un terzo livello gerarchico (*netid + subnetid + hostid*) allo schema di indirizzamento iniziale. Il *subnetting* ha risolto il problema della crescita delle tabelle di *routing* facendo in modo che le sottoreti di una rete non siano visibili all'esterno della rete stessa. Il percorso da Internet a qualsiasi sottorete di una certa rete IP è lo stesso, in quanto tutte le sottoreti condividono lo stesso indirizzo di rete (pur avendo differenti *subnetid*). Quindi, mentre i *router* all'interno della rete devono distinguere le singole sottoreti, i *router* di Internet hanno un'unica *entry* nella tabella di *routing* che individua tutte le sottoreti. Ciò consente all'amministratore di rete di introdurre una complessità arbitraria alla rete senza accrescere le dimensioni delle tabelle di *routing* di Internet. Il *subnetting* ha risolto il problema della continua richiesta di indirizzi IP, assegnando ad ogni organizzazione uno (o al più alcuni) indirizzi di rete. L'organizzazione è poi libera di assegnare un differente numero di sottorete per ognuna delle sue reti interne. Ciò consente ad un'organizzazione di usufruire di sottoreti addizionali, senza la necessità di richiedere ed ottenere un nuovo indirizzo di rete.

***Netmask* (esempio)**



L'ampiezza dei campi *subnet* e *host* viene definita tramite un parametro detto *netmask*. La *netmask* contiene bit a uno in corrispondenza dei campi *network* e *subnet*, e a zero in corrispondenza del campo *host*. Per determinare la *subnet* di appartenenza di un *host* a partire dal suo indirizzo IP, basta mettere in *AND* bit a bit la *netmask* con l'indirizzo IP. L'importanza di comprendere se due indirizzi appartengono o no alla stessa *subnet* è fondamentale, in quanto nel primo caso l'*host* mittente del pacchetto lo invierà direttamente verso il destinatario (*routing* diretto), nel secondo caso lo invierà ad un *router* a valle verso la destinazione (*routing* indiretto). Questo comportamento deriva dall'assunzione implicita che *ad ogni rete logica (subnet IP) corrisponda una stessa rete fisica*. Nella figura viene mostrato ad esempio un indirizzo IP 193.205.102.36 con maschera 255.255.255.248, relativo ad una *subnet* con al massimo 6 macchine. Bisogna considerare infatti che l'indirizzo con tutti zero nella parte di *host* indica la *subnet* e l'indirizzo con tutti uno indica l'indirizzo di *broadcast* sulla sottorete.

Nella tabella seguente vengono riportati i valori che potranno assumere gli ultimi 3 bit.

bit	*host*	quarto numero IP
000	*subnet*	32
001	disponibile	33
010	disponibile	34
011	disponibile	35
100	disponibile	36
101	disponibile	37
110	disponibile	38
111	*broadcast* (tutti)	39

Tutti i *router* di Internet instradano in base all'indirizzo di *Network* (193.205.102) di classe C. Il *router* responsabile di questa rete procede con l'ulteriore instradamento verso le *Subnet* in base all'esame degli ulteriori 5 bit (informazione ricavata dalla maschera).

Indirizzi privati ed indirizzi pubblici

Indirizzi privati

IANA
Allocated, Non-Internet Routable IP Address Schemes

Classe	*Network Address Range*
A	da 10.0.0.0 a 10.255.255.255 (10.0.0.0/8)
B	da 172.16.0.0 a 172.31.255.255 (172.16.0.0/12)
C	da 192.168.0.0 a 192.168.255.255 (192.168.0.0/16)

La IANA (*Internet Assigned Numbers Authority*) ha riservato i tre blocchi di indirizzi indicati in figura per le reti IP private, ovvero reti IP che non sono interconnesse ad Internet. Il primo blocco (10.0.0.0/8) rappresenta un'intera classe A. Il secondo blocco (172.16.0.0/12) è costituito dall'insieme di 16 reti di classe B contigue. Il terzo blocco (192.168.0.0/16) rappresenta 255 reti di classe C contigue.

Logical IP subnet

LIS

Con la definizione di *Logical IP Subnet* si definisce un'entità amministrativa separata composta da un gruppo di nodi IP (*host* e ***router***) collegati alla stessa rete ATM e appartenenti alla stessa IP *subnet*. Si tratta in definitiva di una rete fisica in cui gli *host* possono colloquiare direttamente tra loro senza passare attraverso *router*, ma utilizzando sistemi posti a livelli inferiori della pila **OSI** (o equivalente), quali ***switch*** , ***bridge*** e ***hub*** .

I requisiti necessari per appartenere a una LIS sono i seguenti:

- avere lo stesso **indirizzo** di *Net* e *Subnet*;
- essere configurati da una singola autorità amministrativa per la configurazione e gestione;
- essere collegati direttamente alla stessa rete ATM;
- ogni accesso tra LIS diverse deve avvenire attraverso un border *router*;
- avere un meccanismo di traduzione degli indirizzi da IP ad ATM (e viceversa);
- la rete di connessione deve essere a maglia completa.

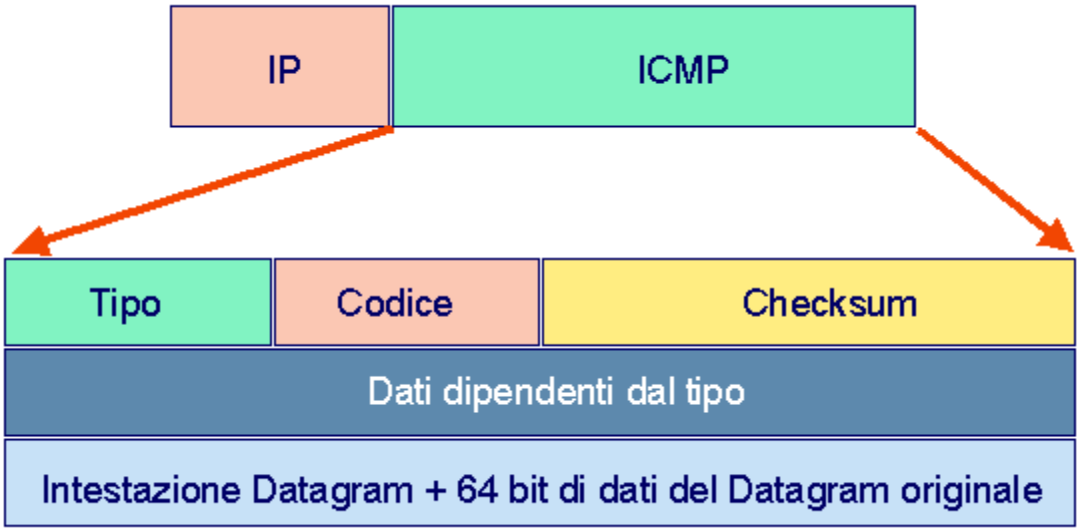
Protocolli correlati a IP e loro impiego

Il protocollo IP, impiega il corrispondente indirizzo per permettere ai *gateway* di prendere le decisioni di instradamento del datagramma. Tuttavia, affinché possano essere consegnati i dati nell'ambito di una rete locale, occorre fare riferimento all'indirizzo della stazione destinataria. Per tale motivo, e non solo, esistono altri protocolli che vengono tipicamente utilizzati nell'ambito delle reti e che possono essere considerati all'*Internet Protocol*:

- **ARP** (*Address Resolution Protocol*) e il corrispondente RARP (*Reverse Address Resolution Protocol*);
- **ICMP** (*Internet Control Message Protocol*).

Di questi due viene fornita una spiegazioni tecnica (e la loro motivazione all'uso) nelle sezioni loro dedicate.

Internet Control Message Protocol (ICMP)



IP non possiede meccanismi di indicazione o correzione degli errori, ma si affida a un modulo denominato *Internet Control Message Protocol* (ICMP) per la segnalazione degli errori sopravvenuti nel corso dell'elaborazione di un datagramma e per la generazione di messaggi amministrativi e di stato. ICMP risiede in ogni *computer host* o *router* come protocollo abbinato a IP. ICMP viene utilizzato tra gli *host* o i *router* quando i datagrammi non possono essere consegnati, quando un *router* non ha sufficiente memoria temporanea per conservare ed inoltrare unità dati del protocollo, eccetera. ICMP comunica all'*host* se una destinazione è irraggiungibile; inoltre, gestisce o crea un messaggio per segnalare il superamento del tempo massimo di permanenza in rete (**TTL**) di un datagramma. Infine, ICMP esegue alcune funzioni di modifica per determinare se l'intestazione IP è errata o in altro modo inintelligibile.

Il protocollo ICMP è descritto in RFC 792 ed è incluso in tutte le implementazioni IP come un protocollo a basso livello che si appoggia direttamente su IP.

È utilizzato per la trasmissione dei messaggi di errore, di messaggi di controllo e misure di prestazioni, ma non specifica le azioni da intraprendere.

I messaggi viaggiano nel campo dati del *datagram* IP e vengono manipolati dal *software* IP, non dagli applicativi utente.

ICMP viene imbustato in IP, indirizzato con 1 nel campo *protocol*. Il formato del pacchetto ICMP prevede:

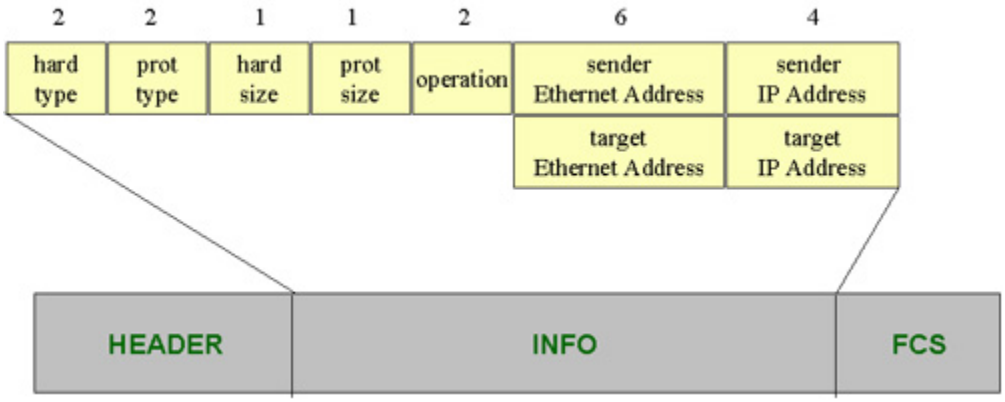
- tipo, indica un particolare messaggio ICMP (si veda la tabella seguente);
- codice, viene usato in alcuni messaggi ICMP per specificare alcune condizioni;
- ***checksum*** , per il controllo di errore; viene calcolato su tutto il pacchetto ICMP;
- la parte rimanente viene usata per trasmettere dei dati legati al particolare messaggio ICMP.

Come esempio, nella figura precedente è mostrato un pacchetto di ICMP, del tipo *error message*, in cui nella parte di dati è inclusa l'intestazione IP e altri 64 bit del pacchetto che ha generato l'errore.

Address Resolution Protocol (ARP) e Reverse ARP

Lo *stack* IP fornisce un protocollo per risolvere gli indirizzi. Il protocollo di risoluzione degli indirizzi (ARP) gestisce la traduzione degli indirizzi IP in indirizzi fisici e nasconde questi indirizzi fisici agli strati superiori. Generalmente, ARP

funziona con tabelle di mappatura, definite *cache* ARP, che forniscono la mappatura 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*.



Il protocollo ARP si appoggia direttamente sul livello *data link* e non su IP. Il pacchetto ARP è incapsulato nella PDU del livello *data link*, che potrebbe essere per esempio una trama *Ethernet*. La richiesta viene inviata all'indirizzo di *broadcast* di livello 2, perché deve essere elaborata da tutte le macchine; contiene inoltre l'indirizzo di livello 2 e quello di livello 3 della macchina sorgente; così la macchina che riconosce il proprio indirizzo di livello 2 sa a chi inviare il *reply*. Nel pacchetto di risposta vengono riempiti tutti i campi; importante è chiaramente l'indirizzo di livello 2 di chi invia il *reply*, che era l'informazione richiesta in partenza. Qualsiasi modulo ARP può avvalersi di un pacchetto ARP per aggiornare la propria *cache*: il modulo esamina l'indirizzo IP e l'indirizzo *hardware* del mittente per determinare se queste voci sono comprese nella propria *cache*. In questo modo, ottiene tutte le informazioni possibili sui dati. Il pacchetto ARP, oltre ai campi per gli indirizzi di livello 2 e 3 di sorgente e destinazione, contiene:

- *hard type*, specifica il tipo di indirizzo di livello 2; per indicare che l'indirizzo è di tipo MAC si usa il valore 1;
- *protocol type*, specifica il tipo di indirizzo di livello 3, si usa 0x0800 per indicare indirizzi IP;
- *hard size*, indica la lunghezza dell'indirizzo di livello 2;
- *protocol size*, indica la lunghezza dell'indirizzo di livello 3;
- *operation*, indica il tipo di comando ARP, 1 per ARP-*request*, 2 per ARP-*reply*.

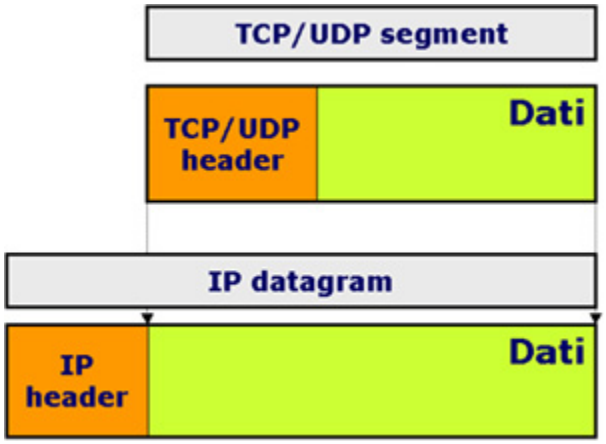
A volte risulta utile risalire all'indirizzo IP a partire dall'indirizzo *Ethernet*; tali funzionalità sono assicurate dal Protocollo RARP (*Reverse Address Resolution Protocol*).

Protocolli di trasporto in Internet

Paolo Zaffoni

5.2.1 (Elencare e definire gli strati dei protocolli di rete TCP/IP e OSI), 5.4.2 (Descrivere protocolli software per LAN come TCP/IP)

TCP - Transmission Control Protocol



Il *Transmission Control Protocol* (**TCP**) è stato progettato al fine di offrire un servizio *end-to-end* perfettamente affidabile alle applicazioni, 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 in datagrammi.

Il protocollo è descritto nelle ***Request For Comments* (RFC) 793** ed è successivamente ampliato a causa di alcune *bug fixes*: RFC 1122. Se ne trova anche una estensione: RFC 1323.

Le funzioni svolte dal protocollo TCP sono:

- **controllo di errore** ;
- **controllo di flusso** ;
- **controllo di sequenza** ;
- *multiplexing* 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 ***piggybacking*** (*acknowledgment* contenuto nelle risposte). Inoltre, i numeri di sequenza servono a TCP per il risequenziamento dei segmenti, 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.

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

TCP - Multiplazione

Compito di TCP è quindi anche quello di distinguere tra i diversi programmi applicativi e i diversi utenti che fanno uso di uno stesso sistema. Come avviene per UDP, si è stabilito che ogni sistema contenga un insieme di punti di destinazione chiamati **porte** . Anche in TCP, ogni porta è identificata da un intero positivo. L'indirizzo di un utente di strato TCP è denominato porta, mentre l'indirizzo completo nell'insieme dei protocolli TCP e IP è denominato ***socket*** ed è costituito dalla coppia:

- `porta@IP_Address`.

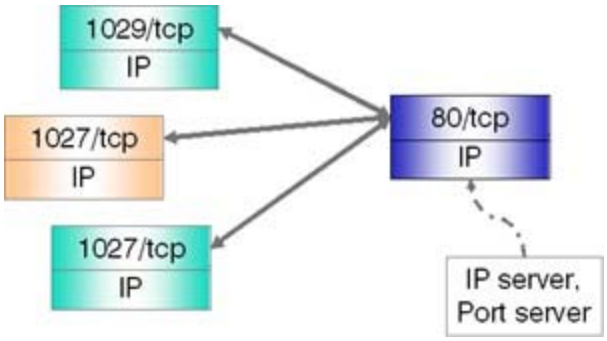
La componente *port* è contenuta nell'intestazione dell'unità di dati di TCP, mentre la componente *IP_Address* è contenuta nell'intestazione dell'unità dati di IP. Questo significa che tutte le sessioni di comunicazione in atto tra due specifici sistemi useranno lo stesso indirizzo IP di sorgente e lo stesso indirizzo IP di destinazione; saranno perciò distinte solo allo strato TCP.

Ne segue che queste sessioni sono multiplate su un unico indirizzo IP, ovvero su un unico canale IP di comunicazione (non su una connessione IP; in questo caso la definizione di multiplazione va usata con cautela dal momento che IP è un protocollo senza connessione).

TCP - Connessione

Come per **UDP** esistono dei numeri di porta ben noti (***well known port***), ma a differenza di UDP, alla stessa porta può corrispondere più di un processo. Tale maggiore complessità deriva dal fatto che TCP è un protocollo con connessione.

In TCP 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 2772 dell'*host* 197.2.7.2 e la porta 80 dell'*host* 151.80.4.1 sarà identificata dalla coppia:

- 2772@197.2.7.2, 80@151.77.4.1.

Grazie a tale meccanismo, un indirizzo di porta di un sistema può supportare connessioni multiple; la porta 2772 dell'*host* 197.2.7.2 potrebbe gestire contemporaneamente le seguenti connessioni (ed anche altre):

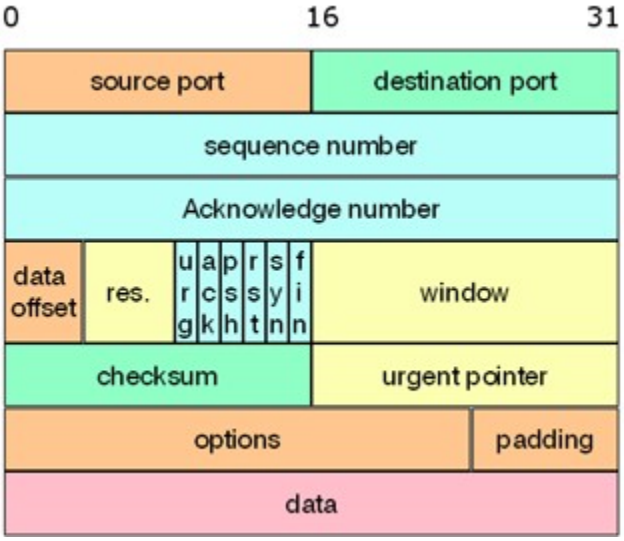
- 2772@197.2.7.2, 80@151.77.4.5;
- 2772@197.2.7.2, 80@165.20.2.3

TCP - Conclusioni

Evidentemente tutte le funzionalità fornite da TCP hanno un costo in termini di aumento del ritardo di trasmissione e di aumento della quantità di informazioni che devono essere trasferite nella rete (*overhead*); ciononostante TCP può essere impiegato anche in reti ad alta velocità. In alcuni esperimenti si sono raggiunte portate utili di 8 Mbit/s su una *Ethernet* con capacità di trasferimento pari a 10 Mbit/s ed è stato dimostrato che in canali opportuni è possibili raggiungere portate utili dell'ordine di 1 Gbit/s. Nel seguito vengono descritti con più dettaglio i meccanismi sin qui elencati e illustrate alcune possibili estensioni di TCP per migliorarne le prestazioni in reti ad alta velocità.

Unità dati e pacchetto TCP

Le unità di dati dello strato TCP sono dette segmenti. Il segmento è composto da una intestazione e da un campo informativo, che contiene i dati di utente. Il formato del segmento TCP è illustrato nella figura seguente. Ogni riga contiene 32 bit.



- *Source Port* (Porta di Origine, 16 bit): definisce l'indirizzo logico del processo sorgente dei dati;
- *Destination Port* (Porta di Destinazione, 16 bit): definisce l'indirizzo logico del processo destinatario dei dati;
- *Sequence Number* (Numero di Sequenza, 32 bit): numero di sequenza in trasmissione; contiene il numero di sequenza del primo *byte* di dati contenuti nel segmento a partire dall'inizio della sessione TCP (se SN=m ed il segmento contiene n *bytes* il prossimo SN sarà pari a m+n); la numerazione dei segmenti è quindi effettuata non numerando i segmenti stessi (come in X.25), ma gli ottetti in essi contenuti;
- *Acknowledgement Number* (Numero di Riscontro, 32 bit): numero di sequenza in ricezione; nei segmenti in cui il bit ACK, presentato più avanti, è posto al valore binario 1, questo campo contiene il numero di sequenza del prossimo *byte* che il sistema che emette tale segmento si aspetta di ricevere; nel caso di connessioni interattive bi-direzionali si usa quindi il meccanismo denominato addossamento (o *piggybacking*) dei riscontri; ovvero si utilizzano segmenti contenenti dati di utente per inviare i riscontri al trasmettitore senza dover, a tal fine, inviare dei segmenti appositi;
- *Offset* (4 bit): contiene il numero di parole di 32 bit contenute nell'intestazione di TCP; l'intestazione di TCP è sempre costituita da un numero di bit multiplo di 32 (questo campo è necessario poiché il campo *Options* è di dimensioni variabili);
- *Reserved* (6 bit): riservato per usi futuri, per ora contiene degli zeri;
- *Control bit* (6 bit): i bit di controllo sono:
  - URG: viene posto uguale al valore binario 1 quando il campo *Urgent Pointer* (definito in seguito) contiene un valore significativo;
  - ACK: viene posto uguale al valore binario 1 quando il campo *Acknowledgement Number* contiene un valore significativo;
  - PSH: viene posto uguale al valore binario 1 quando l'applicazione esige che i dati forniti vengano trasmessi e consegnati all'applicazione ricevente prescindendo dal riempimento delle memorie allocate fra applicazione e TCP e viceversa (solitamente infatti è il riempimento delle suddette memorie che scandisce la trasmissione e la consegna dei dati);
  - RST: viene posto uguale al valore binario 1 quando un malfunzionamento impone il *reset* della connessione;
  - SYN: viene posto uguale al valore binario 1 solo nel primo segmento inviato durante il *3-way handshaking* (stretta di mano a tre fasi, una fase di sincronizzazione fra le entità TCP);
  - FIN: viene posto uguale al valore binario 1 quando la sorgente ha esaurito i dati da trasmettere.
- *Window* (Finestra, 16 bit): dimensione della finestra; contiene il numero di *bytes* che, a cominciare dal numero contenuto nel campo *Acknowledgement Number*, il destinatario del segmento può inviare al mittente del segmento stesso senza ricevere riscontri;
- *Checksum* (16 bit): contiene l'informazione di controllo che permette all'entità TCP ricevente di verificare la correttezza del segmento ricevuto;
- *Urgent Pointer* (Puntatore Urgente, 16 bit): contiene il numero di sequenza del *byte* che delimita

superiormente i dati che devono essere consegnati urgentemente al processo ricevente. Tipicamente sono messaggi di controllo che esulano dalla comunicazione in senso stretto. A tale traffico ci si riferisce di solito con il nome di *out-of-band* (fuori banda);
- *Options* (Opzioni, di lunghezza variabile): sono presenti solo raramente: le più note sono *End of Option List*, *No-operation* e *Maximum Segment Size* (MSS). Ci si soffermerà, in seguito, solo sull'ultima opzione citata; *Padding* (Riempitivo) (di lunghezza variabile): contiene sempre degli zeri. Serve come riempitivo aggiunto per far sì che l'intestazione abbia una lunghezza multipla di 32 bit.

Servizi TCP e TCP port

Il numero di porta è il valore globale e univoco attraverso il quale un programma *client* indirizza un programma *server*; per richiedere un certo servizio, un applicativo *client* deve aprire una connessione con la macchina di destinazione sulla 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 naturale 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 di porta	Servizio
0	Riservata
1	TCPMUX *Multiplexor* TCP
5	RJE *Remote Job Entry*
7	*ECHO* Eco
9	*DISCARD* Scarto
11	*USERS* Utenti attivi
13	*DAYTIME* Ora del giorno
15	Programma di stato della rete
17	*QUOTE* Citazione del giorno
19	*CHARGEN* Generatore di caratteri
20	FTP-DATA *File Tranfer Protocol* (dati)
21	FTP *File Tranfer Protocol* (controllo)
23	TELNET Connessione di terminale
25	SMTP *Simple Mail Transport Protocol*
37	*TIME* Tempo
42	*NAMESERVER Server* di nomi dell'*host*
43	*NICNAME* Chi è
53	*DOMAIN Server* di nomi del dominio DNS

77	Qualunque servizio RJE privato
79	*FINGER Finger* (indicatore)
80	HTTP *HyperText Tranfer Protocol*
93	DCP *Device Control Protocol*
95	SUPDUP Protocollo SUPDUP
101	*HOSTNAME Server* di nomi di *host* NIC
102	ISO-TSAP ISO-TSAP
103	X400 Servizio di posta X.400
104	X400SND Invio di posta X.400
110	POP3
111	SUNRPC RPC di *Sun Microsystems*
113	AUTH Servizio di autenticazione
117	UUCP-PATH Servizio di percorso (*path*) UUCP
119	NNTP Protocollo di trasferimento news USENET
123	NTP NTP
129	PWDGEN Protocollo generatore di *password*
139	NETBIOS-SSN Servizio di sessione di NETBIOS
160-223	Riservati

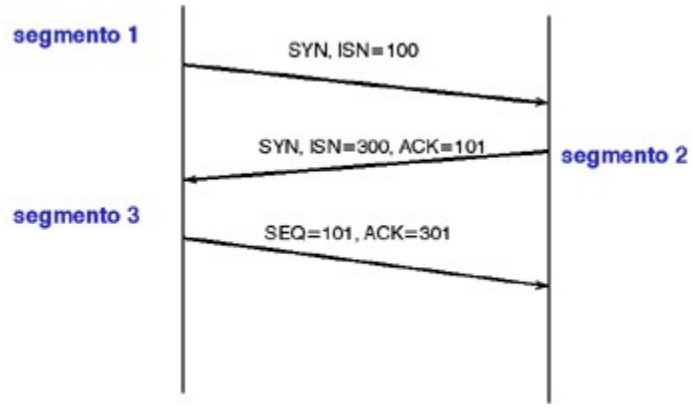
Controllo in TCP - 3-way handshake

Il protocollo **TCP** è un protocollo orientato alla connessione. Tale affermazione implica che l'entità TCP residente nel sistema mittente deve instaurare una connessione con l'entità TCP residente nel sistema di destinazione, prima che la fase di trasferimento delle informazioni possa avere inizio.

Le due entità TCP interagenti si sincronizzano scambiandosi il proprio numero di sequenza in trasmissione iniziale, che rappresenta il numero a partire dal quale tutti i *byte* trasmessi saranno sequenzialmente numerati una volta instaurata la connessione. All'apertura della connessione, prima dell'effettivo scambio di dati, le macchine coinvolte eseguono una fase di inizializzazione per scambiarsi il numero di sequenza iniziale, *Initial Sequence Number* (ISN), e per fissare alcuni parametri.

Ogni macchina sceglie il proprio ISN nello spazio a disposizione da 0 a ((2^32) -1); il numero di sequenza in trasmissione non può iniziare da un dato valore fisso; ogni volta che si instaura una nuova connessione si deve scegliere il numero di sequenza in trasmissione da cui iniziare per evitare di usare numeri relativi a vecchie connessioni, fatto che può creare delle sovrapposizioni se alcuni pacchetti, per ritardi della rete, sono ancora in transito sulla connessione.

Tra i *flag* dell'intestazione TCP, il bit SYN attivato indica, che il contenuto del campo *Sequence Number* è valido; il bit ACK indica che il contenuto del campo *acknowledge* è significativo.

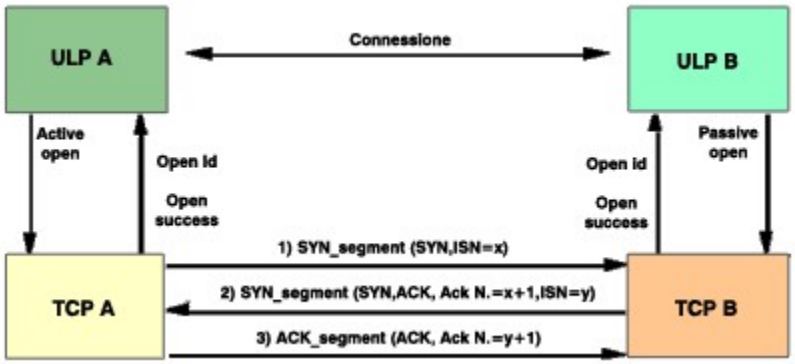


Lo scambio informativo tra le due macchine avviene con i seguenti passi:

- da A a B: il mio ISN è X (SYN=1;ACK=0);
- da B ad A: il tuo ISN è X;
- da B ad A: il mio ISN è Y;
- da A a B: il tuo ISN è Y (SYN=1;ACK=1).

Gli step 2 e 3 sono combinati in un unico messaggio con i bit SYN=1 e ACK=1; quindi i pacchetti di apertura sono 3.

La figura mostra in maggior campo la procedura *three way handshake*.



Quando deve essere instaurata una connessione allo strato di applicazione fra un dato processo applicativo, denominato ULP A (ULP=*Upper Layer Protocol*), residente nel sistema A, ed un ULP B, residente nel sistema remoto B, il primo passo che si deve compiere è l'invio di una *active open* (primitiva di Richiesta di Servizio) da parte dell'ULP A all'entità TCP A, con la quale quest'ultima viene messa al corrente di tale desiderio.

L'entità TCP A risponde ad ULP A tramite la primitiva *open id*, primitiva di Risposta di Servizio, ed avvia il meccanismo *3-way handshaking* inviando, all'entità TCP ricevente, TCP B, un primo segmento. Tale primo segmento, denominato SYN e contenente il bit SYN posto al valore logico 1, ha un numero di sequenza in trasmissione (denominato *Initial Sequence Number* - ISN), pari al valore assunto dal contatore residente nel sistema A. Per ogni segmento scambiato, vi sono:

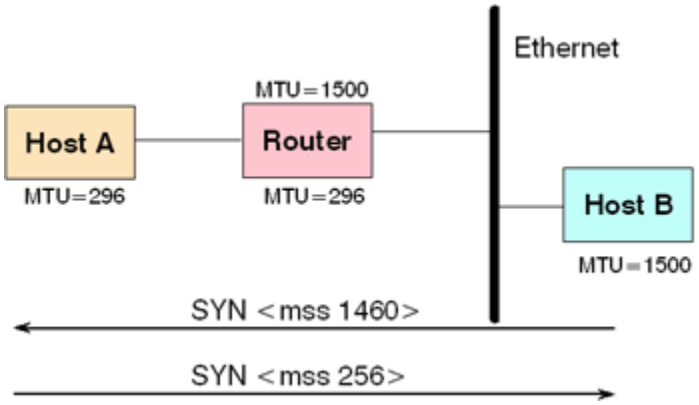
- il primo valore assunto dal campo *Sequence Number*, ISN;
- il valore assunto dal campo *Acknowledgement Number*, Ack. N;
- la scritta SYN e/o ACK quando i relativi bit sono posti al valore logico 1.

Controllo in TCP - MSS

Il *Maximum Segment Size* (MSS) rappresenta la dimensione massima del campo dati che TCP può inviare all'*host* remoto. Quando viene instaurata una connessione, nella fase di apertura, i due *host* annunciano i rispettivi valori di MSS, usando il campo opzioni dell'*header* del TCP. Il valore di *default* è di 536 *byte*. Il datagramma IP risultante è 40 *byte*: 20 *byte* per l'*header* TCP e 20 *byte* per l'*header* IP. Affinché non si abbia frammentazione del datagramma IP deve risultare:

MSS + TCP *header* + IP *header* <= MTU,

dove *Maximum Transfer Unit* (MTU) rappresenta la dimensione massima del pacchetto a livello IP e dipende dalla tecnologia di sottorete. I due *host* si accordano, quindi, per usare il minimo tra i due MSS annunciati; in figura si usano segmenti TCP di 256 *byte*.



Controllo in TCP - Affidabilità

Il TCP garantisce l'affidabilità mediante PAR (*Positive Acknowledge with Retransmission*). Ogni segmento contiene un *checksum* che il ricevitore usa per verificare l'integrità dei dati. Se il segmento è corretto, dal protocollo sulla macchina in ricezione viene inviato un segmento di *acknowledge*. Se il segmento non è corretto, viene semplicemente scartato e non viene inviato nulla alla macchina in trasmissione. Sulla macchina sorgente la mancanza del riscontro, allo scadere di un opportuno *timeout*, indica che il pacchetto è stato scartato o che non è arrivato a destinazione, e che quindi va ritrasmesso.

Il segmento viene costruito cercando di raggiungere la dimensione MSS stabilita al momento della connessione. Ciascun segmento contiene un numero di sequenza che identifica la posizione nel *byte stream* del primo *byte* a partire da ISN. Il riscontro viene inviato su un segmento di *acknowledge* (se è possibile insieme ai dati) con ACK=N, che indica che tutti i *byte* fino ad N-1 sono stati ricevuti correttamente. Insieme all'*acknowledge* viene inviato un valore per la *window*, che definisce il numero di *byte* che il ricevitore è in grado di accettare. Il valore della *window* inviato dal ricevente consente la realizzazione di un controllo di flusso basato sulle necessità della macchina di destinazione.

Controllo in TCP - Finestra

Il trasmettitore determina la sua finestra utilizzabile, che rappresenta quanti dati (*byte*) può trasmettere immediatamente. La finestra si apre man mano che il ricevitore riscontra al trasmettitore i dati inviatigli. Il moto relativo dei due estremi della finestra fa aumentare o diminuire la dimensione della stessa.

La finestra si chiude quando l'estremo sinistro avanza verso destra. Ciò accade quando i dati vengono trasmessi, fino a che gli stessi non sono riscontrati.

La finestra si apre quando l'estremo destro avanza verso destra, consentendo al trasmettitore di inviare ulteriori dati. Ciò accade quando il ricevitore legge i dati riconosciuti, liberando spazio nel suo *buffer* TCP, ed invia i relativi riscontri al trasmettitore.

In questa fase il ricevitore può anche segnalare al trasmettitore una variazione (in più o in meno) della finestra. Se l'estremo sinistro raggiunge quello destro, la finestra è definita zero *window*: il trasmettitore non può inviare dati. In ogni momento, quindi, la finestra di trasmissione fissa il numero di pacchetti che possono essere inviati e, in particolare, la somma dei pacchetti da inviare e di quelli non ancora riscontrati deve essere sempre uguale al valore della finestra.

La finestra di trasmissione è controllata attraverso due meccanismi:

- la finestra annunciata dal ricevitore, che limita la finestra massima di trasmissione;
- la quantità di traffico presente in rete, perché se non ci sono pacchetti riscontrati non se ne possono inviare di nuovi.

In questo modo il TCP si adegua alle condizioni di traffico e trasmette ad una velocità pari alla capacità disponibile in rete.

La finestra di trasmissione viene aumentata per fare in modo che il TCP possa sfruttare tutta la banda disponibile. In partenza la finestra viene aperta con un andamento esponenziale, fino a che non si verifica la prima perdita di un

pacchetto; questo evento può essere individuato dalla scadenza di un *timer* entro il quale doveva arrivare l'***acknowledge***, o dall'arrivo in trasmissione di *acknowledge* che riscontrano sempre lo stesso pacchetto: in ricezione infatti per ogni pacchetto fuori sequenza si invia un *acknowledge* dell'ultimo pacchetto in sequenza.

Alla prima perdita, la finestra di trasmissione viene ridotta ad un solo pacchetto e si calcola il valore di ssthresh (*slow-start threshold*), pari alla metà del valore che aveva la finestra di trasmissione quando si è verificata la perdita; si ha ancora un andamento esponenziale, fino a quando la finestra assume il valore di ssthresh e da lì in poi la finestra viene aperta in modo lineare, fino alla prossima perdita.

Applicazioni per TCP

Al livello più alto della pila di protocolli si pongono gli applicativi, che possono utilizzare come livello di trasporto UDP o TCP a seconda delle necessità. Poiché UDP è un protocollo di tipo ***connection-less*** (non prevede controllo di flusso o recupero di errore), questo non è consigliabile con applicativi per il trasferimento dati, come **FTP** o **HTTP** , ma può essere utile, grazie al ridotto *overhead*, per applicativi che usano pacchetti di piccole dimensioni, nonché per gli applicativi *real-time* in cui è inutile la ritrasmissione di pacchetti errati.

I più comuni protocolli applicativi sono i seguenti:

- **Telnet** ;
- **FTP** ;
- **DNS** ;
- **Posta elettronica** :
  - formato dei messaggi (RFC 822, *MIME*);
  - trasferimento dei messaggi (SMTP, POP3, IMAP);
- **HTTP** ;
- **PROXY** ;

Telnet

Telnet è un protocollo che permette ad un utente di collegarsi, tramite elaboratore locale, ad un qualsiasi altro elaboratore remoto connesso alla rete. La connessione viene attivata facendo seguire al comando telnet il nome del calcolatore remoto o il suo indirizzo. Da quel momento in poi, tutti i caratteri battuti sulla tastiera sono inviati all'elaboratore remoto e le risposte da questo generate sono visualizzate sullo schermo locale. Il calcolatore locale è reso trasparente dal programma telnet e si opera come se si fosse direttamente connessi all'elaboratore remoto.

Quando ci si scollega dall'elaboratore remoto, il programma telnet termina e ci si trova nuovamente a dialogare con il sistema operativo dell'elaboratore locale.
Normalmente il programma telnet include degli emulatori per i terminali più diffusi (esempio: Digital VT100 e IBM 3270). Telnet è specificato dalle RFC 854 e 855. Alternativamente al telnet è possibile utilizzare il comando `rlogin` che ha funzionalità analoghe.

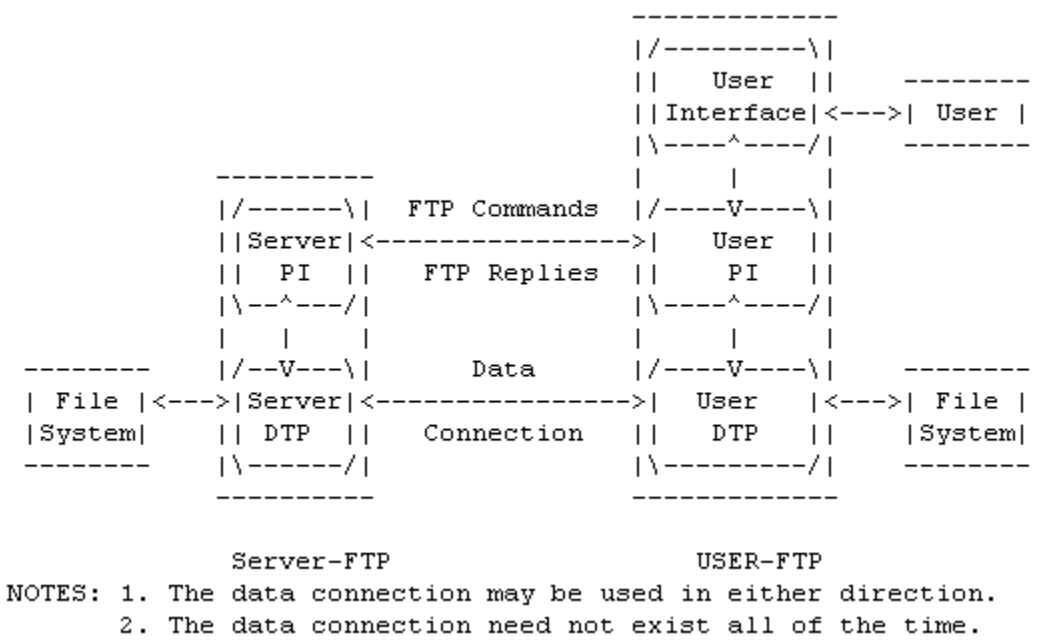
FTP

[FTP è specificato nel RFC 959]

Il *File Transfer Protocol* (**FTP**) è una specifica di protocollo applicativo che permette ad un utente collegato ad un calcolatore, di trasferire *file* da e verso un altro elaboratore. La sicurezza è gestita tramite la richiesta all'utente di fornire uno *username* ed una *password* validi presso l'elaboratore remoto.

FTP gestisce la rappresentazione dei dati in maniera automatica di *file* di testo tra elaboratori con codifiche dei

caratteri diverse (ad esempio quando si ha a che fare con diversi sistemi operativi e quindi diverse strutture di *file* e diverso set di caratteri). Telnet risolve i problemi di eterogeneità forzando entrambe le macchine a lavorare con uno stesso standard: i caratteri scambiati sono codificati con NVT **ASCII** .



FTP differisce dalle altre applicazioni perché usa due connessioni TCP per trasferire un *file*: una connessione di controllo sulla porta 21, in uso durante tutto il trasferimento del *file* e che serve per passare i comandi del *client* e le risposte del *server* (in particolare per inizializzare il trasferimento di un *file*), e una connessione per i dati, che è creata ogni volta che va trasferito un *file*. FTP supporta un limitato set di tipi di *file* e di strutture di memoria: per trasferire un *file* la macchina *client* e quella *server* devono inizializzarsi e fare delle scelte per le opzioni previste.

Per decidere come un *file* deve essere trasferito e memorizzato, la macchina *client* e quella *server* devono fare una scelta per un formato comune di rappresentazione e trasmissione dei dati ed in particolare:

Tipo di *file*

- *file* **ASCII** , è trasferito con codifica NVT ASCII e necessita per chi trasmette la conversione dal formato locale in ASCII e per chi riceve la conversione opposta; viene inviata la fine di ogni linea, quindi in ricezione si fa una scansione dei *byte* in attesa del *carriage return*; è usato per trasferire *file* di testo;
- *file* immagine o binario, trasferito come un flusso continuo di bit; è usato di solito per trasferire *file* binari;

Struttura

- *file* come flusso continuo di *byte*, senza nessuna struttura interna;
- *file* organizzato con una struttura a record, usato per i *file* di testo;
- *file* organizzato per pagine, in cui si trasmette una pagina alla volta, con numero di pagina che permette al ricevitore di memorizzarle in modo casuale;

Modo di trasmissione

- *stream*, cioé come flusso continuo di bit; per un *file* senza struttura, la fine del *file* viene individuata dalla chiusura della connessione, mentre per un *file* con struttura a record, una speciale sequenza di due *byte* indica la fine dei record e del *file*;

- a blocchi, con *file* trasferito a blocchi ognuno preceduto da un *header*. La combinazione delle precedenti opzioni dà le possibili combinazioni nel trasferimento e memorizzazione dei *file*. La scelta più comune in ambiente *Unix* è come tipo di *file* ASCII o binario, senza struttura e modo di trasmissione *stream*.

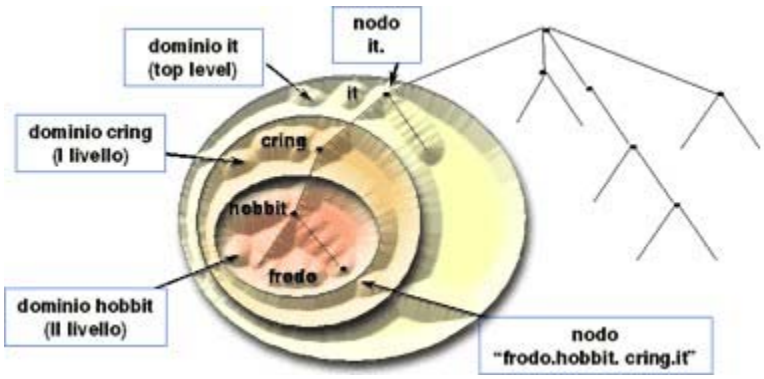
I comandi e le repliche che il *client* e il *server* FTP si scambiano sul canale di controllo sono codificati in NVT ASCII. I comandi che il *client* può inviare al *server* sono circa 30; i più importanti sono riportati nella tabella. Le repliche del *server* sono costituite da un numero di tre cifre usato dal *client* per individuare il tipo di risposta, e da un commento per l'utente. Esempi di *reply* sono: `200 Command OK`, `331 Username OK - password required`, eccetera.

Comando	Descrizione
ABOR	annulla (*abort*) il precedente comando FTP e ogni trasferimento di dati
LIST filelist	elenca (*list*) *file* e *directory*
PASS password	*password* sul *server*
PORT n1, n2, n3, n4, n5, n6	*client IP address* (*n1.n2.n3.n4*) e *port* (*n5 x 256 + n6*)
QUIT	*logoff* dal *server*
RETR filename	ottieni (*retrieve*, *get*) un *file*
STOP filename	immagazzina (*store*, *put*) un *file*
SYST	*server returns system type*
TYPE type	specifica il tipo di *file*: A per ASCII, I per *image*
USER username	*username* sul *server*

TFTP (*Trivial* FTP) è una versione semplificata di FTP usata normalmente per *downloading* di *software* e specificata nel RFC 1350.

DNS

[Il DNS è specificato negli RFC 1035, 883 e 882]



I programmi raramente si riferiscono agli *host*, alle *mailbox* e ad altre risorse mediante i loro indirizzi di rete IP e tantomeno tramite numeri binari. Sarà preferibile rivolgersi ai sistemi tramite stringhe, come ad esempio utente@dominio. Tuttavia, gli apparati di rete dispongono della sola nozione di indirizzo binario, quindi è necessario un meccanismo che consenta di convertire le stringhe in indirizzi di rete.

Il *Domain Name Server* (**DNS**) è una base di dati distribuita e replicata per gestire principalmente la corrispondenza tra nomi e indirizzi IP. DNS si avvale di una struttura gerarchica ad albero per stabilire i nomi. La radice è la voce di massimo livello ed è anche il nodo genitore rispetto ai livelli inferiori di un albero. L'albero è costituito da rami, che collegano i nodi.

Le etichette dei nodi dello stesso livello nell'albero devono essere completamente univoche e distinte: ciò significa che l'etichetta deve essere un nome unico e inconfondibile nel livello di nodo specifico.

Ogni dominio, identificato da un nome univoco, controlla ed ha la responsabilità dell'allocazione dei domini nel suo comprensorio. Per creare un nuovo dominio, è necessaria l'autorizzazione del dominio nel quale questo verrà incluso. Una volta che il nuovo dominio è stato creato e registrato, esso può creare a sua volta dei sottodomini senza aver bisogno di richiedere l'autorizzazione a nessuno dei domini superiori.

- **com**: Organizzazioni commerciali (hp.com, *sun*.com ...);
- **edu**: Organizzazioni educative (*berkeley*.edu, *purdue*.edu ...);
- **gov**: Organizzazioni governative (nasa.gov, nsf.gov ...);
- **mil**: Organizzazioni militari (*army*.mil, *navy*.mil ...);
- **net**: Organizzazione di gestione reti (nsf.net ...);
- **org**: Organizzazioni non commerciali (eff.org ...);
- **int**: Organizzazioni internazionali (nato.int ...);
- ***country-code***: Codice di due caratteri per indicare una nazione.

Lo spazio dei nomi è diviso in diversi domini di massimo livello (*top-level domains*), tra i quali distinguiamo dei *top-level domain* generici (*generic domains*) e dei *top-level domain* geografici (*country domains*). Almeno in teoria, un unico *name server* potrebbe contenere l'intero DNS *database* e rispondere a tutte le interrogazioni che lo riguardano. In realtà, questo *server* sarebbe così sovraccarico da essere inutilizzabile. Inoltre, se per qualsiasi motivo questo si guastasse, l'intera Internet si non disporrebbe più del servizio dei nomi.

Non è pensabile quindi che tutte le traduzioni indirizzo IP - *name_address* siano contenute all'interno di un unico *database* o siano decise da una sola organizzazione. Il sistema è organizzato invece con la modalità di *database* distribuito e con il meccanismo della *delegation*: una società o università, proprietaria di una rete, viene delegata per scegliere le traduzioni *IP address - name address* come vuole, e si impegna a mettere a disposizione un *server* DNS che, quando viene interrogato dall'esterno, possa fare queste traduzioni, che quindi sono conosciute solo su quel *server*.

Posta elettronica

[Standard per la formazione di messaggio è specificato nel RFC 822]

La posta elettronica è uno dei servizi più consolidati ed usati nelle reti. In Internet è in uso da circa 20 anni, e prima del WWW era senza dubbio il servizio più utilizzato. Un servizio di posta elettronica, nel suo complesso, consente di effettuare le seguenti operazioni:

- comporre un messaggio;
- spedire il messaggio (a uno o più destinatari);
- ricevere messaggi da altri utenti;
- leggere i messaggi ricevuti;
- stampare, memorizzare, eliminare i messaggi spediti o ricevuti.

Di norma, un messaggio ha un formato ben preciso. In Internet un messaggio ha un formato (definito nell'RFC 822) costituito da un *header* e da un *body*, separati da una linea vuota. L'*header* è a sua volta costituito da una serie di linee, ciascuna relativa a una specifica informazione (identificata da una parola chiave che è la prima sulla linea); alcune informazioni sono:

- ***To***: indirizzo di uno o più destinatari.
- ***From***: indirizzo del mittente.
- **Cc**: indirizzo di uno o più destinatari a cui si invia per conoscenza.
- **Bcc**: *blind* Cc: gli altri destinatari non sanno che anche lui riceve il messaggio.

- ***Subject***: argomento del messaggio.
- ***Sender***: chi materialmente effettua l'invio (ad esempio nome della segretaria).

Il *body* contiene il testo del messaggio, in caratteri ASCII. L'ultima riga contiene solo un punto, che identifica la fine del messaggio. Gli indirizzi di posta elettronica in Internet hanno la forma: `username@hostname` dove *username* è una stringa di caratteri che identifica il destinatario, e *hostname* è un nome DNS oppure un indirizzo IP. Ad esempio, frodo@hobbit.cring.it.

La posta elettronica viene implementata in Internet attraverso la cooperazione di due tipi di sottosistemi:

- *Mail User Agent* (MUA);
- *Mail Transport Agent* (**MTA**).

Il primo permette all'utente finale di:

- comporre messaggi;
- consegnarli a un MTA per la trasmissione;
- ricevere e leggere messaggi;
- salvarli o eliminarli.

Il secondo si occupa di:

- trasportare i messaggi sulla rete, fino alla consegna a un MTA di destinazione;
- rispondere ai MUA dei vari utenti per consegnare loro la posta arrivata;
- in questa fase l'MTA richiede ad ogni utente una *password* per consentire l'accesso ai messaggi.

SMTP, POP3 e IMAP

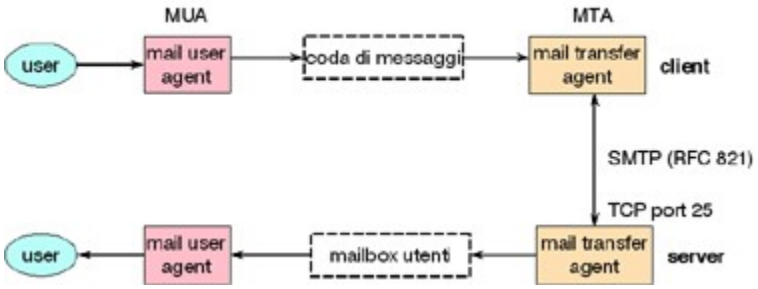
[SMTP è specificato nel RFC 821]
[POP3è specificato nel RFC 1225]

Esiste la definizione di due protocolli per la posta elettronica:

- **SMTP** (*Simple Mail Transfer Protocol*) per il trasporto dei messaggi: dal MUA di origine ad un MTA; fra vari MTA, da quello di partenza fino a quello di destinazione;
- **POP** 3 (*Post Office Protocol* versione 3) per la consegna di un messaggio da parte di un MTA al MUA di destinazione.

Il *Simple Mail Transfer Protocol* (SMTP) è probabilmente l'applicativo più importante del TCP/IP. Esso permette di inviare posta elettronica agli utenti della rete.

Ogni utente è identificato dalla sintassi 'Utente@Elaboratore' e non è richiesta alcuna autorizzazione per poter inviare un messaggio di posta elettronica. Il procedimento di invio avviene in *batch*, riprovando più volte sino a quando l'elaboratore remoto non diventa raggiungibile. L'utente remoto viene avvisato dell'arrivo di un nuovo messaggio. Recentemente sono stati introdotti altri protocolli più sofisticati, quali **IMAP** (*Interactive Mail Acces Protocol*, RFC 1064) e DMSP (*Distributed Mail System Protocol*, RFC 1056), il cui supporto però non è ancora molto diffuso nel *software* disponibile agli utenti.



Inoltre, non è detto che il primo MTA consegni i messagi direttamente all'MTA di destinazine. È possibile che le macchine siano configurate in modo da trasferire i messaggi attraverso un certo numero di *server* SMTP intermedi.

Se un *host*, tipicamente un PC, non è collegato direttamente ad Internet (ad esempio, nel caso di accesso remoto tramite un *Internet provider*), esso utilizza un *mail server* per inviare e ricevere messaggi di posta elettronica. POP3 consente di prelevare i messaggi di posta e memorizzarli sul PC locale, per poi poterli leggere (consultazione *off-line*). Un protocollo più sofisticato è IMAP (*Interactive Mail Access Protocol*). Esso, a differenza di POP3, consente all'utente di leggere i messaggi direttamente dal *server*, senza doverli quindi prelevare e memorizzare sul proprio PC (consultazione *on-line*).

Infine, vanno citate due significative estensioni di funzionalità della posta elettronica:

- possibilità di inviare messaggi di posta contenenti informazioni di qualunque tipo (per esempio programmi eseguibili, immagini, filmati, suoni, eccetera) attraverso lo standard ***MIME*** (*Multipurpose Internet Mail Extension*, RFC 1341 e 1521);
- possibilità di inviare messaggi corredati di firma digitale o crittografati, attraverso lo standard in via di definizione **S/*MIME*** (*Secure/MIME*, RFC 1847).

HTTP

[HTTP 1.0 è specificato nel RFC 1945]
[HTTP 1.1 è specificato nel RFC 2616]

Il protocollo *Hypertext Transfer Protocol* (**HTTP**) è la base del *World Wide Web* (**WWW**). Un *Web client*, chiamato comunemente *browser*, comunica con un *Web server* usando una o più connessioni TCP. La ***well-known port*** **per indirizzare sul *server* il servizio è la 80**.

HTTP è il protocollo usato dal *client* e dal *server* per lo scambio di messaggi attraverso connessioni TCP. I documenti che il *server* invia al *client* possono essere immagini, *file* di testo o documenti di tipo HTML (*HyperText Markup Language*).

HTTP è un protocollo semplice: il *client* stabilisce una connessione TCP con il *server* sulla porta 80, fa una richiesta e aspetta il documento di risposta, che in genere contiene puntatori (*hypertext link*) ad altri *file*; questi possono risiedere sullo stesso *server* o su altri. Il *server* indica la fine del documento chiudendo la connessione.

Per poter richiedere un certo servizio da un determinato *host* della rete, si usa un **URL** (*Uniform Resource Locator*). Il formato per URL è:

```
scheme://hostname[:port]/directory/file
```

dove *scheme* individua il tipo di servizio richiesto, *hostname* è il nome della macchina *server*, segue la *directory* di appartenenza e il **nome** del *file*.

Esempi di schemi sono:

- http: per un *file* su *Web server* (protocollo HTTP);
- ftp: per un *file* su ftp *server* (protocollo FTP);
- telnet: per una connessione su un servizio basato su telnet.

Esempi di URL sono:

- http://info.cern.ch/;
- http://www.ietf.org/;
- ftp://ftp.nis.garr.it/.

Quando un *client* effettua una richiesta invia diverse informazioni:

- il metodo (cioè il comando) che si chiede al *server* di eseguire;
- il numero di versione del protocollo HTTP in uso;
- l'indicazione dell'oggetto al quale applicare il comando;
- varie altre informazioni, fra cui:
  - il tipo di *client*;
  - i tipi di dati che il *client* può accettare.

I metodi definiti in HTTP sono:

- *GET*: richiesta di ricevere un oggetto dal *server*;
- *HEAD*: richiesta di ricevere la sola parte *head* di una pagina HTML;
- *PUT*: richiesta di mandare un oggetto al *server*;
- *POST*: richiesta di appendere sul *server* un oggetto a un altro;
- *DELETE*: richiesta di cancellare sul *server* un oggetto;
- *LINK* e *UNLINK*: richieste di stabilire o eliminare collegamenti fra oggetti del *server*.

In proposito, si noti che il metodo che si usa più frequentemente è *GET*; *POST* ha il suo più significativo utilizzo in relazione all'invio di dati tramite form; *HEAD* si usa quando il *client* vuole avere delle informazioni per decidere se richiedere o no la pagina; *PUT*, *DELETE*, *LINK*, *UNLINK* non sono di norma disponibili per un *client*, tranne che in quei casi in cui l'utente sia abilitato alla configurazione remota (via *Web*) del *server Web*.

Ad esempio, supponiamo che nel *file* HTML visualizzato sul *client* vi sia un'ancora:

```
<A HREF="http://pippo.net/pluto/minnie/index.html"> ..... </A>
```

e che l'utente attivi tale link. A tal punto il *client*:

- chiede al DNS l'indirizzo IP di pippo.net;
- apre una connessione con pippo.net, porta 80;
- invia la sua richiesta.

Essa è costituita da un insieme di comandi (uno per ogni linea di testo) terminati con una linea vuota:

- ***GET* /pluto/minnie/index.html HTTP/1.0**: metodo, URL e versione protocollo;
- ***User-agent*: Mozilla/3.0**: tipo del *client*;
- ***Host*: 160.10.5.43**: indirizzo IP del *client*;
- ***Accept: text/html***: *client* accetta pagine HTML;
- ***Accept: image/gif***: *client* accetta immagini;

- ***Accept: application/octet-stream***: *client* accetta *file* binari qualunque;
- ***If-modified-since*: data e ora**: inviare il documento solo se è più recente della data specificata.

La risposta del *server* è articolata in più parti, poiché il *client* non può sapere in che modo dovrà gestire le informazioni che gli arriveranno. Si consideri ad esempio il fatto che non si può mostrare sotto forma di testo un'immagine o un *file* sonoro, e dunque si deve informare il *client* sulla natura dei dati che gli arriveranno prima di iniziare a spedirglieli.

Per questo motivo la risposta consiste di 3 parti:

- una riga di stato, che indica quale esito ha avuto la richiesta (tutto ok, errore, eccetera);
- delle metainformazioni che descrivono la natura delle informazioni che seguono;
- le informazioni vere e proprie (ossia, l'oggetto richiesto).

La riga di stato, a sua volta, consiste di tre parti:

- Versione del protocollo HTTP;
- Codice numerico di stato;
- Specifica testuale dello stato.

Tipici codici di stato sono:

Esito	Codice numerico	Specifica testuale
Tutto ok	200	*OK*
Documento spostato	301	*Moved permanently*
Richiesta di autenticazione	401	*Unauthorized*
Richiesta di pagamento	402	*Payment required*
Accesso vietato	403	*Forbidden*
Documento non esistente	404	*Not found*
Errore nel *server*	500	*Server error*
SYST	*server returns system type*	*OK*

Dunque, ad esempio, si potrà avere:

```
HTTP/1.0 200 OK
```

Le metainformazioni comunicano al *client* ciò che deve sapere per poter gestire correttamente i dati che riceverà. Sono elencate in linee di testo successive alla riga di stato e terminano con una linea vuota. Tipiche metainformazioni sono:

- ***Server*: ...** : identifica il tipo di *server*;
- ***Date*: ...** : data e ora della risposta;
- ***Content-type*: ...** : tipo dell'oggetto inviato;
- ***Content-length*: ...** : numero di *byte* dell'oggetto inviato;
- ***Content-language*: ...** : linguaggio delle informazioni;
- ***Last-modified*: ...** : data e ora di ultima modifica;
- ***Content-encoding*: ...** : tipo di decodifica per ottenere il *content*;

Il *Content-type* si specifica usando lo standard *MIME* (*Multipurpose Internet Mail Exchange*), nato originariamente per estendere la funzionalità della posta elettronica.

Un tipo *MIME* è specificato da una coppia:

MIME type/MIME subtype

Vari tipi *MIME* sono definiti, e molti altri continuano ad aggiungersi. I più comuni sono:

Type/Subtype	Estensione	Tipologia delle informazioni
text/plain	.txt, .java	testo
text/html	.html, .htm	pagine HTML
image/gif	.gif	immagini gif
image/jpeg	.jpeg, .jpg	immagini jpeg
audio/basic	.au	suoni
video/mpeg	.mpeg	filmati
application/octet-stream	.class, .cla, .exe	programmi eseguibili
application/postscript	.ps	documenti *Postscript*
x-world/x-vrml	.vrml, .wrl	scenari 3D

Il *server* viene configurato associando alle varie estensioni i corrispondenti tipi *MIME*. Quando gli viene chiesto un *file*, deduce dall'estensione e dalla propria configurazione il tipo *MIME* che deve comunicare al *client*.

Se la corrispondenza non è nota, si usa quella di *default* (tipicamente *text/html*), il che può causare errori in fase di visualizzazione. Anche la configurazione del *client* (in merito alle applicazioni *helper*) si fa sulla base dei tipi *MIME*. Tornando al nostro esempio, una richiesta del *client* quale:

```
GET /products/toasters/index.html HTTP/1.0
User-agent: Mozilla/3.0
eccetera
```

riceverà come risposta dal *server* (supponendo che non ci siano errori) le metainformazioni, poi una riga vuota e quindi il contenuto del documento (in questo caso una pagina HTML costituita di 6528 *byte*):

```
HTTP/1.0 200 OK
Server: NCSA/1.4
Date: Tue, july 4, 1996 19:17:05 GMT
Content-type: text/html
Content-length: 6528
Content-language: en
Last-modified: Mon, july 3, 1996 15:05:35 GMT
_____________________________________<----- notare la riga vuota
<HTML>
<HEAD>
...
<TITLE>...</TITLE>
...
</HEAD>
<BODY>
...
</BODY>
</HTML>
```

Sulla base di quanto detto finora, si possono fare alcune osservazioni:

- il protocollo HTTP è molto semplice, essendo basato su interazioni che prevedono esclusivamente l'invio di

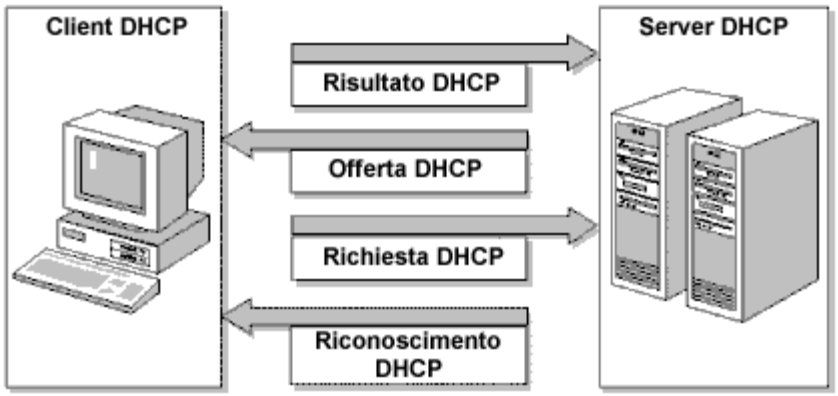
una singola richiesta e la ricezione della relativa risposta;
- questa semplicità è insieme un punto di forza e di debolezza:
  - di forza perché è facilissimo, attraverso la definizione di nuovi tipi *MIME* e di corrispondenti funzioni sui *client*, estendere le tipologie di informazioni gestibili (il *server* non entra nel merito di ciò che contengono i *file*: si limita a consegnare i dati che gli vengono richiesti, senza preoccuparsi della loro semantica);
  - di debolezza perché queste estensioni di funzionalità talvolta mal si adattano alla concezione originaria (*stateless*) del protocollo, come ad esempio è il caso delle transazioni commerciali.

Dynamic Host Configuration Protocol (DHCP)

DHCP (*Dynamic Host Configuration Protocol*) è standard, secondo quanto definito dalle specifiche RFC 2131 e 2132 IETF. DHCP è in grado di configurare automaticamente un *host* durante il suo avvio su una rete TCP/IP, e può modificare le impostazioni mentre l'*host* è connesso. Ciò consente di memorizzare tutti gli indirizzi IP disponibili insieme alle relative informazioni di configurazione, quali le ***subnet*** *mask*, i ***gateway*** e gli indirizzi dei *server* DNS, su un *database* centralizzato.

Il protocollo DHCP si basa sul protocollo *BOOTStrap Protocol* (BOOTP), standard Internet (RFC 951 e 1084), che consente l'assegnazione dinamica degli indirizzi IP oltre al riavvio a distanza di *workstation* prive di disco. DHCP supporta l'assegnazione dinamica degli indirizzi IP e fornisce inoltre tutti i dati di configurazione richiesti dai protocolli TCP/IP, più dati aggiuntivi richiesti per *server* specifici.

Come osservato, ciò semplifica i compiti dell'amministratore di rete, al quale adesso sarà sufficiente configurare manualmente solo un *computer*: il *server* DHCP. Quando viene connesso un nuovo *host* sul segmento di rete servito dal *server* DHCP, oppure quando viene riacceso un *host* esistente, il *computer* richiede un indirizzo IP univoco e il *server* DHCP ne assegna uno dal *pool* degli indirizzi IP disponibili.



Questo processo comprende quattro fasi: il *client* DHCP richiede un indirizzo IP (Risultato DHCP), il *server* DHCP offre un indirizzo al *client* DHCP (Offerta DHCP), il *client* DHCP accetta l'offerta e richiede l'indirizzo (Richiesta DHCP), quindi il *server* DHCP assegna ufficialmente l'indirizzo al *client* DHCP (Riconoscimento DHCP).

Server DHCP

Il *Server* DHCP, attraverso uno strumento di gestione consente agli amministratori di rete di definire le configurazioni dei *client* DHCP. Il *server* DHCP comprende inoltre un *database* per la gestione dell'assegnazione degli indirizzi IP e di altri parametri di configurazione.

I parametri di configurazione **TCP** /IP che possono essere assegnati dal *server* DHCP includono:

- Indirizzi IP di ciascuna scheda di rete dei *computer client*.
- ***Subnet*** *mask*, che vengono utilizzate per identificare la parte IP della rete dalla parte *host* dell'indirizzo IP.
- ***Gateway*** predefiniti (*router*), che vengono utilizzati per collegare un singolo segmento della rete agli altri segmenti.
- Parametri di configurazione aggiuntivi che possono essere assegnati ai *client* DHCP, quali ad esempio gli indirizzi IP per i *server* **DNS** o *Windows Internet Naming Service* (*WINS*) che un *client* potrebbe utilizzare.

Client DHCP

Molte piattaforme economiche standard sono in grado di funzionare come *client* DHCP, secondo quanto stabilito dalla specifica RFC 2132 aggiornata.

Le quattro fasi necessarie a un *client* DHCP per ottenere un ***lease*** da un *server* DHCP vengono avviate automaticamente quando il *computer* viene avviato per la prima volta. La configurazione *client* minima richiesta da DHCP può essere abilitata velocemente durante l'installazione del *client* oppure mediante l'esecuzione manuale di una breve reimpostazione delle proprietà TCP/IP del *client*.

Oltre a rendere disponibili le informazioni di configurazione mediante DHCP, gli amministratori di rete sono in grado di sovrascrivere le impostazioni dinamiche mediante impostazioni manuali. Ogni informazione inserita manualmente nella configurazione TCP/IP di un *client* sovrascrive le impostazioni dinamiche.

Per l'esecuzione del proprio lavoro, i protocolli **BOOTP** e DHCP si basano sui *broadcast* di rete. I *router*, in ambienti di *routing* normale, non inoltrano automaticamente *broadcast* da un'interfaccia a un'altra, pertanto, è necessario utilizzare un agente di inoltro che trasmetta tale comunicazione. Un agente di inoltro DHCP può essere un *router* oppure un *computer host* configurato per ascoltare i messaggi ***broadcast*** DHCP/BOOTP e indirizzarli verso *server* DHCP specifici. L'utilizzo degli agenti di inoltro elimina la necessità di disporre di un *server* DHCP fisico su ogni segmento della rete. Gli agenti di inoltro non soltanto indirizzano le richieste dei *client* DHCP locali ai *server* DHCP remoti, ma restituiscono le risposte dei *server* DHCP remoti ai *client* DHCP.

I *router* conformi alla specifica **RFC** 2131 (che sostituisce la RFC 1542) contengono agenti di inoltro che consentono di inoltrare pacchetti DHCP.

Amministrazione DHCP

Ambiti DHCP

Un ambito DHCP è un raggruppamento amministrativo che identifica gli intervalli consecutivi completi di indirizzi IP possibili per tutti i *client* DHCP su una *subnet* fisica. Gli ambiti definiscono una *subnet* logica destinata a essere fornita di servizi DHCP e consentono al *server* di identificare i parametri di configurazione che vengono assegnati a tutti i *client* DHCP sulla *subnet*. È necessario definire un ambito prima che i *client* DHCP siano in grado di utilizzare il *server* DHCP per la configurazione TCP/IP dinamica.

Pool di indirizzi

Una volta definito un ambito DHCP e applicati gli intervalli di esclusione, gli indirizzi rimanenti formano all'interno dell'ambito ciò che viene chiamato un *pool* di indirizzi disponibili. Gli indirizzi del *pool* possono quindi venire assegnati dinamicamente ai *client* DHCP sulla rete.

Intervalli di esclusione

Un intervallo di esclusione rappresenta una sequenza limitata di indirizzi IP all'interno di un intervallo di ambito che non devono essere assegnati dal servizio DHCP. Se utilizzati, gli intervalli di esclusione agiscono in modo che ai *client*

del *server* DHCP non rilasciato offerto alcun indirizzo contenuto in un determinato intervallo di esclusione.

Prenotazioni

Le prenotazioni consentono al *server* DHCP di assegnare *lease* di indirizzi permanenti. Se utilizzate, le prenotazioni garantiscono la capacità di utilizzare sempre lo stesso indirizzo IP a una periferica *hardware* specifica sulla *subnet*.

Ambiti estesi

È possibile utilizzare una funzionalità amministrativa inclusa nello strumento *Manager DHCP Microsoft* per creare un numero di ambiti separati, raggruppati in una singola entità denominata ambito esteso. Gli ambiti estesi sono utili per risolvere diversi problemi relativi al servizio DHCP.

Lease

Un *lease* rappresenta la durata dell'utilizzo di un indirizzo IP assegnato specificata da un *server* DHCP a un *client*. Quando un *lease* viene rilasciato a un *client*, viene descritto come attivo. A metà della durata del *lease*, è necessario che il *client* rinnovi l'assegnazione del *lease* di indirizzo con il *server*. La durata dei *lease* influisce sulla frequenza delle richieste di rinnovo dei *client* al *server* DHCP relative ai *lease* che sono stati loro assegnati.

Opzioni DHCP

Le opzioni DHCP rappresentano altri parametri di configurazione *client* che un *server* DHCP è in grado di assegnare durante la distribuzione di *lease* ai *client* DHCP. Ad esempio, gli indirizzi IP per un *router* o per un *gateway* predefinito, per i *server WINS* o per i *server* DNS vengono normalmente forniti per un ambito singolo oppure globalmente per tutti gli ambiti gestiti dal *server* DHCP. Molte opzioni DHCP sono predefinite secondo la specifica RFC 2132.

Bibliografia

Introduzione

Libri

J. F. Kurose, K. W. Ross; *Internet e reti di calcolatori;* 2001McGraw-Hill
D. Comer; *Internet e reti di calcolatori;* 2000Addison Wesley Longman Italia
A. S. Tanenbaum; *Reti di computer - Terza edizione;* 1998UTET/Prentice Hall
W. Stallings; *Local and Metropolitan Area Networks - Sesta edizione;* 2000Prentice Hall
W. R. Stevens; *TCP/IP Illustrated, Volume 1: The Protocols;* 1994Addison-Wesley

Glossario

10Base2: standard IEEE/ISO 802.3 per la trasmissione a 10 Mb/s su **cavo coassiale** RG58 da 50 W. Questo tipo di mezzo trasmissivo è spesso indicato come *ThinWire cable* o *thinnet cable*. Un segmento 10Base2 può essere lungo fino a 185 metri.

10Base5: standard IEEE/ISO 802.3 per la trasmissione a 10 Mb/s sul **cavo coassiale** definito dalla specifica originale ***Ethernet*** *thick cable* a 50 W. Un segmento 10Base5 può essere lungo fino a 500 metri.

10BaseF: standard IEEE/ISO 802.3 che racchiude tre standard per la trasmissione a 10 Mb/s su fibra ottica: **10BaseFP** , **10BaseFB** , **10BaseFL** .

10BaseFB: standard IEEE/ISO 802.3 per la trasmissione su fibra ottica che prevede l'uso di trasmissione **sincrona** per la realizzazione di dorsali in fibra ottica (FB significa *Fiber Backbone*) fra ***hub*** . Un segmento 10BaseFB può avere una lunghezza massima di 2000 metri.

10BaseFL: standard IEEE/ISO 802.3 a 10 Mb/s che prevede l'uso di segmenti in fibra ottica (FL: *Fiber Link*) per la connessione di stazioni e ***hub*** . 10BaseFL è compatibile con lo standard FOIRL, ma può avere una lunghezza massima di 2000 metri.

10BaseFP: standard IEEE/ISO 802.3 per la trasmissione a 10 Mb/s su fibra ottica che prevede l'uso di *star* ottiche passive. Un segmento che interconnette un **MAU** ad una *star* passiva può avere una lunghezza massima di 500 metri.

10BaseT: standard IEEE/ISO 802.3 per la trasmissione a 10 Mb/s su un cavo **UTP** (*Unshielded Twisted Pair*) da 24 AWG. Un segmento 10BaseT può ammettere una distanza massima di 100 metri.

100BaseT: standard del gruppo IEEE 802.3, per una versione della rete locale ***Ethernet*** /IEEE 802.3 in grado di operare a 100 Mb/s.

ACK (acknowledgement): risposta inviata per indicare una corretta ricezione di un messaggio; gli *acknowledgement* possono essere presenti a vari livelli del modello di riferimento **OSI** (si veda anche *confirmed service*).

ADDRESS MASK: maschera di 32 bit usata in TCP/IP per individuare l' **indirizzo** della sottorete logica **IP** .

ANSI (American National Standards Institute): organismo standardizzatore operante negli USA.

ARP (Address Resolution Protocol): **protocollo** utilizzato per ottenere l' **indirizzo** specifico (conforme a quanto previsto nella sottorete a cui si è connessi) di una macchina, conoscendone solo l' **indirizzo IP** .

AS (Autonomous System): insieme di reti nell'architettura TCP/IP gestite da un'unica **entità** amministrativa; i ***router*** che le collegano utilizzano un **protocollo di *routing*** univoco.

ASCII: *American Standard Code for Information Interexchange*. Sistema di codifica standard utilizzato largamente nel settore dell'informatica. Mediante parole di 7 bit (8 se si considera anche il bit di **parità**), vengono codificati i simboli alfanumerici e alcuni caratteri di controllo per la trasmissione delle informazioni.

ASINCRONA: tipo di trasmissione dati, a volte chiamata trasmissione ***start-stop*** , in cui la sincronizzazione tra trasmettitore e ricevitore viene ripristinata tramite uno o più bit di *start* all'inizio di ogni carattere.

ATTENUAZIONE: processo di riduzione della potenza di un segnale in seguito all'attraversamento di un mezzo trasmissivo. Risulta proporzionale alla distanza e spesso limita la distanza massima alla quale può essere trasmesso un segnale in maniera da garantirne la corretta ricezione ed il riconoscimento.

AUTOCOMMUTATORI: sono gli apparati che svolgono la funzione di **commutazione** in una rete di Telecomunicazioni. Il nome deriva dal fatto che ai primordi della telefonia la **commutazione** veniva realizzata manualmente da operatori umani che ricevevano dal chiamante l'indicazione della linea da connettere. Successivamente, utilizzando dispositivi elettromeccanici denominati selettori, la funzione di **commutazione** poté essere svincolata dalla presenza di un operatore e resa completamente automatica (**commutazione** automatica analogica) inviando verso tali dispositivi degli impulsi elettrici corrispondenti alle cifre di selezione.

AUTOCOMMUTATORI NUMERICI: sono **autocommutatori** realizzati con tecnologia elettronica in grado di commutare segnali di tipo PCM. Il loro funzionamento si basa sulla possibilità di trasferire trasparentemente dall'ingresso all'uscita dell' **autocommutatore** le parole binarie (8 bit) derivanti dalla codifica del segnale vocale.

AUI CABLE (Attachment Unit Interface cable): cavo di interconnessione tra l'interfaccia ***Ethernet*** ed il ***transceiver*** , comunemente chiamato cavo *drop*.

BACK-OFF: procedura con cui si ritenta una trasmissione in un **MAC** CSMA/CD.

BACKBONE: dorsale di rete. Indica l'insieme dei nodi e dei ***link*** di interconnessione fra questi, preposti alle funzionalità di *switching*/ ***routing*** del traffico in una rete di comunicazioni.

BACKBONE COLLASSATO: dorsale di rete collassata in un centro stella realizzato mediante un **concentratore** o uno ***switch*** .

BANDA: intervallo di frequenze trasmissibili da un **canale** ; termine anche utilizzato per indicare l'intervallo di frequenze occupato da una trasmissione.

BANDWIDTH: larghezza di **banda** .

BAUD: numero di simboli al secondo; i simboli possono essere binari, nel qual caso la velocità in baud coincide con la velocità in bit al secondo, oppure si possono utilizzare codifiche o modulazioni più complesse per rappresentare più bit con un solo simbolo.

BER (Bit Error Ratio): esprime una misura della qualità trasmissiva (per esempio, 10-7 indica 1 bit errato mediamente ogni 10.000.000).

BILANCIATA: tecnica di trasmissione differenziale di segnali elettrici su coppie simmetriche.

BIT STUFFING: tecnica usata per delimitare le trame in modo non ambiguo e consentire la trasmissione di dati binari su una linea trasmissiva **sincrona** .

BIT TIME: tempo dedicato alla trasmissione di un singolo bit; pari al reciproco della velocità trasmissiva espressa in b/s.

BPS (bit per second): bit al secondo, anche abbreviato b/s; misura della velocità di una trasmissione dati.

BRIDGE: dispositivo utilizzato per il supporto delle comunicazioni da **LAN** a **LAN** . Opera l'interconnessione di reti locali, anche eterogenee, a livello **MAC** con riferimento alla pila dei protocolli di reti locali ed è in grado di separare i traffici che interessano i singoli spezzoni di rete (segmenti).

BROADCAST: trasmissione dati diretta da una sorgente alla totalità dei terminali di una ben definita rete.

BROUTER: apparato in grado di operare sia come ***bridge*** che come ***router*** in funzione dei protocolli e della configurazione.

BROWSER: programma utilizzato per esplorare e navigare su un *file system*, oppure su un insieme di risorse fisiche e logiche legate alla gestione di rete, oppure sui *computer* collegati in **Internet** , su una base di dati, o altro.

BSC (Binary Synchronous Communication Protocol): **protocollo** implementato in ambiente IBM per comunicazioni *half-duplex* a livello ***Data Link*** , orientato al carattere.

BURSTINESS: nell'ambito di una rete dati, caratterizza il rapporto fra la **banda** di picco e la **banda** media. Può assumere valori anche superiori a 100 per le **LAN** , assume valore 1 nel caso di applicazioni voce/video senza compressione o con compressione a rapporto fisso.

BUFFER: area di memoria temporanea spesso utilizzata per compensare differenze di velocità tra trasmettitore e ricevitore.

BUS: topologia per reti locali in cui le stazioni sono collegate ad un singolo mezzo trasmissivo di tipo ***broadcast*** .

CABLAGGIO ORIZZONTALE: quella porzione di **cablaggio strutturato** che serve a collegare i posti di lavoro con gli armadi di piano.

CABLAGGIO STRUTTURATO: infrastruttura per la trasmissione di segnali in ambito locale, realizzato contestualmente alla costruzione o ristrutturazione organica di un edificio, in conformità ai vigenti standard internazionali.

CABLAGGIO VERTICALE: quella porzione di **cablaggio strutturato** che realizza i collegamenti di dorsale.

CANALE: parte di un sistema di comunicazione che connette una sorgente ad una o più destinazioni. Chiamato anche circuito, linea, ***link*** o *path*.

CAPACITÀ DI CANALE: termine che esprime la massima velocità di trasmissione che può essere utilizzata su un **canale** .

CAVO COASSIALE: tipo di cavo elettrico in cui un conduttore centrale è ricoperto da un isolante e poi circondato da uno schermo conduttore cilindrico il cui asse di simmetria coincide col conduttore centrale, da cui il termine coassiale.

CDA (Collegamento Diretto Analogico): servizio di interconnessione fornito dal gestore di una rete pubblica di telecomunicazioni. Consiste nel realizzare fra due sedi dell'utente una connettività analogica permanente adatta al trasferimento di un segnale caratterizzato da una dinamica in ampiezza e frequenza prestabilite.

CDM (Code Division Multiplexing): tecnica per trasmettere più canali diversi su un unico mezzo trasmissivo utilizzando codici diversi.

CDMA (Code Division Multiple Access): condivisione di un unico mezzo trasmissivo da parte di più canali tramite tecnica **CDM** .

CDN (Circuito Diretto Numerico): è un collegamento fisico permanente ***full duplex*** , realizzato tra due sedi del cliente mediante apparati **DCE** che rappresentano la terminazione del collegamento, installati in entrambe le sedi e mediante apparati della rete trasmissiva pubblica. Equivale ad una linea diretta dedicata tra le due sedi. Viene fornito con diverse opzioni di velocità: da 2400 bit/s fino a 2048 kbit/s (volgarmente detto 2Mbit/s), per passi discreti (2.4, 4.8, 9.6, 14.4, 19.2, 48 , 64, Nx64 kbit/s, con N variabile da 2 a 32). La rete trasmissiva che consente di fornire tale servizio è caratterizzata da bassi tassi di errore, alta disponibilità e possibilità di gestione da remoto; la trasmissione dati tra gli apparati disposti agli estremi del CDN è trasparente temporalmente (ritardo costante) e la rete è trasparente ai codici utilizzati.

CDN-RED (Ripartitore Elettronico Digitale per Collegamenti Diretti Numerici): utilizzato come permutatore della rete trasmissiva del gestore pubblico.

CHECKSUM: sequenza di bit calcolata a partire da una sequenza di bit (costituenti l'informazione da proteggere da errori) e da un algoritmo di calcolo prestabilito stabilito (vedi anche **CRC**).

CIRCUIT SWITCHING: modo di trasferimento a circuito. Le informazioni vengono trasferite attraverso la rete su una connessione fisica costruita su richiesta (servizio commutato) o in maniera permanente (servizio permutato) che garantisce la trasparenza temporale.

CLAIM TOKEN: processo di inizializzazione e generazione di un nuovo ***token*** ; la **stazione** che vince questo processo emette il nuovo ***token*** .

CLNP (Connectionless Network Protocol): **protocollo ISO** di livello *Network*, non connesso, documentato in ISO 8473.

CLNS (ConnectionLess-mode Network Service): servizio di livello *Network* in cui i pacchetti sono trasmessi da un **protocollo** non connesso (detto anche **protocollo *datagram***); l'arrivo del **pacchetto** non è garantito, e le eventuali procedure di correzione degli errori devono essere implementate dai livelli superiori.

COLLISION DOMAIN: porzione di una rete CSMA/CD nella quale ha luogo una **collisione** se due o più **entità MAC** trasmettono contemporaneamente; le **entità MAC** separate da ripetitori sono nello stesso *collision domain*, quelle separate da ***bridge*** , ***router*** e ***gateway*** no.

COLLISION HANDLER: circuito di gestione delle collisioni.

COLLISIONE: trasmissione simultanea di due o più stazioni su un mezzo trasmissivo condiviso.

COMMUTAZIONE: è la funzione svolta dai nodi di una rete di telecomunicazioni preposta alla fornitura di servizi commutati. Su ciascuna unità informativa ricevuta da una linea fisica entrante, il **nodo** decide quale debba essere la linea di uscita sulla quale far proseguire l'informazione e quindi la trasferisce fisicamente dall'interfaccia di ingresso all'interfaccia di uscita, modificando eventualmente l'etichetta e la coda dell'unità informativa.

COMMUTAZIONE DI CIRCUITO: si veda ***circuit switching*** .

COMMUTAZIONE DI PACCHETTO: si veda ***packet switching*** .

CONCENTRATORE: nelle reti locali cablate a stella l'apparato che funge da centro stella.

CONNECTION-MODE SERVICE: servizio affidabile realizzato tipicamente tramite un **protocollo** connesso.

CONNECTIONLESS-MODE SERVICE: servizio realizzato tramite un **protocollo** non connesso che non garantisce la consegna delle **PDU** .

CONS (Connection-mode Network Service): servizio affidabile di livello *Network* in cui le **PDU** sono scambiate tramite un **protocollo** connesso.

CONTROLLO DI ERRORE: tecnica volta al riconoscimento ed al recupero di errori di trasmissione sui bit dei dati.

CONTROLLO DI FLUSSO: tecnica che tende a evitare o a risolvere congestioni di nodi sospendendo o riducendo l'immissione di nuovi dati sui mezzi trasmissivi.

CONTROLLO DI SEQUENZA: tecnica volta a far si che i dati vengano ricevuti nello stesso ordine in cui sono stati trasmessi.

CRC (Cyclic Redundancy Check): algoritmo matematico che calcola un valore numerico sulla base di una sequenza di bit (blocco di dati). In ricezione il valore numerico ricevuto viene confrontato con quello ricalcolato in base ai bit informativi ricevuti e, in caso di discordanza si attuano procedure per la **ritrasmissione** del blocco errato.

CSMA-CD (Carrier Sense Multiple Access with Collision Detection): tecnica di controllo dell'accesso ad un mezzo di trasmissione condiviso, utilizzata nell'ambito delle reti locali (es. ***Ethernet***). Ogni **stazione** collegata alla **LAN** , prima di trasmettere, ascolta l'attività sul mezzo trasmissivo e, se questo è libero, inizia a trasmettere. Durante la trasmissione ascolta ciò che accade sul mezzo trasmissivo ed è in grado di rivelare fenomeni di **collisione** , in base al cambiamento della tensione elettrica sul mezzo. Rivelata la **collisione** , interrompe la trasmissione e la ritenta successivamente.

CUT-THROUGH: metodo di **commutazione** in cui la **ritrasmissione** di un **pacchetto** in un **nodo** inizia mentre è ancora in corso la sua ricezione.

DATA LINK: secondo livello del modello di riferimento **OSI** ; si occupa della trasmissione di trame tra nodi fisicamente adiacenti.

DATAGRAM: pacchetti trasmessi tramite un **protocollo** non connesso.

DATAGRAM SERVICE: si veda ***connectionless-mode service*** .

dB (decibel): misura della potenza di un segnale relativamente ad un altro segnale; il valore in decibel viene calcolato come 10 volte il logaritmo del rapporto fra le potenze dei due segnali, oppure come 20 volte il logaritmo del rapporto fra le ampiezze (tensioni o correnti).

DCE (Data Communication Equipment): definizione generica di apparato che permette il collegamento di un **DTE** (terminale) ad una rete.

DECnet: nome originale dell'architettura di rete della *Digital Equipment Corp*. ed ora parte della più generale DNA (*Digital Network Architecture*).

Distance vector: algoritmo adattativo e distribuito per il calcolo delle tabelle di instradamento basato su un processo iterativo di scambio delle stesse tra ***router*** adiacenti; talvolta anche chiamato algoritmo di *Bellman-Ford*.

DNS (Domain Name System): sistema/servizio per l'associazione e la traduzione di indirizzi numerici **IP** in nomi logici alfanumerici mnemonici. È basato su una struttura gerarchica ad albero, ad ogni ramo del quale corrisponde un dominio.

DOPPINO: termine indicante una coppia di fili elettrici ritorti, spesso usato anche per indicare cavi a più coppie.

DROP CABLE: si veda **AUI *cable*** .

DS-0 (Digital Signal, Level 0): rappresenta, nella gerarchia trasmissiva Nordamericana un **canale** numerico a velocità 64 kbps ed è il mattone su cui si basano le gerarchie trasmissive USA ed europee.

DS-1 (Digital Signal, Level 1): nella gerarchia trasmissiva numerica Nordamericana rappresenta un segnale complesso ottenuto multiplando 24 canali di tipo **DS-0** . Viene spesso denominato T1 (1.5 Mbit/s).

DS-2 (Digital Signal, Level 2): nella gerarchia trasmissiva Nordamericana rappresenta il segnale complesso ottenuto multiplando 4 flussi di tipo T1 (6 Mbit/s).

DS-3 (Digital Signal, Level 3): segnale multiplo della gerarchia trasmissiva Nordamericana, ottenuto multiplando 28 flussi di tipo T1 ed aggiungendo dei bit di *overhead* per la supervisione delle funzioni trasmissive (44.736 Mbps).

DSAP (Destination Service Access Point): sigla usata per indicare l' **indirizzo** del destinatario nel modello di riferimento **OSI** .

DTE (Data Terminal Equipment): generica definizione indicante un apparato di utente con funzioni di terminale. Il termine è usato negli standard CCITT per indicare un dispositivo di elaborazione, come un *computer* o un terminale; i DTE si collegano normalmente ai **DCE** .

E1: segnale numerico a velocità 2.048 Mbit/s utilizzato nei sistemi trasmissivi europei; equivale alla multiplazione di 32 canali a 64 kbit/s ciascuno.

E3: segnale numerico a velocità 34.368 Mbps utilizzato nelle reti trasmissive europee ed equivalente alla multiplazione di 16 flussi di tipo **E1** .

EARLY TOKEN RELEASE: tecnica di rilascio anticipato del ***token*** utilizzato nella rete ***Token Ring*** a 16 Mb/s e in FDDI.

EIA (Electronic Industries Association): associazione di industrie elettroniche con attività nel campo della standardizzazione.

E-MAIL: abbreviazione di *electronic mail* (posta elettronica). È un sistema che consente la trasmissione e la ricezione su una rete informatica, di messaggi indirizzati secondo indirizzi a struttura standard. È una comunicazione di tipo asincrono perché anche in caso di indisponibilità dell'utente ricevitore, i messaggi vengono memorizzati nel *server* a cui questo utente riferisce.

END NODE: termine usato per indicare a un **nodo** che può agire solamente come una sorgente o destinazione finale di dati dell'utente e che non effettua le funzioni di ***routing*** .

ENTITÀ: nel modello di riferimento **OSI** , un elemento attivo in un dato livello.

ES (End System): termine **OSI** usato per indicare a un **nodo** che può agire solamente come una sorgente o destinazione finale di dati dell'utente e che non effettua le funzioni di ***routing*** .

ETHERNET: **protocollo** di trasmissione dati su rete locale. È caratterizzato da una velocità di trasmissione di 10 Mbit/s, con pacchetti trasmessi dalle stazioni interconnesse tramite un unico mezzo condiviso. La trasmissione, quindi, avviene con una tecnica **CSMA-CD** (*Carrier Sense Multiple Access - Collision Detection*) che prevede che le stazioni ascoltino se il mezzo trasmissivo è libero prima di iniziare a trasmettere e continuino ad ascoltare anche durante la trasmissione, per rilevare eventuali collisioni.

ETHERNET FULL-DUPLEX: utilizzo di due collegamenti ***Ethernet*** in parallelo (normalmente tra due ***bridge*** o tra due ***switch***) per permettere la trasmissione contemporanea nei due sensi.

ETHERNET SWITCH: dispositivo multiporta in grado di commutare trame ***Ethernet*** /IEEE 802.3.

ETHERNET SWITCHING: tecnica per realizzare reti locali ***Ethernet*** /IEEE 802.3 che utilizza ***Ethernet Switch*** per aumentare la capacità trasmissiva globale della rete.

ETSI: *European Telecommunications Standards Institute*.

FCS (Frame Check Sequence): parola di 16 (o 32 in alcuni casi) calcolata su una stringa di bit informativi allo scopo di rivelare gli errori contenuti in un **pacchetto** (vedi **CRC**).

FEC (Forward Error Correction): tecnica per rivelazione e autocorrezione di errori in stream dati numerici.

FLAG: nei protocolli di ***Data Link*** della famiglia **HDLC** (**HDLC** , *Frame Relay*, **PPP** , **LAP-B** , LAP-D) è un **ottetto** (01111110) che indica l'inizio e la fine di una **trama** .

FLOODING: algoritmo di ***routing*** non adattativo in cui un ***router*** propaga i pacchetti a tutti i ***router*** adiacenti.

FLOW CONTROL: si veda **controllo di flusso** .

FRAME: si veda **trama** .

FTP (File Transfer Protocol): **protocollo** definito nella RFC 959. Rappresenta un modo comune per il trasferimento di file tra due *computer* **Internet** . Impiega il servizio di trasporto offerto da **TCP** .

FTP (Foiled Twisted Pair): cavo, normalmente a quattro coppie, avente uno schermo globale realizzato con foglio di alluminio.

FULL DUPLEX: modalità di trasmissione bidirezionale simultanea.

GATEWAY: dispositivo usato per connettere due architetture di rete diverse mediante la conversione di alcuni protocolli applicativi dell'una in quelli omologhi dell'altra.

HALF DUPLEX: modalità di trasmissione bidirezionale non simultanea nei due sensi; in ogni istante la comunicazione è monodirezionale.

HDLC (High Level Data Link Control): ***link*** , standardizzato dall'ITU per le funzioni di ***Data Link*** nell'architettura **X.25** . Prevede l'impiego di linee punto punto e di linee punto multipunto. È derivato da **SDLC** e capostipite di una famiglia di protocolli a cui appartengono **LAP-B** , LAB-D, LAP-F e **LLC** .

HEADER: parte iniziale di una **PDU** che contiene informazioni di controllo.

HOP: attraversamento di un ***link*** , spesso usato come metrica a livello *Network*.

HOST: nell'architettura di rete TCP/IP, sinonimo di *end system*.

HTTP (HyperText Transport Protocol): il trasferimento di file multimediali su **Internet** necessita del **protocollo** HTTP per il *server* e per il *client*. Risulta il più diffuso **protocollo** applicativo per **Internet** , al momento e si basa sul servizio fornito da **TCP** .

HUB: apparato impiegato in reti locali di calcolatori avente funzioni di multiplatore statistico e **ripetitore** . Concentra in un punto fisico gli accessi alla **LAN** da parte delle diverse stazioni collegate, come se queste fossero connesse al **cavo coassiale** (a ***bus***).

Hz (Hertz): unità di misura della frequenza pari al numero di eventi al secondo.

ICMP (Internet Control Messagge Protocol): nell'architettura di rete TCP/IP rappresenta un **protocollo** ausiliario di livello *Network* utilizzato per funzioni di *neighbor greetings* e per riportare anomalie nell'instradamento dei pacchetti.

IEEE (Institute of Electrical and Electronics Engineers): associazione internazionale anche con attività nel campo della standardizzazione delle reti locali.

IEEE 802: il progetto 802 dell' **IEEE** è relativo alla definizione delle funzioni e dei protocolli per le reti locali. È logicamente suddiviso in diversi sottoprogetti:
IEEE 802.1, 802.2, 802.3, 802.5, ecc.
L'802.1 è lo standard che contiene le specifiche generali ed è composto da molte parti tra cui:
- 802.1 *Part A: Overview and Architecture*
- 802.1 *Part B: Addressing Internetworking and Network Management*
- 802.1 *Part D:* ***MAC Bridges***

IEEE 802 ha suddiviso il livello *Data-Link* in due sottolivelli:
- **LLC** : *Logical Link Control*
- **MAC** : *Media Access Control*

LLC è comune a tutte le **LAN** ed è l'interfaccia verso il livello *network* ed è specificato nell'802.2.
Per quanto riguarda il **MAC** , ogni **LAN** ha il suo standard, e comunque la funzione è quella di risolvere il problema della condivisione del mezzo trasmissivo (CSMA/CD specificato dall'802.3, ***Token Ring*** specificato dall'802.5, ecc).

IETF (Internet Engineering Task Force): organizzazione dell' **ISOC** che coordina il processo di standardizzazione e di sviluppo delle specifiche per il *networking* TCP/IP.

INCAPSULAMENTO: processo corrispondente al riempimento di una **trama** di livello i relativa ad un **protocollo** di livello i+1.

INDIRIZZO: stringa che identifica univocamente un' **entità** di rete.

INDIRIZZO INTERNET: **indirizzo** a 32 bit assegnato alle interfacce degli ***host*** e dei ***router*** che utilizzano l'architettura di rete TCP/IP; lo si scrive come quattro numeri decimali separati da punti.

INDIRIZZO MAC: **indirizzo** di livello ***Data Link*** , sottolivello **MAC** , usato nelle reti locali, tipicamente lungo 48 bit e

assegnato dal produttore della scheda di rete; lo si scrive come sei coppie di cifre esadecimali.

INTERNET: la più grande rete di calcolatori al mondo, basata sull'architettura di rete TCP/IP.

INTERNET PROTOCOL SUITE: l'architettura di rete normalmente nota con il nome di TCP/IP.

IP (Internet Protocol): nell'architettura di rete TCP/IP, il **protocollo** dati di livello *Network*.

ISDN (Integrated Services Digital Network o Rete Numerica Integrata nei Servizi): indica una prestazione della rete telefonica mediante la quale è possibile accedere da un unico punto fisico a servizi a circuito e a servizi a **pacchetto** .

ISO (International Standard Organization): principale organismo di standardizzazione mondiale di cui fanno parte gli organismi di standardizzazione nazionali quali l' **ANSI** per gli USA e l'UNINFO per l'Italia.

ISO/IEC DIS 11801: bozza di standard internazionale per il cablaggio degli edifici commerciali approvata nel mese di luglio 1994.

ISOC (Internet SOCiety): organizzazione per lo sviluppo della rete **Internet** e dell'architettura di rete TCP/IP.

ISP (Internet Service Provider): fornitore di servizio di accesso ad **Internet** . Generalmente, per gli utenti residenziali l'accesso è fornito mediante collegamento telefonico al **POP** del *provider*, mentre per categorie di utenti di tipo affari, il collegamento può essere su linea dedicata e collegamento diretto numerico fra la sede dell'utente ed il ***router*** del *provider*.

ITAPAC: nome commerciale della Rete Pubblica italiana (Telecom Italia) a **commutazione di pacchetto** a standard **X.25** . I servizi offerti da questa rete vengono indicati commercialmente con il nome di *Business Packet*.

ITU-T (International Telecommunications Union Telecommunications): ente normativo internazionale per il settore delle telecomunicazioni (la precedente denominazione di ITU era CCITT).

Jabber error: in IEEE 802.3 errore dovuto ad una **trama** la cui lunghezza eccede la massima consentita.

Jamming sequence: in IEEE 802.3 sequenza illegale di bit per segnalare un'avvenuta **collisione** .

LAN (Local Area Network): rete di calcolatori ad estensione locale/aziendale/dipartimentale, caratterizzata da mezzi trasmissivi condivisi, alta velocità trasmissiva, basso tasso di errore.

LAP (Link Access Procedure): termine generico che indica un **protocollo** della famiglia **HDLC** .

LAP-B (Link Access Protocol, Balanced mode): versione evoluta di **HDLC** operante in modalità **bilanciata** (punto punto fra **DTE** e **DCE**). Viene impiegato per le funzioni di livello ***Data Link*** in reti **X.25** all'interfaccia utente-rete.

LINK: **canale** tra due nodi.

LINK STATE: tecnica di calcolo delle tabelle di instradamento in cui un ***router*** comunica a tutti gli altri ***router*** della rete lo stato dei ***link*** a lui direttamente connessi tramite un **pacchetto** LSP.

LLC (Logical Link Control): nello standard **IEEE 802** il sottolivello superiore del livello ***Data Link*** ; **protocollo** appartenente alla famiglia **HDLC** .

LSB (Least Significant Bit): il bit meno significativo in una stringa ovvero in una sequenza di cifre binarie che rappresentano un numero secondo le regole dell'aritmetica posizionale.

MAC (Media Access Control): specifica **IEEE** per la parte bassa del livello ***Data Link*** , che definisce le regole per l'accesso ad un mezzo trasmissivo condiviso da più stazioni, in mutua esclusione. Il MAC prevede funzioni di indirizzamento ed un trasferimento connectionless fra stazioni.

MAC-BRIDGE: ***bridge*** che operano al sottolivello **MAC** del livello 2.

MAIN CROSSCONNECT (MC): locale tecnologico o armadio di distribuzione che è il centro stella del comprensorio ed è situato nell'edificio principale secondo la nomenclatura **EIA** /TIA 568.

MAN (Metropolitan Area Network): rete dati ad estensione cittadina.

MANCHESTER: codifica a livello fisico che combina i valori dei bit di dato con le transizioni di un segnale di *clock*; usata in ***Ethernet*** e ***Token Ring*** .

MASTER: nei sistemi trasmissivi **punto-multipunto** , la **stazione** che arbitra il **canale** mediante operazioni di *polling*.

MAU (Medium Attachment Unit): ***transceiver*** , cioè elemento di connessione al mezzo trasmissivo in ***Ethernet*** e IEEE 802.3.

MAU (Multistation Access Unit): nei sistemi trasmissivi **punto-multipunto** , la **stazione** che arbitra il **canale** mediante operazioni di *polling*.

MMF (Multi Mode Fiber): fibra multimodale, in cui il segnale luminoso si propaga secondo diversi cammini (o modi). Poiché tali cammini multipli hanno diverse lunghezze, i raggi interferiscono fra loro producenso interferenze fra simboli consecutivi ed **attenuazione** .

MODEM (Modulatore-DEModulatore): dispositivo per la trasmissione di dati digitali su canali trasmissivi analogici (tipicamente telefonici) tramite opportuna modulazione (ad esempio FSK, QAM, PSK).

MSB (Most Significant Bit): bit più significativo in una stringa, ovvero bit di peso maggiore nel caso di numero binario.

MULTICAST: trasmissione di informazioni da una sorgente ad un gruppo precostituito ed indirizzabile di ricevitori.

MULTIDROP o PUNTO-MULTIPUNTO: tipo di **canale** a cui sono connesse più stazioni di cui una ne arbitra l'utilizzo svolgendo le operazioni di ***master*** .

MULTIPLEXING: funzione realizzata in una rete di telecomunicazioni, a diversi livelli della pila **OSI** , necessaria veicolare su un unico **canale** trasmissivo flussi informativi appartenenti a diverse sorgenti.

NODI ADIACENTI: nodi che sono raggiungibili in un singolo ***hop*** .

NODO: termine usato in DNA (*Digital Network Architecture*) per riferirsi ad un dispositivo che contiene almeno una istanza del livello *Network* e dei sottostanti livelli ***Data Link*** e Fisico. È sinonimo del termine **OSI** *system*. In ambito Informatico il termine indica un generico sistema di elaborazione di una rete di *computer*.

NOTAZIONE PUNTATA: rappresentazione di un numero intero su 32 bit tramite quattro numeri decimali separati da punti ciascuno dei quali rappresenta il valore di un **ottetto** . Utilizzato per gli indirizzi TCP/IP.

NSAP (Network Service Access Point): **indirizzo** di livello *network* nell'architettura **OSI** .

NT1: apparato di terminazione della rete telefonica per il servizio **ISDN** . Tramite questo vengono realizzate tutte le funzioni di livello fisico (telealimentazione, codifica di linea, sincronizzazione, ...).

NT1-PLUS: oltre a svolgere le funzioni dell' **NT1** , consente di collegare alla rete apparecchi telefonici tradizionali, senza l'interposizione di adattatori di terminali (TA).

NULL MODEM: cavo di interfaccia seriale utilizzato per il collegamento diretto **DTE** - **DTE** , senza **modem** .

OSI (Open Systems Interconnection): standard internazionale, dell' **ISO** , descritto nel documento ISO 7498, per un modello di riferimento per l'interconnessione di sistemi; è organizzato in 7 livelli (*Physical*, ***Data Link*** , *Network*, *Transport*, *Session*, *Presentation*, *Application*), ciascuno dei quali si basa sui servizi forniti dal sottostante strato e fornisce a sua volta servizi allo strato sovrastante. Lo scopo è di realizzare sistemi aperti, capaci di far comunicare sistemi diversi fra loro.

OSPF (Open Shortest Path First): **protocollo** di tipo ***LINK STATE*** , utilizzato fra ***router*** nell'architettura TCP/IP per il calcolo delle tabelle di instradamento.

OTTETTO: termine **OSI** per indicare una stringa di 8 bit.

PABX (Private Automatic Branch eXchange): termine indicante un **nodo** di **commutazione** telefonica automatico privato.

PACCHETTO: nome informale per una *Protocol Data Unit*.

PACKET SWITCHING: tecnica di **commutazione** che prevede di raggruppare dati digitali in **PDU** e di inoltrare queste su mezzi trasmissivi condivisi dai nodi della rete.

PARITÀ: bit di controllo per il rilevamento di errori di trasmissione calcolato su ogni singola parola di n bit.

PDH (Plesiochronous Digital Hierarchy): (plesiocrono significa quasi sincrono) sistema di trasmissione numerica per reti geografiche, per il quale non esiste una sorgente di sincronizzazione che diffonde il suo cronosegnale a tutti gli apparati. Tutti gli apparati utilizzano un segnale di *clock* nominalmente uguale ma istantaneamente diverso in fase e frequenza. La gerarchia PDH è caratteristica anche dello schema di multiplazione, in base al quale, per estrarre un segnale tributario a 64 kbit/s da un flusso per es. 8 Mbit/s (costruito con 4 flussi a 2 Mbit/s, ciascuno dei quali è il multiplo di 32 segnali a 64 kbit/s) si opera come segue:
- si demultipla il segnale secondo il primo *step* da 1 flusso 8 a 4 flussi a 2 Mbit/s
- dal flusso a 2 Mbit/s di interesse si estrae il segnale tributario a 64 kbit/s
- si ricompongono i flussi a 2 e poi si ricostituisce il segnale ad 8 Mbit/s
Per l'Europa i sistemi trasmissivi plesiocroni sono indicati con **E1** (2048 kbit/s), **E3** (34 Mbit/s), eccetera; per il Nord America si utilizzano i sistemi T1 (1.5 Mbit/s), T3 (45 Mbit/s), eccetera.

PDN (Public Data Network): termine usato per indicare le reti pubbliche geografiche per trasmissione dati.

PDU (Protocol Data Unit): unità informativa caratteristica di un **protocollo** .

PHY (OSI Physical Layer): il livello fisico fornisce il supporto per la trasmissione fisica delle informazioni su un mezzo trasmissivo, tenendo conto anche delle procedure necessarie a richiedere il livello fisico. Infatti il livello fisico può essere permanente (connessione diretta) oppure commutato (occorre effettuare una chiamata).

PIGGYBACKING: tecnica utilizzata per trasportare il criterio di *acknowledge* nei pacchetti informativi.

POP (Post Office Protocol): è il **protocollo** utilizzato dal *client* di posta elettronica per richiedere al *server* associato i messaggi ricevuti.

PORTA, PORT: nell'architettura di rete TCP/IP, punto di accesso ai protocolli applicativi.

POTS (Plain Old Telephone Service): sigla usata per indicare la rete telefonica classica.

PPP (Point to Point Protocol): **protocollo** di livello 2 utilizzato per la trasmissione dati seriali in ambito **Internet** fra un *client* (tipicamente PC) ed un apparato di *networking* (***router***). È tipicamente impiegato per l'accesso ad **Internet** fra l'utente ed il *service provider*; viene anche impiegato per collegare fra loro due ***router*** attraverso rete pubblica geografica, utilizzando per esempio una connessione commutata telefonica, una connessione commutata numerica (**ISDN**) oppure una connessione numerica permanente.

Pps (packets per second): pacchetti al secondo, anche abbreviato p/s.

PREAMBOLO: sequenza di bit posta all'inizio di una **trama** per sincronizzare il *clock* del ricevitore, nel caso di trasmissione **asincrona** .

PROTOCOLLO: insieme di regole definite per consentire la comunicazione di dati fra elaboratori.

PROTOCOLLO DI ROUTING: **protocollo** utilizzato per lo scambio delle informazioni necessarie ad una rete di ***router*** ad istradare correttamente i pacchetti in rete e individuare opportunamente le ***route*** .

PROTOCOL TYPE: campo della **trama** ***Ethernet*** v.2.0 indicante il **protocollo** di livello superiore contenuto nel campo dati.

PSDN (Packet Switched Data Network): termine usato per indicare le reti a **commutazione di pacchetto** (in particolare quelle **X.25**).

PSN (Packet Switched Node): **nodo** a **commutazione di pacchetto** .

PSTN (Public Switched Telephone Network): rete telefonica pubblica.

RARP (Reverse Address Resolution Protocol): **protocollo** usato principalmente nell'architettura di rete TCP/IP per ottenere un **indirizzo** di livello *Network* a partire da un **indirizzo** di livello ***Data Link*** .

REPEATER: si veda **ripetitore** .

REQUEST: nel modello di riferimento **OSI** , primitiva di servizio attivata per richiedere la trasmissione di una **PDU** .

RESPONSE: nel modello di riferimento **OSI** , primitiva di servizio dei protocolli che prevedono *acknowledge* attivata per indicare l'avvenuta ricezione sul **nodo** remoto di una **PDU** precedentemente trasmessa tramite una primitiva ***request*** (si veda anche *confirm*).

RFC (Request For Comment): specifica implementativa di un **protocollo** /servizio/applicazione per il mondo TCP/IP. Le RFC sono documenti pubblici che evolvono per stadi successivi ben definiti e controllati dall' **IETF** , fino al momento della loro approvazione o del rifiuto.

RIP (Routing Information Protocol): è un **protocollo di *routing*** tra i più semplici, utilizzato in ambiente **Internet** , soprattutto in reti di piccole dimensioni. È il più implementato sulle piattaforme *hardware* più disparate (anche su *UNIX* e *Windows* NT). Utilizza il numero di ***router*** attraversati per confrontare i diversi percorsi alternativi di istradamento.

RIPETITORE: unità di *relaying* a livello Fisico; ad esempio, nello standard IEEE 802.3, un dispositivo usato per rigenerare il segnale ed interconnettere ***link*** in **cavo coassiale** , fibra ottica e **doppino** .

RITRASMISSIONE: tecnica utilizzata nei protocolli connessi per garantire la ricezione corretta dei dati.

ROUND TRIP DELAY: in IEEE 802.3, parametro di progetto dipendente dalla **velocità di propagazione** sul mezzo trasmissivo e dalla dimensione della rete, pari al tempo necessario perché un **pacchetto** si propaghi da un'estremità all'altra e qualsiasi eventuale **collisione** raggiunga la **stazione** trasmittente.

ROUTE: percorso di instradamento; nei ***router*** **IP** esiste una ***route*** per ogni *subnet* raggiungibile.

ROUTER: dispositivi fisico operante a livello 3 del modello **OSI** , in grado di effettuare il *forward* dei pacchetti in base alle regole su cui si basano i livelli 3 delle reti a cui risulta connesso e per le quali svolge il servizio di ***routing*** .

ROUTING: funzione di instradamento dei pacchetti a livello *Network*.

ROUTING ADATTATIVO o DINAMICO: tecnica di calcolo delle tabelle di instradamento in grado di considerare dinamicamente la topologia e lo stato della rete.

ROUTING CENTRALIZZATO: calcolo delle tabelle di instradamento per tutti i nodi della rete da parte di un singolo RCC centralizzato.

ROUTING DISTRIBUITO: tecnica di ***routing*** **adattativo** in cui il calcolo delle tabelle avviene tramite un algoritmo distribuito sui vari ***router*** .

ROUTING GERARCHICO: tecnica di partizionamento di una rete di grandi dimensioni in sottoreti, in modo da semplificare il problema del ***routing*** suddividendolo in ***routing*** inter-area e ***routing*** intra-area.

ROUTING STATICO: tecnica di instradamento in cui le tabelle sono determinate in fase di configurazione della rete.

RS-232: standard per interfacce seriali, sincrone o asincrone, operanti sino a 19.200 b/s.

RTN (Rete Telefonica Nazionale): (riferita anche come Rete Telefonica Generale) rappresenta l'infrastruttura geografica di un gestore pubblico, preposta all'espletamento del servizio telefonico tradizionale.

SAP (Service Access Point): individua un punto di comunicazione in corrispondenza del quale un' **entità** fornisce un servizio ad un'altra.

SAPI (Service Access Point Identifier): identificatore del servizio di livello 3 al quale vengono consegnati i dati provenienti dal livello 2.

SAR (Segmentation and Reassembly): metodo per segmentare in frammenti più piccoli (esempio: celle) un messaggio arbitrariamente lungo.

SBILANCIATA: tecnica di trasmissione di segnali elettrici con riferimento a massa.

SCHERMATURA: realizzazione di una gabbia di *Faraday*, da collegare a terra, attorno a un cavo o a un circuito in modo che i disturbi elettromagnetici non si propaghino dall'esterno all'interno e viceversa.

SDH (Synchronous Digital Hierarchy): gerarchia numerica **sincrona** standardizzata in ambito **ITU-T** per la trasmissione di segnali numerici su fibra.

SDLC (Synchronous Data Link Control): **protocollo** di livello 2 concepito dell'IBM per l'architettura SNA, da cui è derivato l' **HDLC** , per poter realizzare una trasmissione dati affidabile in ambienti SNA. È un **protocollo** orientato al bit e viene utilizzato su linee punto-punto e **punto-multipunto** ; prevede una **stazione** primaria e una o più stazioni secondarie. Ha un unico modo di funzionamento corrispondente al *Normal Response Mode* dell' **HDLC**). Al pari di quest'ultimo prevede la rivelazione degli errori ed il loro recupero mediante **ritrasmissione** . La struttura della **trama** prevede una ***flag*** inimitabile (01111110), un campo **indirizzo** di 8 bit, un campo controllo di 8 bit, un campo informativo di lunghezza variabile (trattato a carattere, secondo codifica **ASCII** o EBCDIC), un campo di controllo di 16 bit per rivelare errori e una ***flag*** (01111110) di chiusura.

SDU (Service Data Unit): unità informativa relativa ad uno strato di **protocollo** . È l'unità di dati passata da un' **entità** a livello superiore che sta richiedendo un servizio a un' **entità** di livello inferiore che lo fornisce.

SEGMENTAZIONE: funzione in cui una **SDU** viene divisa in segmenti, ognuno dei quali viene trasmesso in una **PDU** separata.

SIMPLEX: modalità di trasmissione monodirezionale.

SINCRONA: tipo di trasmissione dati in cui la sincronizzazione tra trasmettitore e ricevitore viene mantenuta permanentemente.

SLAVE: nei sistemi trasmissivi **punto-multipunto** , una delle stazioni il cui accesso al **canale** è controllato dalla **stazione *master*** .

SLOT TIME: nelle reti CSMA/CD è la finestra di tempo necessaria per trasmettere una **trama** di lunghezza minima.

SMF (Single Mode Fiber): fibra ottica monomodale. Il segnale luminoso si propaga in un solo cammino (ovvero un solo modo). Poiché tutti i raggi luminosi seguono lo stesso cammino, ovvero attraversano la stessa distanza, non si ha dispersione come nelle fibre multimodali. Le fibre monomodali possono supportare alti *bit rate* e coprire lunghe distanze, proprio in virtù di questa caratteristica che ne determina una bassa **attenuazione** .

SMTP (Simple Mail Transfer Protocol): **protocollo** definito nella RFC 821, ed utilizzato per il trasferimento della posta elettronica tra *computer*. È un **protocollo** utilizzato per la trasmissione della posta, per cui per l'accesso ai messaggi dal *client* vengono impiegati altri protocolli. (esempio: **POP**).

SOCKET: nell'ambito dell'architettura TCP/IP indica un connettore logico, ossia un identificatore di una connessione logica fra un *client* ed un *server* **Internet** . Un *socket* è rappresentato da una quadrupla di valori: **indirizzo IP** sorgente, TCP/UDP ***port*** sorgente, **indirizzo IP** destinatario, TCP/UDP ***port*** destinatario.

SONET (Synchronous Optical Network): standard **ANSI** per la trasmissione **sincrona** delle infromazioni numeriche su fibra ottica. È utilizzato largamente nel Nordamerica e nel Canada.

SPF (Shortest Path First): termine spesso usato per indicare l'algoritmo di *Dijkstra*, in cui i cammini verso tutte le destinazioni sono calcolati a partire dal grafo della rete; utilizzato dai protocolli di ***routing*** di tipo ***LINK STATE*** *packet*.

SSAP (Source Service Access Point): sigla usata per indicare l' **indirizzo** del mittente.

START-STOP: nome alternativo per indicare la tecnica di trasmissione **asincrona** il cui nome deriva dai bit di *start* e stop che delimitano l'inizio e la fine della trasmissione.

STAZIONE: termine usato nelle reti locali per indicare un *end system* o un *intermediate system*, evidenziandone le funzionalità a livello ***Data Link*** .

STM-1 (Synchronous Transport Module 1): standard **SDH** per la trasmissione di un segnale numerico su fibra OC-3 a velocità 155.52 Mbit/s.

STM-n (Synchronous Transport Module n): (con n intero) standard **SDH** per la trasmissione su fibra ottica (OC-n x 3) impiegante uno schema di multiplazione di n trame trasmissive di tipo **STM-1** (esempio: STM-4=622.08 Mbit/s; STM-16=2.488 Gbit/s).

STORE AND FORWARD: metodo di **commutazione** in cui un **pacchetto** viene prima interamente ricevuto, quindi analizzato e poi ritrasmesso.

STP (Shielded Twisted Pair): cavo in rame a coppie simmetriche schermate (normalmente a 4 coppie). Ciascuna coppia viene schermata con rivestimento di materiale metallico a calza per limitare le interferenze fra coppie diverse. Viene impiegato nelle reti locali e nella trasmissione ATM in reti private su brevi distanze.

STS-1 (Synchronous Transport Signal 1): standard **SONET** per la trasmissione di un segnale numerico su fibra OC-1 alla velocità 51.84 Mbit/s.

STS-n (Synchronous Transport Signal n): (con n intero) standard **SONET** per la trasmissione numerica delle informazioni su fibra di tipo OC-n, che prevede uno schema di multiplazione di n trame di tipo **STS-1** (esempio: STS-3= 155.52 Mbit/s; STS-12=622.08 Mbit/s; STS-48=2.488 Gbit/s).

SWITCH: dispositivo multiporta in grado di commutare trame a livello ***Data Link*** (in una rete dati locale o geografica); dispositivo in grado di realizzare connessioni commutate logiche o fisiche.

SWITCHED LAN: **LAN** in cui vengono utilizzati ***switch*** per aumentarne le prestazioni globali. Una *switched* LAN consente di avere un ***throughput*** aggregato pari teoricamente alla somma dei ***throughput*** relativi alle sue porte fisiche.

TABELLA DI ROUTING: tabella contenente le informazioni utili per gli algoritmi di instradamento quali, per ogni destinazione, la linea da utilizzare, il costo e il numero di ***hop*** .

TCP (Transmission Control Protocol): **protocollo** di livello trasporto dell'architettura **Internet** in grado di fornire un servizio end to end di tipo affidabile e riscontrato. In particolare il TCP implementa le funzioni di **controllo di flusso** , riscontro dei pacchetti ricevuti e controllo di sequenza).

TELNET: applicazione **Internet** basata sul **protocollo TCP** , che consente di remotizzare attraverso una rete **IP** , l'accesso a un ***host*** remoto. Il *client* si comporta come terminale remoto del *server telnet* ed accede alle risorse dell' ***host*** mediante l'autenticazione con una *username* ed una *password*.

THROUGHPUT: misura, normalmente espressa in **pps** , (ovvero in bit/s) l'effettiva capacità trasmissiva di una rete o di un elemento di essa.

TIME-TO-LIVE: campo nelle **PDU** di livello *Network* utilizzato per limitarne temporalmente la vita nel caso si verificassero *loop* nella rete.

TOKEN: particolare **pacchetto** la cui ricezione indica il permesso di trasmettere su un mezzo condiviso.

TOKEN PASSING: algoritmo di accesso ad un mezzo condiviso basato su ***token*** .

TOKEN RING: tipologia di rete locale ad anello, funzionante con un **protocollo** di accesso basato su un ***token*** (testimone) che consente a ciascuna **stazione** della rete di acquisire il controllo del mezzo trasmissivo in maniera deterministica e di trasmettere le informazioni. La rete, inizialmente proposta da IBM, è stata standardizzata da **IEEE** con il documento IEEE 802.5.

TRAMA: nome generico per indicare una **PDU** di livello ***Data Link*** . Indica, nel senso della terminologia impiegata per le tecnologie trasmissive, una struttura di bit il cui formato si ripete periodicamente (esempio: la trama di un sistema trasmissivo a 2048 kbit/s, costituita da 256 bit trasmessi ogni 125 microsecondi).

TRANSCEIVER: nelle reti ***Ethernet*** /IEEE 802.3, dispositivo che si occupa di trasmettere e ricevere le trame sul mezzo fisico e di rilevare le collisioni.

TRANSPARENT BRIDGE: ***bridge*** di derivazione ***Ethernet*** che ha le tabelle d'instradamento a bordo ed è trasparente, nel senso che i nodi ad esso connessi ne ignorano l'esistenza.

TWISTED PAIR: si veda **doppino** .

UDP (User Datagram Protocol): **protocollo** dell'architettura TCP/IP che fornisce un servizio di trasporto in senso **OSI** di tipo *connection-less*; essendo non affidabile, non prevede controllo di errore, **ritrasmissione** né *acknowledge*.

Viene impiegato per esempio per la trasmissione della voce e del video su reti **IP** . È utilizzato, per esempio da NFS ed SNMP.

UNACKNOWLEDGE SERVICE O SERVIZIO NON CONFERMATO: servizio in cui il richiedente non viene informato del completamento della richiesta inoltrata.

UNI (ente nazionale italiano di UNIficazione): ente italiano con attività principalmente nel settore della standardizzazione.

UNICASTING: trasmissione di informazioni da una sorgente verso una singola destinazione.

UTP (Unshielded Twisted Pair): cavo in rame a coppie simmetriche non schermato, normalmente a 4 coppie, utilizzato per trasmissioni in reti locali. Viene impiegato anche per interfacce ATM in ambito locale.

VELOCITÀ DI PROPAGAZIONE: velocità con cui un segnale elettrico o ottico si propaga attraverso un mezzo trasmissivo; espressa come percentuale della velocità della luce nel vuoto.

WAN (Wide Area Network): indica una rete ad estensione geografica a livello di regione/nazione, ed impiega differenti tecniche di trasporto dell'informazione di utente (circuito, **pacchetto** , **trama** , cella).

WELL-KNOWN PORT: nell'architettura di rete TCP/IP, le porte preassegnate ai principali protocolli applicativi.

WWW (World Wide Web): indica la ragnatela mondiale costituita dai *server* **Internet** in grado di fornire servizi di accesso a pagine HTML ed altri servizi applicativi.

X.21: standard che definisce l'interfaccia **DTE** / **DCE** per la trasmissione dati **sincrona** ***full duplex*** su reti a **commutazione di pacchetto X.25** , comprese le procedure per il controllo delle chiamate virtuali. Il livello fisico è basato sull'impiego di connettori a 15 poli, le velocità previste non superano 9600 bit/s.

X.21 BIS: definisce le modalità di interfacciamento fra terminali dati sincroni e **modem** sincroni della serie V. È impiegato per trasmissioni a velocità superiori a 9600 bit/s, ed impiega connettori a 15 oppure 25 poli; in caso di velocità superiori (48 e 64 kbit/s) cambiano la connettorizzazione (tipo V.35 a 34 poli) ed i criteri all'interfaccia.

X.25: standard per la trasmissione di dati tramite reti a **commutazione di pacchetto** . Utilizzato su linee trasmissive di accesso con velocità da 2 kbit/s fino a 64 kbit/s.

Autori

Hanno realizzato il materiale di questo modulo:

Prof. Franco Callegati
Franco Callegati è professore associato di Reti di Telecomunicazioni presso il Dipartimento di Elettronica, Informatica e Sistemistica (D.E.I.S.) dell'Università di Bologna. Presso la Facoltà di Ingegneria di Bologna prima ed ora presso la Facoltà di Ingegneria di Cesena ha tenuto e tiene corsi di base di Reti di Telecomunicazioni e corsi avanzati su teoria del traffico e progettazione di reti. Si interessa di problematiche di dimensionamento e progettazioni di reti di telecomunicazione a larga banda e la sua attività di ricerca più recente ha come oggetto le reti ottiche ad altissima velocità, argomento sul quale ha pubblicato numerosi lavori, partecipando a progetti di ricerca nazionali ed internazionali con ruoli di coordinamento.
Dott.Ing. Walter Cerroni
Walter Cerroni ha ottenuto il titolo di Dottore di Ricerca in Ingegneria Elettronica ed Informatica presso l'Università di Bologna. Svolge attività di ricerca nell'ambito dell'analisi di prestazioni di reti di telecomunicazioni e del progetto di architetture per commutazione ottica a pacchetto, collaborando con il gruppo di Reti di Telecomunicazioni dell'Università di Bologna. Svolge attività didattica come collaboratore per i corsi di Reti di Telecomunicazioni nell'ambito sia delle Lauree in Ingegneria dell'Informazione che del Master in *Management* e *Information Technology*

dell'Università di Bologna, oltre a fornire servizi di consulenza a ditte ed enti di formazione nel settore delle tecnologie dell'informazione.

Dott.Ing. Paolo Zaffoni

Paolo Zaffoni si è laureato in Ingegneria delle Telecomunicazioni presso l'Università di Bologna nel giugno del 2001. È iscritto al secondo anno del Corso di Dottorato di Ricerca in Ingegneria Elettronica, Informatica e delle Telecomunicazioni presso l'Università degli Studi di Bologna. Svolge attività di ricerca nel campo dell'analisi del traffico, del progetto e della gestione di reti ad alte prestazioni. Ha svolto ed è attualmente impegnato in attività di supporto alla didattica per gli insegnamenti di Reti di Telecomunicazioni relativi al Corso di Laurea in Ingegneria dell'Informazione presso l'Università degli Studi di Bologna e fornisce servizi di consulenza ad imprese attive nel settore delle tecnologie dell'informazione.

Modulo realizzato sulla base di materiali prodotti nell'ambito di un piano di formazione di 12.000 tecnici delle pubbliche amministrazioni e messi a disposizione del MIUR dall'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA).