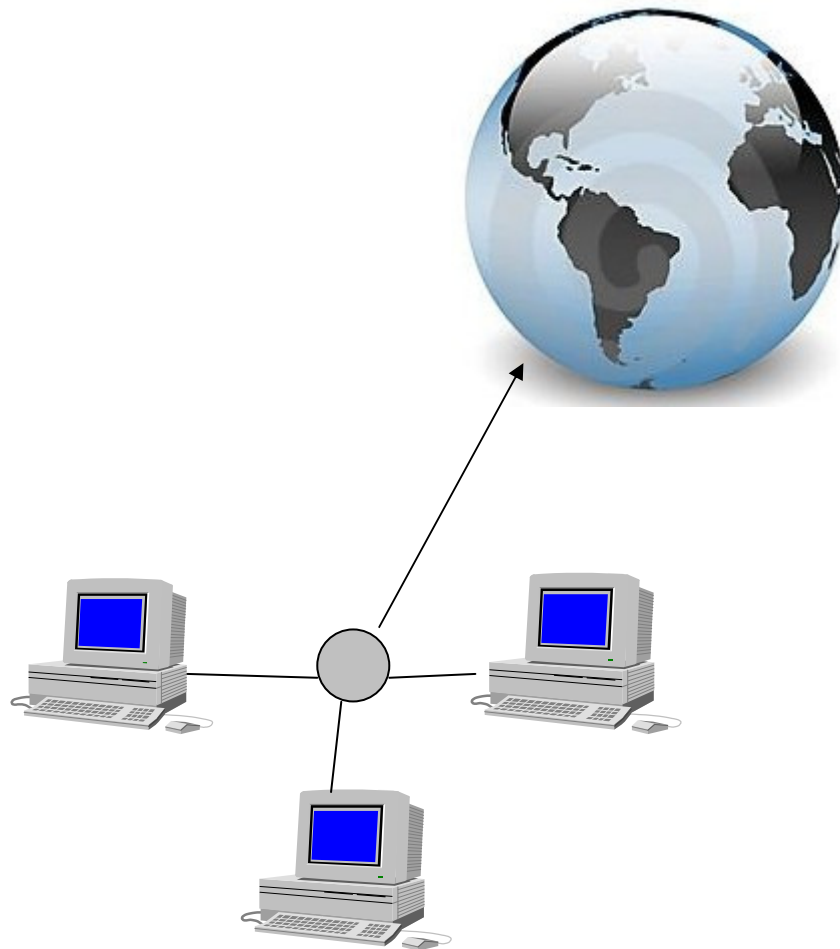


Appunti di RETI di computer

LAN

Internet



Prof. Claudio Maccherani

Perugia 2004

INDICE

RETI	1
CLASSIFICAZIONE PER ESTENZIONE	1
TOPOLOGIE FISICHE.....	1
RETI FISICHE (TOPOLOGIE LOGICHE)	2
SCHEDE DI RETE	3
COLLEGAMENTI DI RETE (CANALI)	4
TECNOLOGIE DI TRASMISSIONE.....	5
TECNOLOGIE DI COMUNICAZIONE	5
TECNICHE DI COMMUTAZIONE.....	6
MODELLI "CLIENT/SERVER" E "PEER TO PEER"	7
ARCHITETTURA DI RETE	7
MODELLO ISO/OSI	8
MODELLO TCP/IP	11
LIVELLO 1 – FISICO	11
LIVELLO 2 – RETE (PROTOCOLLO IP).....	11
LIVELLO 3 – TRASPORTO (PROTOCOLLO TCP)	15
LIVELLO 4 – APPLICAZIONI.....	16
ALTRI PROTOCOLLI.....	17
LAN DOMESTICHE E INTERNET	18
INTERNET	23
STORIA.....	23
CONNESSIONE E INDIRIZZI	24
ACCESSO	24
LIVELLI E PROTOCOLLI	26
SERVIZI	26
E-MAIL (POSTA ELETTRONICA)	26
FTP (TRASFERIMENTO FILE).....	27
WORLD WIDE WEB	27
TELNET (ACCESSO REMOTO)	28
MAILING LIST	28
NEWS	28
SEARCH ENGINE (MOTORI DI RICERCA).....	28
CHAT	28
VIDEOCONFERENZA	29
E-QUALCOSA	29
INTRANET ED EXTRANET.....	29
I "LINGUAGGI" DI INTERNET	30
ACRONIMI	31

RETI

Il termine *Telematica* (telecomunicazioni+informatica) indica il settore di integrazione tra informatica e telecomunicazioni. In tale ambito rientrano le Reti (*Network*) di computer, sistemi di elaborazione interconnessi, che comunicano tra di loro. Dai sistemi centralizzati degli anni '60 (mainframe ai quali sono connessi decine di videotermini), dopo l'avvento negli anni '80 dei PC, si è via via passati ai sistemi distribuiti, cioè alle reti di computer locali (LAN) e mondiali (Internet). In un sistema distribuito ciascun nodo, oltre a poter funzionare autonomamente, può usufruire di risorse hw e sw condivise (stampanti, dischi, masterizzatori, scanner, accesso a Internet, applicazioni, database, etc.).

Classificazione per estensione

In base all'estensione, le reti si possono classificare in:

- ❑ LAN (*Local Area Network*), reti locali, all'interno di uno stesso edificio o tra edifici vicini
- ❑ MAN (*Metropolitan Area Network*), reti metropolitane, oramai WAN
- ❑ WAN (*Wide Area Network*), reti di estensione mondiale (Internet).

Topologie fisiche

In base alla disposizione dei nodi di una rete si possono avere diverse topologie:

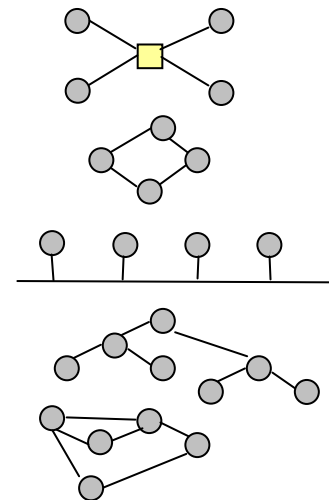
Stella (Lan) c'è un nodo centrale – Hub/Switch - al quale tutti i computer sono collegati

Anello (Lan) i computer sono collegati ad anello ad un cavo circolare

Bus (Lan) i computer sono collegati ad un unico cavo rettilineo, il "bus"

Albero (Wan) struttura gerarchica ad albero

Maglie (Wan) grafo completamente connesso o meno

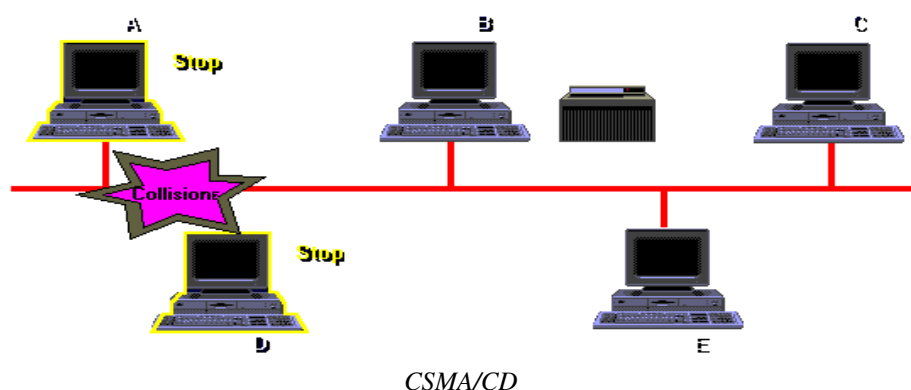


Due nodi di una rete possono essere interconnessi mediante una connessione fisica (esiste un canale che li collega direttamente) o logica (che usa diversi canali fisici).

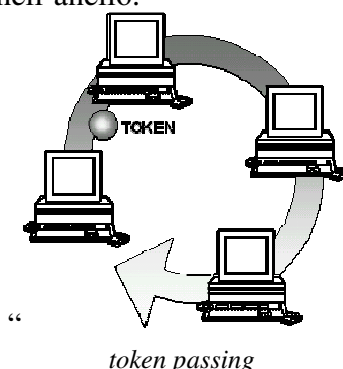
Reti fisiche (Topologie logiche)

Sono le regole per il trasferimento dei dati in rete. Le principali sono Ethernet, Token Ring, FDDI e Wireless. Tali topologie non possono comunicare direttamente tra loro, ma solo attraverso opportuni dispositivi (gateway).

- **Ethernet** - standard IEEE 802.3 - è nata nel 1973 (3COM). Esistono diversi standard (10Base-2, 10Base-5, 10Base-T, 100Base-TX, 100Base-FX, dove il numero indica la velocità in Mbps, milioni di bit per secondo) che utilizzano cavi coassiali o doppini interallacciati "Twisted pair", su topologie a bus o a stella con la presenza di un hub centrale. Per le reti Wi-Fi c'è lo standard IEEE 802.11. Per regolare l'accesso al canale si utilizza il metodo CSMA/CD¹ (*Carrier Sense Multiple Access / Collision Detection*).



- **Token Ring**, della IBM, utilizzata per reti ad anello. L'accesso al canale è regolamentato da un Token² elettronico circolante nell'anello.



- **FDDI** (*Fiber Distributed Data Interface*, interfaccia a fibra ottica) è basato su tipologie ad anello in fibra ottica può connettere stazioni distanti da 2 a un massimo di 100 Km.
- **Wireless**³ sono le "reti senza fili" dove i dati sono trasmessi tramite onde radio o raggi infrarossi. In questo contesto rientra anche la telefonia cellulare (GSM, UMTS, etc).

¹ **CSMA/CD** (*Carrier Sense Multiple Access/Collision Detection* - accesso multiplo a rilevazione di portante / individuazione delle collisioni): il computer che deve trasmettere testa il cavo; se esso risulta libero invia il pacchetto e si resta in "ascolto" sul cavo per vedere se si verifica una collisione; se rileva una collisione (aumento della tensione) ritenta l'invio dopo un intervallo di tempo (in nanosecondi) casuale.

² **Token**: il token è un "gettone elettronico" che circola nell'anello; il nodo che deve trasmettere attende che gli arrivi il token e se esso è vuoto vi inserisce i dati e lo rilascia; ogni nodo dell'anello esamina il token e controlla se i dati sono a lui indirizzati, nel qual caso li preleva e reinvia il token con la "ricevuta di ricevimento" al mittente il quale, una volta avuta conferma dell'avvenuta consegna del pacchetto, provvede a vuotare il token e a reinserirlo nella rete.

³ **reti Wireless**: in queste reti "senza fili" i dati sono trasmessi tramite onde radio o raggi infrarossi, eliminando così ogni connessione fisica. Nell'ambito di tale tecnologia rientra anche la telefonia cellulare (GSM - *Global System for Mobile communications*, UMTS - *Universal Mobile Telecommunications System*, etc). Nell'ambito delle LAN si parla di



- Nell'ambito delle LAN si parla di tecnologia Bluetooth⁴, HiperLan e Wi-Fi (standard IEEE 802.11⁵).

Schede di rete

Tutti i computer collegati in rete debbono essere dotati di apposite schede o adattatori di rete NIC (*Network Interface Card*) che consentano loro il collegamento alla topologia logica mediante cavo di connessione (o onde radio, se rete wireless). Ogni scheda di rete dispone di un proprio indirizzo

tecnologia **Bluetooth** (tecnologia rivolta a reti di cellulari, palmari, videocamere e altri piccoli dispositivi, 1 Mbps), HiperLan (europea, 20 e 54 Mbps) e **Wi-Fi**, *Wireless Fidelity*, (11 Mbps, tecnologia rivolta a reti di PC). La trasmissione dei dati è cifrata. La WLAN può essere collegata a una LAN cablata mediante punto di accesso (AP - *Access Point*), che in questo caso, oltre a fungere da ripetitore, avrà anche la funzione di bridge. La LAN cablata può essere costituita anche da un hub e un solo PC che magari funge da gateway verso Internet. Una WLAN è basata su due tipologie di dispositivi: Access Point (AP) e Wireless Terminal (WT).

- Gli AP (*Access Point*) sono dei bridge che collegano la sottorete wireless con la sottorete cablata; possono essere dispositivi hardware dedicati o programmi software che girano su un computer dotato sia di interfaccia wireless che di scheda ethernet.
- I WT (*Wireless Terminal*) possono essere qualsiasi tipo di dispositivo o apparecchiatura che interfaccia lo standard IEEE 802.11 (PC, notebook, pda, palmari, cellulari) o sistemi consumer su tecnologia Bluetooth.

La copertura di una cella radio varia da 20 a 300 mt, con possibilità di collegamento da 10 a 250 utenze per ciascun AP.

⁴ tecnologia **Bluetooth**: consente di far dialogare "senza fili" dispositivi diversi (telefoni, cellulari, stampanti, PDA, notebook, PC, TV, elettrodomestici, etc.). Le informazioni viaggiano attraverso onde radio o raggi infrarossi ed ogni dispositivo collegato dovrà avere un chip integrato in grado di ricevere e trasmettere informazioni via etere. Questa tecnologia è rivolta specialmente alla connessione di apparecchiature di piccole dimensioni.

⁵ protocollo **IEEE 802.11**: denominato anche **Wi-Fi**, detta le specifiche a livello fisico e datalink per l'implementazione delle reti wireless. Con velocità di trasmissione da 5.5 a 11 Mbps, esso consente di variare la velocità di trasmissione per adattarsi al canale, di scegliere automaticamente la banda meno utilizzata e di scegliere automaticamente l'access point in funzione della potenza del segnale e del traffico di rete.

identificativo, univoco a livello mondiale, chiamato indirizzo MAC (*Media Control Access* – controllo di accesso al mezzo) di 6 byte.



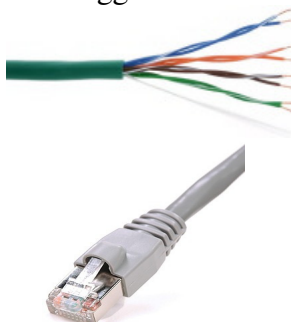
NIC (Network Interface Card) - scheda di rete

Collegamenti di rete (canali)

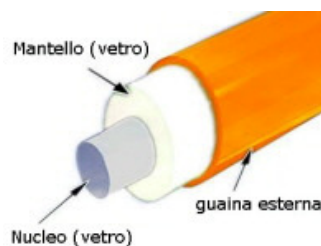
I collegamenti di rete, cioè i canali attraverso i quali transitano i dati, nelle reti cablate sono costituiti da cavi di diversi tipi (coassiale⁶, doppino telefonico⁷ -, fibra ottica⁸), mentre nelle reti wireless sono costituiti da onde radio o raggi infrarossi.



cavo coassiale con
connettore BNC



doppino telefonico
twisted pair con
connettore RJ-45



cavo in fibra ottica (sezione)



cavo in fibra
ottica con
connettore



onde radio
[Wi-Fi]

⁶ cavo **Coassiale**: simile al cavo che trasporta segnali radio e TV su lunghe distanze, è stato riadattato per il trasporto di dati digitali, ma la presenza di rumore e di distorsione del segnale fa sì che tale cablaggio possa estendersi solo per brevi distanze (a meno di utilizzare dei particolari ripetitori di segnale – repair). Sono costituiti da un conduttore centrale di rame circondato da uno strato isolante rivestito da una calza di materiale intrecciato (il secondo conduttore) a sua volta rivestito da un altro strato isolante. È immune ai campi magnetici e viene utilizzato per reti a bus di tipo Ethernet. Il cavo sottile RG58 è usato per 10Base2, mentre il cavo spesso RG213 è usato per 10Base5. Vengono utilizzati connettori a T (BNC) per il collegamento alla scheda di rete e ai due nodi adiacenti.

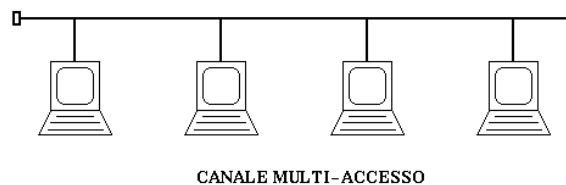
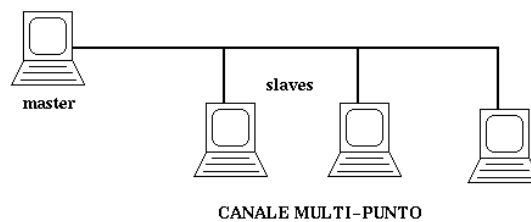
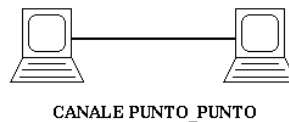
⁷ **doppino** ritorto Twisted Pair: sono i cavi UTP (*Unshielded Twisted Pair* - doppino ritorto non schermato) e STP (*Shielded Twisted Pair* - doppino ritorto schermato), costituiti da 4 coppie di conduttori di rame ritorti.. Utilizzati nella topologia Ethernet 10BaseT e 100BaseTX, hanno agli estremi dei connettori RJ-45 che ne consentono l'innesco ai concentratori Hub e Switch. Per il collegamento al concentratore si utilizzano cavo dritti, mentre per il collegamento diretto tra due computer si utilizza un cavo incrociato.

⁸ **cavi in fibra ottica**: sono totalmente immuni dalle interferenze elettromagnetiche, utilizzati in sistemi preposti alla trasmissione di una notevole quantità di dati o in reti che richiedono il trasferimento di file ad elevata velocità (FDDI, ATM o altri). Il cavo è costituito da un nucleo, un rivestimento, una copertura, una fibra di irrigidimento e una guaina esterna. I dati viaggiano attraverso il nucleo sotto forma di segnali luminosi. Sono sicuri, immuni da interferenze, possono coprire lunghe distanze (diversi Km) e trasportare una grande quantità di informazione.

Tecnologie di trasmissione

Si hanno più tipi di trasmissione:

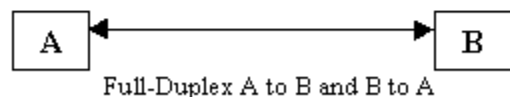
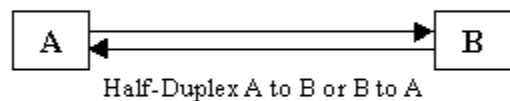
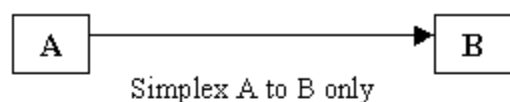
- Punto-Punto (*Point to Point*), collegamento diretto tra coppie di computer
- Multipunto (*Broadcast*), con più nodi collegati attraverso un'unica connessione fisica, il messaggio viene ricevuto da tutti ma letto solo dal nodo destinazione.



Tecnologie di comunicazione

Ci sono tre i tipi di linee di comunicazione:

1. Simplex,
comunicazione monodirezionale
(tipo canale radio-televisivo)
2. Half-duplex,
comunicazione bidirezionale alternata
(tipo ricetrasmittitori)
3. Full-duplex,
comunicazione bidirezionale contemporanea
(tipo telefono)

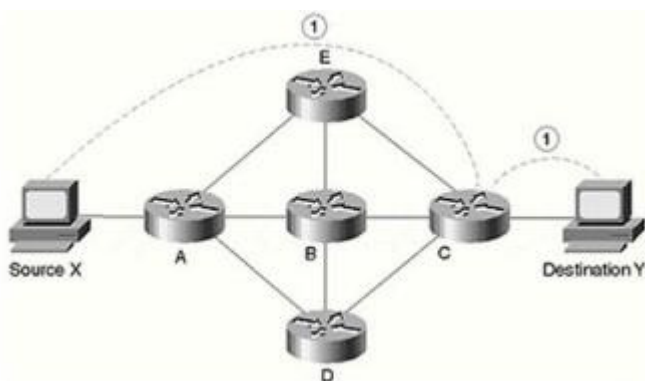
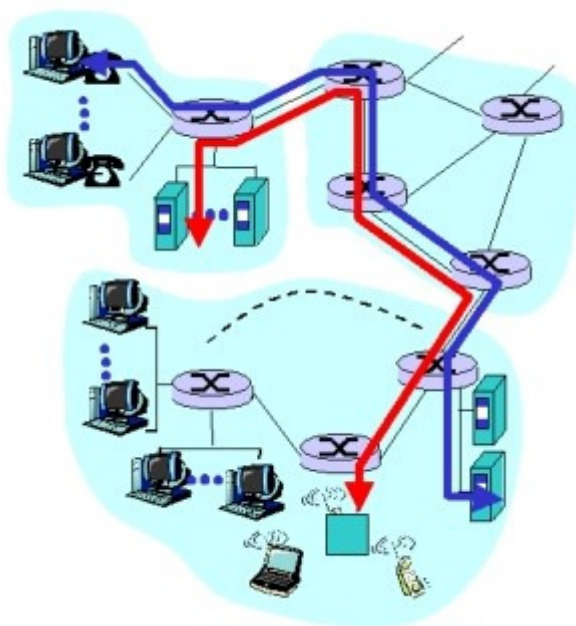


Tecniche di Commutazione

Per commutazione si intende la definizione di un percorso per la comunicazione tra due nodi di una rete. Tre sono le diverse tecniche di commutazione:

1 - Commutazione di **CIRCUITO**:

si crea un collegamento fisico tra i due nodi che resta attivo per tutta la durata della sessione di comunicazione, come ad esempio nel collegamento telefonico. In tal caso la linea così stabilitasi risulta "occupata" per tutti gli altri nodi della rete fino a che la sessione non verrà chiusa.

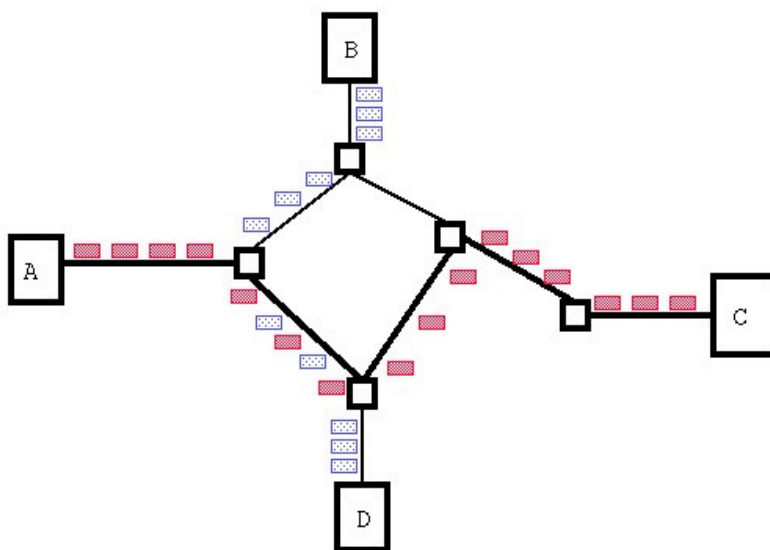


2- Commutazione di **MESSAGGIO**:

il messaggio viene trasmesso a un nodo adiacente, che lo memorizza temporaneamente e poi lo reinstrada verso un altro nodo ad esso adiacente, e così via fino a che il messaggio non giunge a destinazione (*store and forward*). Ogni nodo deve essere capace di instradare il messaggio verso la destinazione finale.

3- Commutazione di **PACCHETTO**:

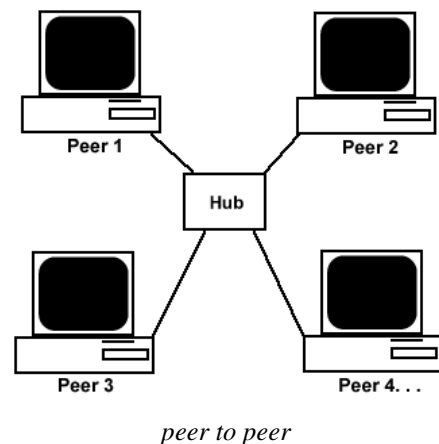
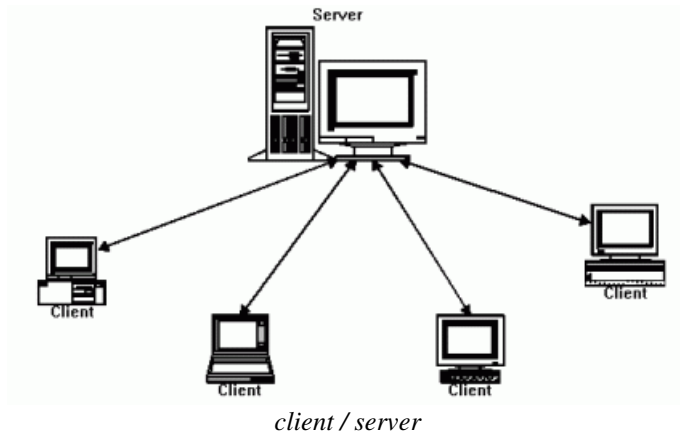
tecnica analoga alla Commutazione di Messaggio, solo che il messaggio da trasmettere viene suddiviso in diversi "pacchetti" ciascuno dei quali può essere diversamente instradato. Ogni pacchetto dovrà avere, oltre ai dati, ind.destinatario, ind.mittente, numero e flag ultimo sì/no (perché il destinatario possa ricostruire il messaggio). In caso di errore si richiederà il reinvio del solo pacchetto errato (e non di tutto il messaggio).



Modelli "client/server" e "peer to peer"

Una rete (locale/globale) di tipo "client/server" (*cliente/servitore*) è una rete dove uno o più host (computer ospitanti) sono dedicati alla funzione di server (servente o servitore) per fornire agli altri computer client (clienti o richiedenti) vari servizi. Tali servizi possono essere applicazioni, database, spazio disco, code di stampa, fax, posta elettronica, pagine web, etc.

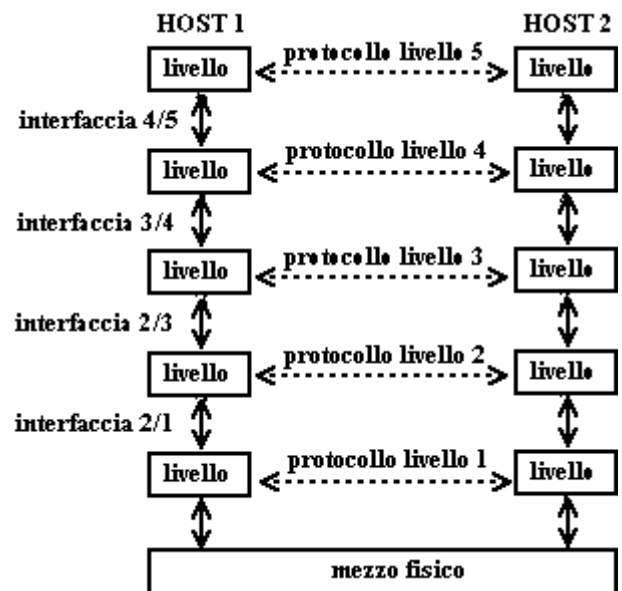
Una rete di tipo "peer to peer" (*da pari a pari*) è una rete paritetica, senza server dedicati, dove ogni computer funziona sia da client che da server, decidendo cosa condividere con gli altri computer della rete.



Architettura di rete

Le reti, come i sistemi operativi, sono organizzate a *livelli* (cipolla-like). Ogni livello fornisce a quello superiore i servizi richiesti e fa le proprie richieste al livello successivo, senza preoccuparsi di come questi funzionino, conoscendo solo la modalità di richiedere e fornire servizi. I livelli di ogni nodo comunicano tra di loro tramite delle *interfacce* e comunicano con gli equivalenti livelli degli altri nodi tramite dei *protocolli* di comunicazione (insieme di regole e di convenzioni da rispettare per la comunicazione).

L'insieme dei livelli e dei protocolli costituisce l'*architettura di rete*.



Modello ISO/OSI

Per realizzare la comunicazione tra due sistemi fisicamente connessi tra di loro si utilizzano dei protocolli ben definiti. Un protocollo è un insieme di regole e di convenzioni che tutti i partecipanti alla comunicazione sono obbligati a rispettare perché la comunicazione stessa sia possibile. Nel 1984 l'**ISO** (*International Standard Organization*) ha definito un modello di riferimento standard per l'interconnessione dei sistemi aperti, l'**OSI** (*Open System Interconnection*).

Tale modello, strutturato in 7 diversi livelli, non è una specifica, ma una direttiva generale. Nella maggior parte dei casi i progettisti optano per un modello semplificato quale il modello TCP/IP a 4 livelli, più avanti esaminato. I 7 livelli del modello OSI sono:

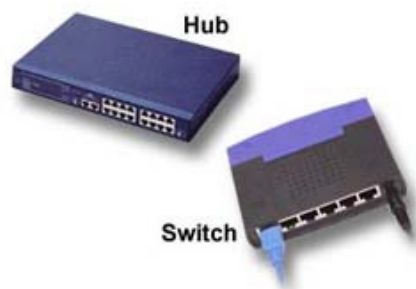
1. livello **FISICO**. Definisce le funzioni basilari della connessione fisica, a livello hardware. A questo livello è definita la topologia di rete (a bus, a stella), il mezzo di trasmissione (doppino telefonico, cavo coassiale, etc.), la tecnica di trasmissione (csma/cd, token, ..), le schede di rete⁹, l'Hub¹⁰.
2. livello **COLLEGAMENTO DATI**. Fornisce servizi per ripartire in "trame" i bit della trasmissione, serializzarli, controllare la correttezza della ricezione. Ogni trama ha l'indirizzo del destinatario e l'indirizzo del mittente (indirizzo fisico MAC delle relative schede di rete), l'FCS - Frame Check Sequence - per il rilevamento degli errori¹¹. Appartengono a questo livello gli Switch¹² e i Modem¹³. A questo livello si collocano anche i protocolli di collegamento (o protocolli di linea) quali BSC¹⁴ e HDLC¹⁵, PPP¹⁶.

⁹ **Nic** (*Network Interfaced Card*): le schede di rete sono dispositivi che permettono il collegamento del computer alla rete. Sono munite di connettori (Bnc, Rj45) per i cavi di rete e si inseriscono in appositi slot di espansione (ISA, EISA, VESA, PCI).

¹⁰ **Hub**: concentratore di reti a stella che riceve le informazioni da un nodo e le reinvia a tutti gli altri nodi collegati alle sue porte (4, 8, 16, 32 o 48). I nodi della LAN si connettono all'hub mediante cavi twisted pair con connettori Rj-45.

¹¹ **Rilevamento degli errori**: le tecniche di controllo degli errori sono basate sul concetto di "bit di parità", il bit che si aggiunge ad ogni byte trasmesso per rendere pari il numero di "1" dei 9 bit così trasmessi. Questo tipo di controllo è detto *checksum*, somma di controllo. In trasmissione, utilizzando una formula matematica, viene creato il blocco FCS (*Frame Check Sequence*) in base ai bit di dati trasmessi; in ricezione, applicando la stessa formula matematica, viene ricalcolato il blocco FCS e, se questo non coincide con quello ricevuto significa che c'è stato un errore di trasmissione, nel qual caso si richiederà il rinvio del pacchetto. Per evitare la ritrasmissione del pacchetto in caso di errore si possono usare tecniche di **correzione degli errori** quali quella che consiste nell'invio di 3 bit di parità (c1, c2, c3) per ogni 4 bit di dati (b1, b2, b3, b4) in sequenze b1-b2-b3-b4-c1-c2-c3. c1 rende pari gli "1" di b1, b2, b4; c2 rende pari gli "1" di b1, b3, b4; c3 rende pari gli "1" di b2, b3, b4. Con questo sistema si può non solo rilevare l'errore, ma anche correggerlo, individuando quali sono le sequenze errate e quindi quale è il bit errato.

¹² **Switch o Bridge**: è un dispositivo somigliante all'hub, ma più "intelligente", essendo capace di analizzare il contenuto del pacchetto ricevuto e di inoltrarlo al nodo destinatario, senza inviarlo a tutti i nodi collegati (per far questo esamina l'indirizzo MAC del destinatario contenuto nel pacchetto).



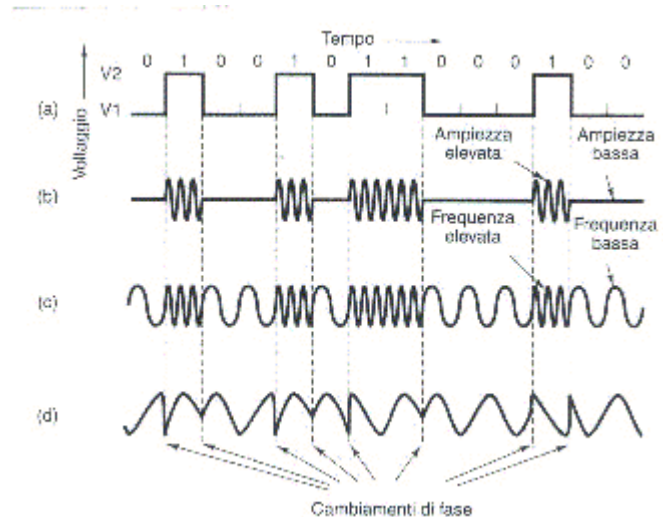
¹³ **Modem**: è il dispositivo che consente di utilizzare le linee telefoniche per il collegamento. Trasforma i segnali digitali (bit) in segnali analogici modulati (onde elettromagnetiche) e viceversa per poter essere trasmessi nelle linee telefoniche. Il

3. livello di **RETE**. A questo livello gli indirizzi logici IP vengono trasformati in indirizzi fisici Mac (in trasmissione) e gli indirizzi fisici Mac vengono trasformati in indirizzi logici IP (in ricezione). I pacchetti vengono suddivisi in trame (in trasmissione) e le trame riorganizzate in pacchetti (in ricezione). A questo livello si collocano i Bridge¹⁷ ed i Router¹⁸.

loro compito è di MODulare (in trasmissione) e DEModulare (in ricezione) il segnale. La **modulazione** può essere di *ampiezza*, di *frequenza* o di *fase*. La velocità di trasmissione dei modem attuali - standard V.90 - è di 56Kbps.



modem PSTN a 56Kbps



modulazioni: di ampiezza, di frequenza, di fase

¹⁴ protocollo **BSC** (*Binary Synchronous Protocol*): protocollo IBM "byte oriented" specifico delle comunicazioni Half-duplex. I messaggi possono essere di controllo [syn, syn, ack, syn] o di testo [syn, syn, soh, header, stx, testo, etx, bcc, bcc, syn]. (syn-sincronizzazione; ack-affermative cknowledgegement, riconoscimento positivo; soh-start of heading, inizio intestazione; stx-start of text; etx-end of text; bcc-block check character, carattere di controllo; eot-end of trasmission; ...)

¹⁵ protocollo **HDLC** (*High level Data Link Control Procedure*): protocollo ISO "bit oriented" generalmente utilizzato nelle reti geografiche per trasmissioni sincrone full-duplex. Ci sono tre sequenze con particolare significato: a) 01111110 flag di inizio/fine messaggio; b) 15 o più "1" consecutivi per "idle" o collegamento non attivo; c) da 7 a 14 "1" consecutivi per "abort", errore. I messaggi hanno la seguente struttura: flag (8 bit), indirizzo (8 bit), controllo (8 bit), informazione (n bit), check (16 bit), flag (8 bit). I bit successivi al primo flag non possono avere più di 5 "1" consecutivi, per evitare di confonderli con il flag finale. Per questo il trasmettitore, dopo 5 "1" consecutivi inserisce il bit di stuffing 0 e il ricevitore elimina il primo "0" - bit di strapping - dopo una sequenza di 5 "1".

¹⁶ protocollo **PPP** (*Point to Point Protocol*): serve per gestire le comunicazioni via modem a 56 Kbps lato client. Al lato server si suppone che il computer contattato sia collegato con altri in una rete locale Ethernet che prevede il protocollo di interfaccia al mezzo fisico HDLC. Il protocollo PPP è l'evoluzione dell'HDLC, consente di trasmettere sullo stesso canale pacchetti generati da protocolli diversi di livello superiore. La trama PPP contiene il campo *protocol* di 2 byte che identificano il protocollo di livello superiore.

¹⁷ **Bridge**: dispositivo di connessione di due reti locali in grado di mantenere i pacchetti di ogni rete nel proprio ambito, a meno che non sia esplicitamente indirizzato ad un computer dell'altra rete. Un bridge non necessariamente è un dispositivo specifico, ma può anche essere un PC con due schede di rete e software idoneo.

¹⁸ **Router**: dispositivo in grado di instradare i pacchetti nelle reti sia locali che geografiche, inviando il pacchetto ad un router "adiacente" per instradarlo verso la destinazione, in base al suo indirizzo logico. È dotato di una "tabella di instradamento" o tabella di routing - aggiornata frequentemente - che gli consente di "conoscere" i router vicini. I router sono dotati di algoritmi di routing che consentono di individuare i router adiacenti ai quali instradare il pacchetto e, in caso di malfunzionamento di una parte della rete, di ricalcolare la tabella di instradamento per trovare percorsi alternativi. Un tipo particolare di router è il **Gateway** (router multiprotocollo) che, oltre ad instradare i pacchetti, consente di interconnettere due reti geografiche strutturalmente incompatibili. Un Gateway non necessariamente è un dispositivo specifico, ma può anche essere un PC dotato di software idoneo (ad esempio un PC che collega la rete locale a Internet). I Router possono essere usati anche come **FireWall**, cioè come barriere di sicurezza contro le intromissioni esterne non autorizzate quali i virus informatici. Il FireWall separa fisicamente la rete locale da quella esterna e governa il traffico dei

4. livello di **TRASPORTO**. A questo livello i messaggi vengono trasformati in pacchetti alla trasmissione - ad esempio secondo il protocollo TCP o UDP – e ricostruiti alla ricezione. Se si verifica un errore, è a questo livello che viene richiesto il rinvio di un pacchetto erroneamente ricevuto o che si conferma l'esatta ricezione dei pacchetti.
5. livello di **SESSIONE**. A questo livello vengono stabilite le comunicazioni tra le applicazioni di computer diversi tramite lo stabilimento, l'utilizzazione e la terminazione di una connessione o "sessione".
6. livello di **PRESENTAZIONE**. Questo livello non è sempre presente in tutte le reti. Quando esiste tale livello è preposto al controllo del formato dei dati a livello di cifratura (per la riservatezza e la sicurezza dell'informazione), codifica (per l'ottimizzazione della comunicazione), transcodifica (da un alfabeto ad un altro, ad esempio da ASCII ad EBCDIC), conversione (nelle rappresentazioni interne dei dati numerici).
7. livello di **APPLICAZIONE**. È il livello attraverso il quale le applicazioni accedono ai servizi di rete, quello che fornisce il servizio direttamente all'utente finale. A questo livello appartengono i protocolli HTTP, FTP, TELNET, SMTP, POP, etc. attraverso i quali le applicazioni stabiliscono collegamenti di tipo "peer to peer" o "client/server". A questo livello le applicazioni si scambiano messaggi e non più semplici dati.



modello ISO/OSI a 7 livelli

pacchetti con una serie di regole sui permessi di accesso interni ed esterni. Tipicamente esso blocca alcuni tipi di socket, rifiutando a determinati utenti interni alcuni servizi Internet e bloccando alcune porte delle macchine interne.



router / gateway

Modello TCP/IP

Il modello semplificato di rete TCP/IP a 4 livelli è, grazie ad Internet, oramai standard di fatto delle architetture di rete. La semplificazione riguarda i livelli superiori della pila Osi.

TCP/IP (a 4 livelli)	OSI (a 7 livelli)
4 – <i>Applicazioni</i>	7 – <i>Applicazioni</i>
	6 – <i>Presentazione</i>
	5 – <i>Sessione</i>
3 – <i>Trasporto (TCP)</i>	4 – <i>Trasporto</i>
2 – <i>Rete (IP)</i>	3 – <i>Rete</i>
1 – <i>Fisico</i>	2 – <i>Collegamento dati</i>
	1 – <i>Fisico</i>

Livello 1 – FISICO

I protocolli del livello **FISICO** sono implementati dall'hardware di rete e trattano le specifiche elettriche e meccaniche della rete, si occupano della trasmissione dei bit nel canale di comunicazione [livello Fisico], organizzano i messaggi in pacchetti, elaborano le risposte del ricevente [livello di Collegamento Dati] e sincronizzano le diverse velocità di trasmissione / ricezione [prima parte del livello di Rete].

A questo livello si hanno le reti fisiche IBM Token Ring, Ethernet, FireWire. Lo standard di fatto è Ethernet (standard IEEE 802.3) con tecnica di trasmissione CSMA/CD. I pacchetti di dati inviati sulle reti Ethernet vengono chiamati trame¹⁹ (*frame*). In esse sia il nodo mittente che quello destinatario sono identificati mediante l'indirizzo MAC delle relative NIC.

A questo livello appartengono i cavi (coassiali o twisted pair STP e UTP), i connettori (BNC e RJ45), le schede di rete NIC alloggiate in appositi slot²⁰ di espansione, gli Hub, gli Switch, i Gateway. A questo livello appartengono anche i protocolli HDLC, BSC e PPP.

Livello 2 – RETE (protocollo IP)

I protocolli del livello di **RETE** si occupano della traduzione degli indirizzi fisici in indirizzi logici e viceversa (ARP) e dell'inoltro dei pacchetti dal mittente al destinatario (IP) [seconda parte del livello di Rete].

Per la traduzione degli indirizzi fisici MAC in indirizzi logici IP e viceversa si usa il protocollo ARP²¹ (*Address Resolution protocol*). Se l'indirizzo IP non appartiene alla Lan la risoluzione ARP dello stesso viene demandata al Gateway.

¹⁹ **frame**: le trame, cioè i pacchetti dati inviati sulle reti Ethernet, sono così strutturate:

8	6	6	2	da 46 a 1.500	4
preambolo	ind.MAC destinatario	ind.MAC mittente	lunghezza	dati	controllo errori

Il preambolo serve per permettere alla stazione ricevente di sincronizzarsi sul segnale di clock della stazione trasmittente.

²⁰ **Slot**: i principali slot di espansione sono ISA (*Industry Standard Architecture*) a 16 bit e 8 Mhz, EISA (*Extended ISA*) a 32 bit e 32 Mhz, VESA/VLB bus locale nato per lavorare con i processori 486, PCI (*Peripheral Component Interconnect*) a 32 bit e con velocità teorica fino a 128 Mbps.

²¹ **protocollo ARP**: una macchina A, a partire dall'indirizzo IP, manda un messaggio broadcast - *ARP request* – per trovare l'indirizzo fisico della macchina destinataria B. Quella cui corrisponde l'indirizzo IP risponde inviando ad A il proprio indirizzo MAC

A questo livello si colloca il **protocollo IP** (*Internet Protocol*), un protocollo che garantisce la comunicazione anche tra computer diversi e con sistemi operativi diversi.

Tale protocollo ha il compito di definire i meccanismi di indirizzamento tra reti diverse di computer, instradare i singoli pacchetti portandoli a destinazione, frammentare ulteriormente i datagrammi nel caso di attraversamento di reti in cui la dimensione del frame è minore di quella del pacchetto in transito (in questo caso i frammenti possono arrivare a destinazione anche non in sequenza).

L'indirizzo IP che caratterizza ogni nodo della rete è un indirizzo IPV4 di 4 byte del tipo xxx.xxx.xxx.xxx (xxx da 0 a 255) che identifica sia la rete di appartenenza che l'host all'interno della rete stessa. Tali indirizzi IP, raggruppati in classi²², sono assegnati dal **Garr** (*Gruppo di Autoregolamentazione delle Reti per la Ricerca*). A chi si collega in internet l'indirizzo IP viene fornito dinamicamente dal provider e cambia da collegamento a collegamento (è però possibile, a richiesta, avere un proprio IP statico). A causa della crescente scarsità di indirizzi IPV4 è allo studio il

²² **Indirizzi IP:** gli indirizzi IPV4 sono poco più di 4 miliardi ($2^{32} = 4.294.967.269$) e sono suddivisi nelle seguenti classi:

- A. classe **A** [0] da 1.xxx.xxx.xxx a 126.xxx.xxx.xxx, il primo byte identifica la rete, i restanti l'host, 126 reti ciascuna delle quali può avere 16.777.214 host, classe usata agli esordi per grandissime reti.
- L. 127.xxx.xxx.xxx, indirizzo riservato per il loopback [127.0.0.1]
- B. classe **B** [10] da 128.xxx.xxx.xxx a 191.xxx.xxx.xxx, i primi due byte identificano la rete, i restanti l'host, 16.384 reti ciascuna delle quali può avere 65.534 host, classe usata per grandi organizzazioni.
- C. classe **C** [110] da 192.xxx.xxx.xxx a 223.xxx.xxx.xxx, la classe riservata alle reti locali, i primi tre byte identificano la rete, l'ultimo l'host, 2.097.152 reti ciascuna delle quali può avere 254 host – gli indirizzi 0 e 255 sono riservati, classe per piccole e medie organizzazioni.
- D. classe **D** [1110] da 224.xxx.xxx.xxx. a 239.xxx.xxx.xxx, per trasmissioni multicast, con un solo host che trasmette e tutti gli altri che ricevono
- E. classe **E** [1111] da 240.xxx.xxx.xxx a 254.xxx.xxx.xxx, per utilizzi futuri
- X. 255.xxx.xxx.xxx, indirizzo riservato al broadcast di tutta la rete

Ogni host della rete è individuato dal proprio indirizzo IP **pubblico**, univoco a livello mondiale. L'indirizzo 0.0.0.0 indica l'host corrente senza specificarne l'indirizzo.

Classe A indirizzi da 1.0.0.0 a 127.255.255.255				
0	Rete	Host	Host	Host
Classe B indirizzi da 128.0.0.0 a 191.255.255.255				
1 0	Rete	Rete	Host	Host
Classe C indirizzi da 192.0.0.0 a 223.255.255.255				
1 1 0	Rete	Rete	Rete	Host
Classe D indirizzi da 224.0.0.0 a 239.255.255.255				
1 1 1 0				
Classe E indirizzi da 240.0.0.0 a 255.255.255.255				
1 1 1 1 0				

Per le reti locali sono disponibili, perché non utilizzati in Internet, alcuni indirizzi **privati** riservati (non raggiungibili dalla rete pubblica): per la classe A sono disponibili gli indirizzi da 10.0.0.0 a 10.255.255.255, per la classe B sono disponibili gli indirizzi da 172.16.0.0 a 172.16.255.255 e per la classe C quelli da 192.168.0.0 a 192.168.255.255. Per collegare la rete locale ad internet occorre un gateway che faccia da ponte. La **subnetmask**, maschera di sottorete, serve per poter stabilire quali indirizzi appartengono alla LAN e quali sono esterni. Per indirizzi di classe A la subnetmask è 255.0.0.0, per quelli di classe B è 255.255.0.0, per indirizzi di classe C è 255.255.255.0. Lo 0 è la parte di indirizzo riservata agli host della sottorete. Con un AND logico tra l'indirizzo IP e la subnetmask si stabilisce l'**indirizzo di rete** e se tale indirizzo appartiene ad una macchina della LAN o è esterno. Se indirizzo IP è 207.168.99.100 e la subnet è 255.255.255.0, l'indirizzo di rete sarà 207.168.99.0. Gli host con l'indirizzo di rete uguale appartengono alla stessa LAN e possono comunicare direttamente, per gli altri occorre avvalersi di un gateway o di un router.

Gli indirizzi IP **pubblici** sono distribuiti dagli **ISP** (*Internet Service provider*), aziende che dispongono di intere classi, generalmente di tipo B, che danno ai propri clienti in modo **dinamico** (al momento della connessione; al termine della connessione l'indirizzo può essere assegnato ad un altro cliente) o in modo **statico** (attribuito in modo permanente per un lungo periodo di tempo)

passaggio ad indirizzi IPV6²³. L'instradamento dei pacchetti - datagrammi²⁴ - da una rete all'altra, in base all'indirizzo IP di rete del destinatario, viene fatto dal Router (gateway, porta di interconnessione) che allo scopo utilizza opportune tabelle di instradamento (tabelle di routing) che contengono gli indirizzi dei router "vicini" e le informazioni che consentono la scelta della strada sulla quale "instradare" il pacchetto²⁵.

²³ **IPV4 e IPV6:** gli indirizzi IPV4 a 4 byte - 2^{32} indirizzi, 4.294.697.296 - cominciano a scarseggiare, le prime due classi sono già quasi sature e resta la classe C, con proliferazione di reti locali "invisibili" ad internet ma ad essa collegate tramite gateway o router. Questo consente di risparmiare indirizzi IP, ma appesantisce le tabelle di routing e l'instradamento dei pacchetti. È allo studio il passaggio ad indirizzi IPV6 a di 16 byte - 2^{128} indirizzi - permetterebbe di dare un IP statico ad ogni dispositivo connesso ad internet, senza bisogno di alcun meccanismo di traduzione, come attualmente avviene. Il passaggio da Ipv4 a Ipv6 non richiede però solo un aggiornamento dei driver del sistema operativo, ma anche la riprogrammazione delle applicazioni.

²⁴ **datagramma:** il datagramma, **pacchetto IP** (*Internet Protocol*), è così strutturato:

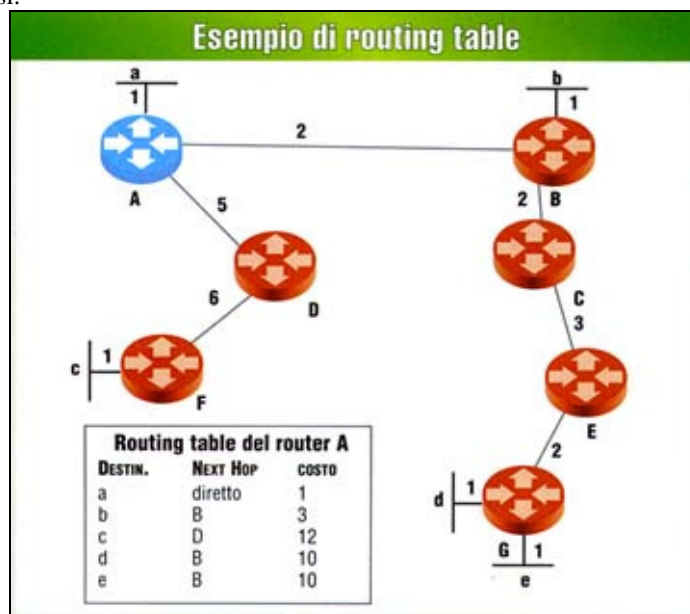
1 byte		1 byte		1 byte		1 byte	
Version	IHL	Service type		Packet lenght			
Identification				Flags	Fragment offset		
Time live		Protocol		Header checksum			
Source address							
Destination address							
Options					Paddin		
dati utente							

- Version: versione, per formato intestazione, attualmente versione 4 (IPV4), ma si sta lavorando alla 6 (IPV6)
- IHL: lunghezza intestazione
- Type of service: tipo di servizio, dice ad IP come gestire il pacchetto e la sua priorità
- Packet length: lunghezza totale – intestazione e dati - del datagramma in byte, massimo 65535
- Identification: numero che identifica univocamente il datagramma, usato per risalire a quale datagramma appartengono i frammenti nei quali eventualmente viene scomposto il datagramma
- Flag: tre bit – primo sempre a 0; secondo a 0 se si può frammentare, ad 1 se non si può frammentare; terzo a 0 se è l'ultimo pacchetto, a 1 se non è l'ultimo pacchetto
- Fragment offset: indica la posizione di questo frammento nel datagramma, serve per riassemblare i frammenti e ricostruire il datagramma
- Time to live: tempo massimo di permanenza del datagramma nella rete, viene decrementato da ogni nodo [router] attraversato (una volta arrivato a 0 il datagramma verrà distrutto)
- Protocol: indica a quale protocollo di livello superiore appartengono i dati del datagramma
- Header checksum: controllo di errore della sola intestazione, viene ricalcolato e confrontato da ogni nodo attraversato dal datagramma
- Source address: indirizzo IP del nodo mittente
- Destination address: indirizzo IP del nodo destinazione
- Options: opzioni sul trasferimento del datagramma quali registrazione percorso e meccanismi di sicurezza
- Padding: bit riempitivi per rendere la lunghezza dell'intestazione multipla di 32 bit

²⁵ **routing:** il routing è l'instradamento dei pacchetti effettuato dai router. Un router può essere visto come una centrale telefonica e funziona in maniera analoga. Gli stessi indirizzi IP vengono assegnati anche in base alla collocazione geografica della rete, analogamente al prefisso telefonico. Il router della LAN sarà collegato al router del provider; quest'ultimo sarà collegato ad altri router di livello superiore, e così via. La *tabella di instradamento (routing)* del router può essere statica, e allora si parla di routing statico, o dinamica, nel qual caso si parla di routing dinamico, con la tabella di instradamento che periodicamente viene aggiornata automaticamente dal router stesso che "chiede" informazioni ai router vicini cui è collegato. Quando il router invia un pacchetto lungo una linea attende la conferma di ricezione del pacchetto; se la conferma non giunge entro un determinato lasso di tempo, ritrasmette il pacchetto su un'altra linea, ma se ciò non fosse possibile avvisa chi ha chiamato che a sua volta tenterà un'altra strada. Il passaggio del pacchetto tra un router e l'altro è un *hop*, salto. In Internet i pacchetti possono fare al massimo 15 salti (*time live*), dopo di che la rete di destinazione è considerata irraggiungibile e il mittente riceve un messaggio di errore. Il limite dei 15 salti è una specifica del **RIP** (*Routing Information Protocol*), il protocollo utilizzato dai router.

La tabella di instradamento non contiene solo gli indirizzi delle reti e degli host, ma anche altre informazioni, quali il tipo di interfaccia fisica utilizzata, la distanza, il ritardo, etc. Una piccola tabella di instradamento è contenuta in tutti i computer -

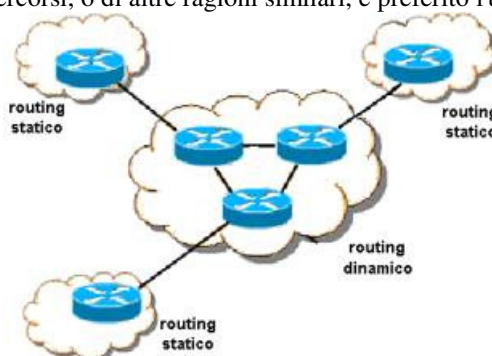
la si può visualizzare con il comando *route* - che hanno sempre almeno due reti cui riferirsi: quella di loop 127.0.0.1 e la LAN alla quale sono connessi.



Gli algoritmi di **routing statico** sono: *a cammino minimo* (*shortest path routing* - sceglie il cammino minimo tra due router), *flooding* (reinvia il pacchetto su tutte le linee tranne quella di provenienza), *a ritardo minimo* (*flow-based routing* - sceglie il cammino più veloce).

Gli algoritmi di **routing dinamico** sono: *basato sulla distanza* (*distance vector routing*- la tabella di routing viene aggiornata con regolarità sfruttando i dati acquisiti dal router stesso sui router adiacenti, che avviene mandando speciali pacchetti *ECHO*, e le tabelle dei router adiacenti; ogni router riceve la tabella dei vicini e manda la propria agli stessi e provvede a calcolare la concatenazione migliore per ogni destinazione; questo algoritmo è usato in Internet col nome di **RIP** - *Routing Internet Protocol*), *basato sullo stato dei collegamenti* (*link state routing* - ogni router analizza lo stato dei collegamenti con i suoi vicini ed invia tali informazioni a tutti gli altri, ricevendo da questi informazioni dello stesso genere.; la tabella di routing viene aggiornata in seguito ad eventi significativi o ad intervalli regolari ed è formata ricostruendo la struttura topologia della rete e calcolando il cammino minimo con tutti gli altri; un pacchetto tipico, oltre ad *ECHO*, è *HELLO* che viene inviato all'avvio del router e in risposta al quale ogni router invia il proprio indirizzo; questo algoritmo è usato in Internet col nome di **OSPF** - *Open Shortest Path First*).

Il routing statico è preferito in situazioni periferiche di dimensioni ridotte o in condizioni di gestione semplificata dell'intera rete. Invece dove sono possibili frequenti cambi di topologia, variazioni di prestazioni in dipendenza del carico di lavoro dei router e dei link, dei guasti e dei percorsi, o di altre ragioni similari, è preferito l'utilizzo del routing dinamico.



Routing gerarchico. Per semplificare il lavoro dei router nella raccolta dei dati e nella formulazione delle tabelle di routing si fa ricorso ad una struttura di tipo gerarchico. Per evitare l'acquisizione e il mantenimento dell'intera topologia, la rete viene divisa in zone o regioni: i router presenti all'interno di una regione (*router interni*) hanno dati di routing relativi ad ogni altro router della regione ; i router di una regione che devono spedire dati in un'altra regione sanno che devono passare attraverso un particolare router della propria regione (*router di confine*); i router di confine che devono far arrivare dati in un'altra regione sanno a quale router dell'altra regione (sempre di confine) devono spedire i dati.

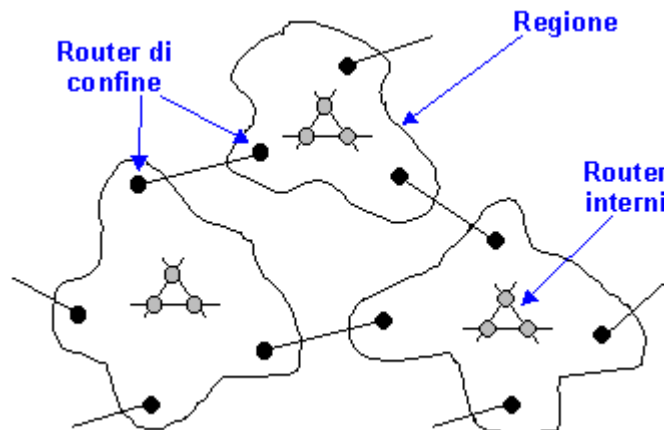
Con questa modalità di instradamento si possono identificare almeno due livelli di routing: il primo si ha all'interno di ogni regione (in questo caso le tabelle di routing contengono una voce per ogni altro router interno e per ogni altra regione, con l'indicazione del router di confine e della linea da percorrere); il secondo si svolge tra tutti i router di confine (in questo caso

Livello 3 – TRASPORTO (protocollo TCP)

I protocolli del livello di **TRASPORTO** - quali TCP e UDP - rendono possibile la comunicazione tra computer collegati a reti diverse, si occupano di suddividere il messaggio in pacchetti da inviare e di riassemblare i pacchetti ricevuti [livello di Trasporto].

A questo livello operano diversi protocolli, primo fra tutti il protocollo **TCP**²⁶ (*Transfer Control Protocol*), un protocollo orientato alla connessione che si occupa della suddivisione dei messaggi in pacchetti (in trasmissione) e della ricomposizione dei pacchetti nel messaggio (in ricezione). TCP stabilisce la connessione²⁷ con il destinatario del messaggio inviando opportuni pacchetti di controllo,

le tabelle di routing contengono una voce per ogni altra regione, con l'indicazione del router di confine e della linea da percorrere).



²⁶ **protocollo TCP** (*Transfer Control Protocol*): il formato di un pacchetto TCP ha la seguente struttura:

1 byte		1 byte		1 byte		1 byte	
Source port				Destination port			
Sequence number							
Acknowledgment number							
HLEN	Reserved	Flags		Windows size			
Cheksum				Urgent pointer			
dati utente							

- Source port: 16 bit, identifica l'applicazione che invia i dati
- Destination port: 16 bit, identifica l'applicazione che riceve i dati. Queste due porte, combinate con i rispettivi indirizzi IP, identificano univocamente la connessione
- Sequence number: 32 bit, è il numero di sequenza del primo byte di questo segmento
- Acknowledgment number: 32 bit, numero di "ack", indica il prossimo byte atteso (e non l'ultimo correttamente spedito)
- HLEN (header length): 4 bit, dimensione dell'header TCP in parole di 32 byte
- Reserved: 6 bit, inutilizzato
- Flags: 6 bit così strutturati: 1-URG (se 1 è valido il campo urgent pointer), 2-ACK (se 1 il campo numero di Acknowledgment è valido), 3-PSH (se 1 indica dati di tipo "push"), 6-RST (reset the connection, se 1 indica la necessità di reinizializzare una connessione), 5-SYN (utilizzato per creare, cioè "sincronizzare", connessioni - vedi più sotto la sincronizzazione), 6-FIN (se 1 indica che è la dfine della connessione perché il mittente non ha più dati da spedire)
- Windows size: 16 bit, indica quanti byte possono essere spediti (se 0 indica che il ricevente per il momento non vuole ricevere ulteriori dati)
- Checksum: 16 bit, per il controllo degli errori.
- Urgent pointer:

²⁷ **connessione**: il processo attraverso il quale si stabilisce una sessione di comunicazione tra due macchine è detto "handshaking – stretta di mano – a tre vie" perché i passi per stabilire la connessione sono i seguenti:

- a) Il client (mittente) invia al server (destinatario) un pacchetto di richiesta dove specifica il numero di porta (applicazione) che vuole usare ed il suo numero di sequenza iniziale (ISN)

così come quando interrompe la connessione. Per ogni pacchetto ricevuto il TCP del destinatario invia conferma di corretta ricezione. Se un pacchetto non giunge a destinazione o giunge errato, il TCP del mittente provvede alla sua ritrasmissione. TCP interagisce direttamente con le applicazioni dei livelli superiori che comunicano tra di loro utilizzando tale protocollo. TCP aggiunge all'header di ogni pacchetto il numero di porta (2 byte), ciascuno dei quali equivale ad una determinata applicazione²⁸.

Un altro protocollo di questo livello è UDP²⁹ (*User Datagram Protocol*), non orientato alla connessione, utilizzato quando l'affidabilità non è essenziale. Tale protocollo ha il compito di gestire trasmissioni (anche multi cast o broadcast) tra host senza garantire la corretta consegna dei pacchetti. Il controllo viene demandato ai protocolli applicativi che ne fanno uso. I vantaggi nell'utilizzo di UDP sono infatti la velocità, e la minore congestione di rete rispetto a TCP (non ci sono pacchetti di conferma) e la possibilità di trasmettere in multicast (invio di un pacchetto ad un gruppo di host) e broadcast (invio di un pacchetto a tutti gli host di un segmento di rete). Questo protocollo si può usare in rete locale, quando il pacchetto contiene tutto il messaggio (non si apre la connessione), non è necessario che tutti i pacchetti arrivino a destinazione, l'applicazione gestisce meccanismi di ritrasmissione. Tale protocollo è usato nelle applicazioni che richiedono elevata velocità di trasmissione, anche con errori, quali la videoconferenza e la telefonia via Internet.

A questo livello appartiene anche il Router, e i protocolli di routing.

Livello 4 – APPLICAZIONI

A questo livello delle **APPLICAZIONI** si stabilisce la sessione tra i due computer coinvolti, si sfrutta la bidirezionalità del canale full-duplex, si sincronizzano i processi, ci si occupa del login delle password, dei permessi di accesso [livello di Sessione]; si definiscono le modalità di interpretazione dei dati - ASCII a 8 bit -, la sintassi e la semantica delle informazioni tramite il linguaggio HTML [livello di Presentazione]; si gestiscono i vari tipi di terminali, si definisce il tipo di interazione con l'utente, si usano i principali protocolli quali HTTP e FTP [livello di Applicazione].

- b) Il server risponde al client con un pacchetto contenente il suo ISN ed un acknowledgement distinto da quello del client, a cui è sommato 1
- c) Il client riconosce l'ISN del server e da inizio alla sessione

²⁸ **porte TCP:** le "porte" del protocollo TCP servono per far comunicare applicazioni diverse su computer diversi. Per ogni indirizzo IP esistono 65.535 diverse porte. Ad ogni porta è associata un'applicazione [20 e 21 Ftp, 23 Telnet, 25 Sntp, 53 Dns, 80 Http, 110 Pop, 119 Nntp, 135 Dcom, 143 Imap, 517 Talk, messaggi immediati, 6667 Irc, etc]. Teoricamente un'applicazione potrebbe funzionare su una qualsiasi delle 65536 porte di TCP e UDP, ma solo le prime 1023 sono utilizzate. Se si definiscono, su un server web, porte alternative dal client per effettuare il collegamento occorre specificare esplicitamente anche la porta (es. <http://192.168.99.60:2341>). L'indirizzo IP più il numero di porta costituisce il **socket**.

²⁹ **protocollo UDP** (*User Datagram Protocol*): il formato di un pacchetto UDP non è molto complesso ed è così strutturato:

1 byte	1 byte	1 byte	1 byte
Source port		Destination port	
Message		Checksum	
dati utente			

- Source Port: campo di 16 bit (facoltativo), contiene la porta UDP di origine dell'host sorgente;
- Destination Port: campo di 16 bit, contiene la porta UDP di destinazione del pacchetto sull'host remoto;
- Length: campo di 16 bit, contiene la lunghezza in byte dell'istanza UDP e dei dati;
- Checksum: campo di 16 bit, è utilizzato per verificare l'integrità dei dati trasportati;
- Data: campo di lunghezza variabile contenente i dati;

La trasmissione di un pacchetto UDP avviene incapsulandolo all'interno di un pacchetto IP. Giunto a destinazione, il pacchetto viene inviato alla porta di destinazione indicata nell'istanza UDP. Qualora la porta non fosse disponibile, viene inviato un pacchetto ICMP (Internet Control Message Protocol) all'host mittente con messaggio di port unreachable (porta irraggiungibile).

UDP viene utilizzato da protocolli come TFTP (*Trivial File Transfer Protocol*), SNMP (*Simple Network Management Protocol*), DNS (*Domain Name Server*), per l'invio di stream audio, ed è ampiamente usato nelle applicazioni videoludiche.

I protocolli del livello delle Applicazioni sono quelli che risolvono gli indirizzi – quali il **DNS**³⁰ (*Domain Name System*) - per la risoluzione dei nomi di dominio³¹ (o indirizzi internet) in indirizzi IP e viceversa e quelli delle applicazioni di rete quali HTTP (*Hiper Text Transfer Protocol*), FTP (*File Transfer Protocol*), SMTP (*Simple Mind Transfer Protocol*), POP (*Post Office Protocol*), NNTP (*Network News Transfer Protocol*), TELNET, etc.

Le applicazioni di rete si connettono tra di loro utilizzando come interfaccia di collegamento i socket³², connessioni bidirezionali (date da Indirizzo IP + numero di porta) che consentono di stabilire e mantenere la comunicazione.

Altri protocolli

Lo standard Tcp/Ip non è l'unico protagonista nel mondo delle reti. Esistono altri standard, molti di essi preesistenti e che ora si affiancano a Tcp/Ip, quali quelli per **reti Microsoft**³³, reti **Appletalk**³⁴ e reti **Ipx/Spx**³⁵.

³⁰ **protocollo DNS** (*Domain Name System*): risolve gli indirizzi internet (nomi di dominio, tipo www.libero.it) in indirizzi IP (tipo 158.23.89.120). È un protocollo gerarchico (ogni server DNS fa riferimento a server di livello superiore) e distribuito (le tabelle di corrispondenza degli indirizzi sono distribuiti su più server). Ogni macchina collegata alla rete ha nei propri parametri di collegamento l'indirizzo IP del DNS di riferimento al quale invierà l'indirizzo internet con cui vuole connettersi e riceverà in risposta il relativo indirizzo IP. Se il server DNS interpellato non risolve l'indirizzo, inoltra la richiesta ad un server di livello superiore che, se non in grado di risolvere l'indirizzo, può a sua volta inoltrare la richiesta ad un server di livello superiore o reindirizzarla "in basso", ad un server di livello inferiore (magari, dopo aver determinato la sottoarea geografica, la rinvia in basso al DNS che si occupa di tale sottoarea), fino ad arrivare all'host finale ed al suo indirizzo IP.

Utilizzando il comando *ping* dal prompt dei comandi si può verificare la presenza di un host e avere il suo indirizzo IP: *ping indirizzo_Internet* restituisce l'indirizzo IP: *ping indirizzo_IP* verifica se l'host è collegato (ad esempio il comando *IP: ping www.google.it* restituisce l'indirizzo IP di Google Italia, che è 74.125.39.99)

³¹ **nome di dominio**: un nome di dominio o indirizzo internet è l'indirizzo mnemonico di un sito o di una risorsa internet del tipo *host.dominio*, dove il dominio è una rete locale o estesa e l'host è un determinato computer all'interno della rete stessa. Tali indirizzi sono organizzati in domini, sottodomini, host del tipo www.ferrari.it, dove *it* è il dominio di primo livello, *ferrari* è il dominio di secondo livello, e *www* indica che si tratta di un sito World Wide Web. L'ultima parte del nome di dominio identifica o la nazione di appartenenza o l'organizzazione: it (Italia), fr (Francia), uk (Gran Bretagna), com (azienda commerciale), edu (scuola o università), gov (ente governativo), mil (organizzazione militare), int (organismo internazionale), net (fornitore di accesso e di servizi di rete), org (altro tipo di organizzazione)

³² **Socket**: il socket rappresenta una connessione in entrata e in uscita (bidirezionale) definita dall'indirizzo IP del sistema che ospita l'applicazione, dal numero di porta che l'applicazione ha aperto sulla rete e dal tipo di socket, ovvero dal tipo di protocollo di trasporto che utilizza (principalmente Tcp o Udp). Perché la comunicazione sia possibile debbono essere presenti due socket, quello del client e quello del server.

³³ **reti Microsoft**: i protocolli per Lan peer to peer utilizzati da Microsoft nei sistemi Windows per la condivisione di file e stampanti sono **SMB** (*Server Message Block*) per la condivisione delle risorse e la gestione dei messaggi – si colloca a livello di presentazione - e **NetBios** (*Network Basic Input Output System*) per stabilire e mantenere la connessione - si colloca a livello di sessione -. Tali protocolli, entrambi a livello di applicazione nel Tcp/Ip, convivono con i protocolli Tcp/Ip e possono utilizzare, al posto di questo, il protocollo di trasporto **Netbeui** (*Net Bios Enhanced User Interface*) o l'Ipx/Spx delle reti Novell. La sigla SMB ha dato origine al nome del pacchetto **Samba** di Linux, responsabile del supporto alle reti Microsoft del sistema del pinguino.

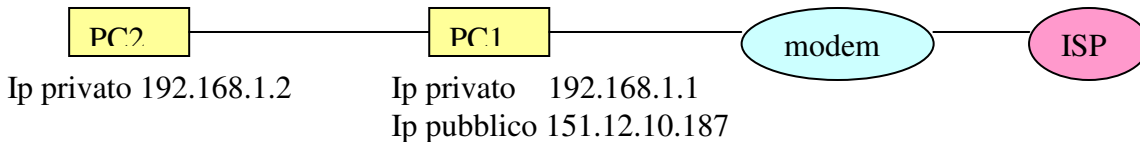
³⁴ **reti Appletalk**: Appletalk è un gruppo di protocolli Apple per l'implementazione di Lan Macintosh. Serve a condividere file e stampanti. Supporta reti logiche multiple, ma è incompatibile con le reti Microsoft, mentre è supportato da Linux.

³⁵ **reti Ipx/Spx**: Ipx (*Internetwork Packed Exchange*) e Spx (*Sequenced Racket Exchanged*) sono un gruppo di protocolli di rete e di trasporto utilizzati nelle reti client/server Netware di Novell. Sono molto semplici e veloci e le Lan possono essere interconnesse tra loro perché Ipx/Spx supporta il routing dei pacchetti. Il server Netware funziona sia da server di condivisione delle risorse che da bridge di rete. La versione Microsoft di Ipx/Spx è NWLink.

LAN domestiche e INTERNET

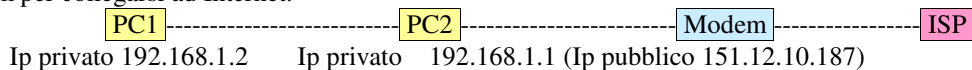
Internet è una "rete di reti" che collega tra di loro reti diverse. Si possono avere semplicissime LAN costituite da due soli PC, LAN che comunicano accedono ad Internet mediante Server/Proxy e LAN che accedono ad Internet mediante Router.

LAN di due computer³⁶: Per collegare in rete due computer occorre un cavo incrociato per collegare le schede di rete ed il modem per connettersi ad Internet.



LAN con Server/Proxy³⁷ Oltre ai cavi di rete, occorre un Concentratore (Hub o Switch). Il PC collegato ad Internet è il PC Server e funge anche da Gateway . Occorre installare su tutti i PC (sia Server che Client) un particolare software **Proxy** (quale, ad esempio, WinGate). I client hanno un indirizzo IP privato, mentre il server ha sia un indirizzo IP privato (quello della LAN) che un indirizzo IP pubblico, fornito dall'ISP al momento della connessione.

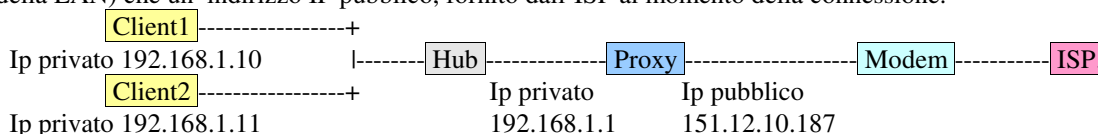
³⁶ **LAN di due computer**: per collegare in rete due computer occorre un cavo incrociato per collegare le schede di rete ed il modem per collegarsi ad Internet.



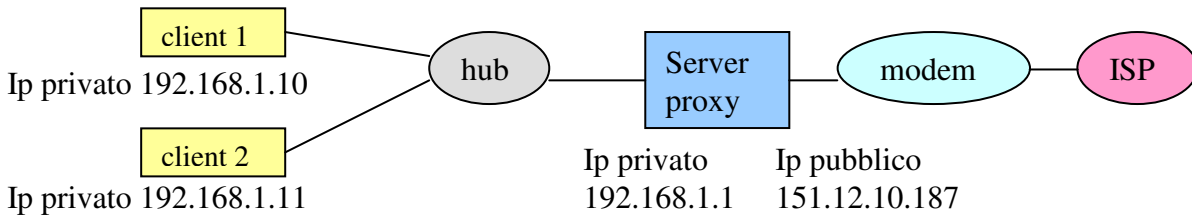
Nel caso di **Windows 95/98/Me** occorre la presenza del "Client per reti Microsoft", del "Dispositivo di accesso remoto" e del relativo "TCP/IP". Si definisce un gruppo di lavoro comune, si identificano i PC e si assegnano gli indirizzi IP, quali ad esempio 192.168.1.1 per PC1, 192.168.1.2 per PC2 e 255.255.255.0 come Subnet Mask per entrambi. Se il PC1 è connesso ad internet e si desidera condividere la commessione con PC2 occorre installare nel PC1 un programma tipo WinGate ed impostare sulla scheda "Gateway" del PC2 l'indirizzo IP del PC1 (192.168.1.1) e nella scheda "Configurazione DNS", dopo aver abilitato "Attiva DNS", gli indirizzi IP delle macchine DNS del provider.

Nel caso di **Windows 2000/XP** si usa "Connessione alla rete locale" del pannello "Rete e connessione remota", si attivano "Client per reti Microsoft", "Condivisione file e stampanti per reti Microsoft" e "Protocollo Internet TCP/IP" e si assegnano gli indirizzi da proprietà di Protocollo TCP/IP. Se il PC1 è connesso ad internet e si desidera condividere la commessione con PC2 occorre installare nel PC1 un programma tipo WinGate, aggiungere in PC1 gli indirizzi DNS dell'ISP, mentre nel PC2 si imposta nel campo Gateway predefinito l'indirizzo IP del PC1 (192.168.1.1), si seleziona "Utilizza i seguenti indirizzi server DNS" e si digitano nel campo "Server DNS predefinito" ancora gli indirizzi DNS dell'ISP. È inoltre necessario abilitare "Non utilizzare mai connessioni remote" presente in Strumenti/ Opzioni/ Connessioni di Internet Explorer, richiamare le proprietà della connessione ad internet che si desidera condividere – tasto destro sull'icona di connessione presente su PC1 – e nella scheda "Condivisione" selezionare "Abilita condivisione connessione Internet per questa connessione". Se non si imposta "Abilita connessione a richiesta" PC2 accederà ad Internet solo se PC1 è già connesso, mentre se la si imposta PC1 si collegherà ad Internet anche a richiesta di PC2.

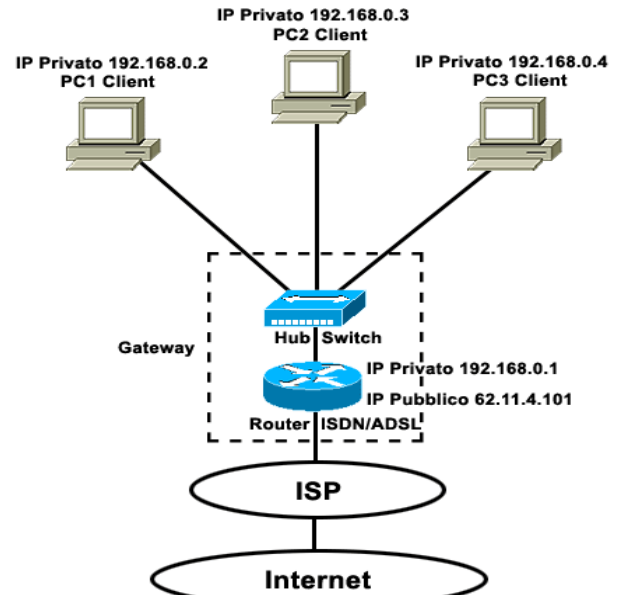
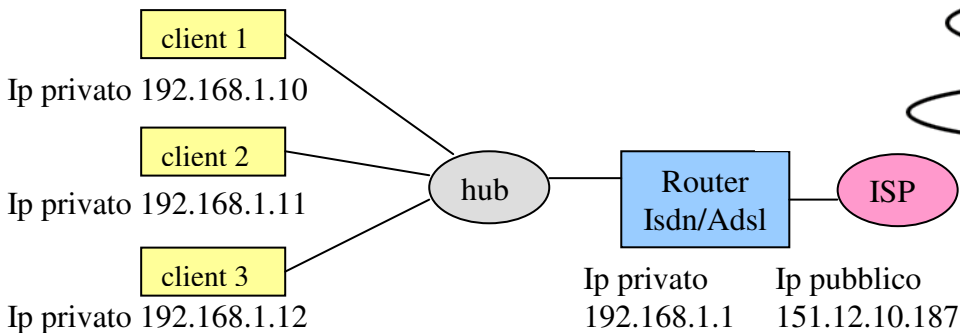
³⁷ **LAN con server Proxy**: oltre ai cavi di rete, occorre un Concentratore (Hub o Switch). Il PC collegato ad Internet è il PC Server (offre il servizio della condivisione dei servizi Internet ai client della LAN) e funge anche da Gateway (mette in collegamento la mini LAN con Internet). Occorre installare su tutti i PC (sia Server che Client) un particolare software **Proxy** (quale, ad esempio, WinGate). I client hanno un indirizzo IP privato, mentre il server ha sia un indirizzo IP privato (quello della LAN) che un indirizzo IP pubblico, fornito dall'ISP al momento della connessione.



Il PC Client che vuole accedere a un sito Internet invia la richiesta, tramite il browser, al PC Proxy (Gateway), attraverso pacchetti TCP/IP comprensivo di indirizzo IP del destinatario e del mittente. Il gateway, prima di inviare la richiesta sostituisce l'IP privato del mittente con il proprio IP pubblico ottenuto dal provider al momento della connessione. Quando riceve la risposta la invia al PC che l'aveva richiesta (si veda la nota "Traduzione degli indirizzi IP privati").

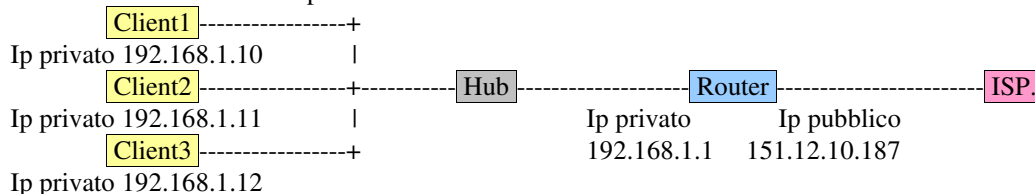


LAN con Router³⁸ Oltre ai cavi di rete, occorre un Concentratore (Hub o Switch). Al posto del PC collegato ad Internet (Server/Proxy) c'è il **Router**, un dispositivo senza tastiera e mouse in grado di effettuare la connessione telefonica (ISDN/ADSL) e, attraverso un software NAT o Proxy, di condividere la connessione tra tutti i computer della LAN. Il router collegato ad Internet è il Server/Gateway (mette in collegamento la mini LAN con Internet). Se il router svolge anche le funzioni di concentratore si può fare a meno dell'Hub/Switch.



L'assegnazione degli **IP privati** ai computer della LAN può essere fatta "manualmente" oppure utilizzando un apposito servizio che si avvale del protocollo **DHCP**³⁹ (*Dinamic Host Configuration Protocol*).

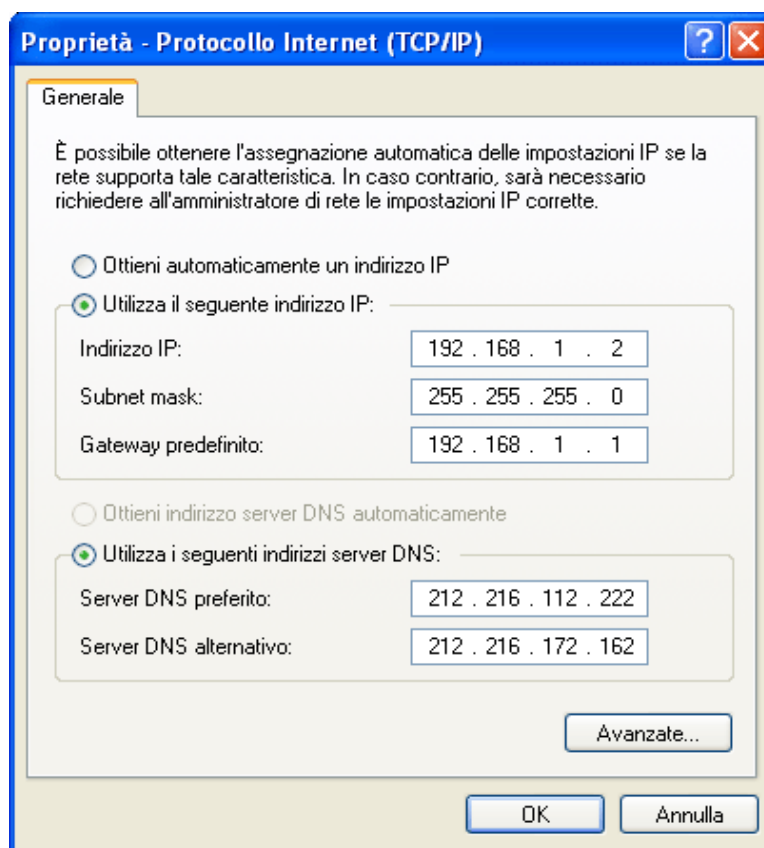
³⁸ **LAN con Router:** oltre ai cavi di rete, occorre un Concentratore (Hub o Switch). Al posto del PC collegato ad Internet (Server/Proxy) c'è il **Router**, un dispositivo senza tastiera e mouse in grado di effettuare la connessione telefonica (ISDN/ADSL) e, attraverso un software NAT o Proxy, di condividere la connessione tra tutti i computer della LAN. Il router collegato ad Internet è il Server/Gateway (che mette in collegamento la mini LAN con Internet). Se il router svolge anche le funzioni di concentratore si può fare a meno dell'Hub/Switch.



Il PC Client che vuole accedere a un sito Internet invia la richiesta, tramite il browser, al Router (Gateway), attraverso pacchetti TCP/IP comprensivo di indirizzo IP del destinatario e del mittente. Il gateway, prima di inviare la richiesta sostituisce l'IP privato del mittente con il proprio IP pubblico ottenuto dal provider al momento della connessione. Quando riceve la risposta la invia al PC che l'aveva richiesta (si veda la nota "Traduzione degli indirizzi IP privati").

³⁹ **protocollo DHCP** (*Dinamic Host Configuration Protocol*): è un protocollo di rete che permette ai dispositivi che ne facciano richiesta di essere automaticamente configurati per entrare a far parte della LAN, al momento del boot, senza dover essere configurati "manualmente". È molto comodo soprattutto nel caso di PC portatili in quanto, per connettersi alla LAN, basta inserirsi alla presa e il DHCP farà il resto. Il DHCP assegna, oltre all'indirizzo IP, i due indirizzi DNS, i due

Per assegnare manualmente gli indirizzi IP privati, con Windows XP, si utilizza la finestra Proprietà del Protocollo Internet (TCP/IP):



server WINS e l'indirizzo dell'eventuale Gateway che il client dovrà utilizzare. Gli indirizzi IP da assegnare ai client vengono configurati nel database del server DHCP chiamato **scope** che li assegna e la loro validità è garantita per un determinato periodo di tempo chiamato **lease**. Il processo di configurazione avviene in tre fasi.

- Richiesta IP. Inizialmente il client configura 'sommariamente' il TCP/IP per ricevere automaticamente un IP dal server DHCP. La richiesta del client - DHCPDISCOVER - viene fatta all'indirizzo broadcast 255.255.255.255, poiché l'indirizzo IP del server è sconosciuto, avrà indirizzo mittente 0.0.0.0 e conterrà l'indirizzo MAC della scheda di rete e il nome del computer.
- Offerta IP. Il server DHCP manda un messaggio - DHCPOFFER - broadcast contenente l'indirizzo IP. Il client utilizzerà il primo IP che riceve (nel caso che ci siano più server DHCP i successivi IP saranno ignorati).
- Selezione IP. Dopo aver accettato un IP il client manda un messaggio - DHCPREQUEST - broadcast informando tutti i server DHCP che ha accettato un IP (tale messaggio include l'indirizzo del server che ha assegnato l'IP) ed essi ritirano le loro offerte. A questo punto il server DHCP manda al client un messaggio di conferma - DHCPACK - contenente il valore di lease per l'IP assegnato. Quando il client riceve il messaggio di ACK completa la propria configurazione IP.

Il rinnovo dell'IP, allo scadere del lease, avviene in tre tentativi al termine dei quali l'IP assegnato precedentemente viene rilasciato e il client tenta di ottenere un nuovo IP mandando un messaggio broadcast di richiesta.

- Primo tentativo. Il client tenta il rinnovo del lease quando questi risulta ridotto del 50% mandando un messaggio DHCPREQUEST broadcast al server. Se il server è disponibile al rinnovo manda un messaggio di conferma con i nuovi parametri, altrimenti il client continua ad utilizzare il suo IP per il tempo rimasto.
- Secondo tentativo. Se il primo tentativo fallisce, il client tenta di rinnovare la richiesta dopo un riavvio, fatto subito dopo il 50% del valore del lease. Se il tentativo fallisce il client continua ad utilizzare il suo indirizzo per il tempo rimasto.
- Terzo tentativo. Il client, allo scadere del tempo di lease rimasto, tenta di rinnovare l'indirizzo IP contattando qualsiasi server DHCP disponibile.
- Scadenza IP. Allo scadere dell'IP il client rilascia l'indirizzo ed esegue nuovamente una richiesta broadcast per un indirizzo IP e, fino a quando la configurazione non sarà completata nuovamente, non sarà possibile utilizzare quell'interfaccia di rete.

NAT - Traduzione degli indirizzi IP privati⁴⁰ Il gateway (Proxy o Router) effettua la traduzione degli indirizzi IP (di tipo IPV4) privati di ciascun client per permettere loro di accedere ad Internet come se ciascuno di essi disponesse di un proprio indirizzo IP pubblico.

La tecnica usata per sostituire nell'intestazione di un pacchetto IP un indirizzo, sorgente o destinazione, con un altro indirizzo è la **NAT** (*Network Address Translation*). Tale tecnica, definita nella RFC 3022 NAT, viene usata per permettere ad una rete che usa una classe di indirizzi privata di accedere ad Internet usando uno o più indirizzi pubblici.

Con gli indirizzi di tipo IPV6 questo problema non sussisterebbe, in quanto ciascun PC potrà essere effettivamente dotato di un proprio indirizzo IP pubblico.

⁴⁰ **Traduzione degli indirizzi IP privati - NAT** (*Network Address Translation*): il gateway (Proxy o Router) effettua la traduzione degli indirizzi IP (di tipo IPV4) privati di ciascun client per permettere loro di accedere ad Internet come se ciascuno di essi disponesse di un proprio indirizzo IP pubblico (con gli indirizzi di tipo IPV6 questo problema non sussisterebbe, in quanto ciascun PC potrà essere effettivamente dotato di un proprio indirizzo IP pubblico). Vediamo più dettagliatamente questo processo di traduzione degli indirizzi IPV4 che effettua il gateway, sia esso Router NAT o proxy, per permettere a tutti i computer della LAN - al quale l'ISP ha assegnato un unico indirizzo IP pubblico - di accedere a Internet, come se ciascuno di essi possedesse un proprio IP pubblico.

- Quando il gateway riceve da uno dei Client della LAN un pacchetto IP destinato ad una macchina esterna:
 - a) memorizza [IP:porta] sorgente e destinazione in una tabella (chiamiamo Entry1 la prima coppia ed Entry2 la seconda);
 - b) cambia l'IP e la porta del sorgente con un IP pubblico ed una porta disponibile, presa da un opportuno pool (in genere da 50000 in su);
 - c) instrada il pacchetto all'esterno della LAN (verso Internet).
- Quando il gateway riceve un pacchetto proveniente dall'esterno della LAN (da Internet):
 - d) cerca nella tabella sopra citata nel campo Entry2 se esiste una voce corrispondente all'[IP:porta] SORGENTE del pacchetto ricevuto (in tal caso la sorgente è ovviamente l'host remoto).
 - e) Se esiste, il router sostituisce l'indirizzo di destinazione del pacchetto con il campo Entry1. Altrimenti il pacchetto viene trattato in maniera diversa (gettato, respinto o altro)

Esempio: il client 1 (192.168.1.10) invia un pacchetto al server web www.tin.it (alla porta 80) e riceve una risposta.

In uscita:	Sorg	192.168.1.10 : 2250		151.12.10.187 : 61251
	Dest	62.211.64.8 : 80	→	62.211.64.8 : 80 ↓
In ingresso:	Sorg	62.211.64.8 : 80		62.211.64.8 : 80
	Dest	192.168.1.10 : 2250	←	151.12.10.187 : 61251

Una comunicazione TCP o UDP è univocamente individuata dalla coppia [IP:porta] di sorgente e destinazione. Per un numero limitato di macchine - fino a un centinaio - un singolo IP è sufficiente (infatti il numero di porte a disposizione del router è enorme rispetto al numero di pacchetti che esso potrebbe processare; volendo usare le sole porte da 50000 in su, sono più di 15000 porte utilizzabili per instaurare altrettante comunicazioni).

INTERNET

Storia

La "rete di reti" Internet ha una breve storia⁴¹ i cui fatti salienti sono:

- 1969, progettazione della rete militare statunitense Arpanet;
- 1972, posta elettronica (mail), collegamento remoto, trasferimento file (FTP);
- 1974, protocolli IP e TCP;



⁴¹ **storia** di Internet

- La nascita di INTERNET risale al 1969, quando il governo degli Stati Uniti fece progettare una rete militare finalizzata allo scambio di informazioni veloce e sicuro, che fosse in grado di connettere sistemi diversi e distanti fra loro e che fosse capace di funzionare anche con più nodi guasti o distrutti. Questa rete, sviluppata da un'agenzia del Dipartimento della Difesa denominata ARPA (*Advanced Research project Agency*) fu chiamata **ARPANET**. Essa era in grado di funzionare anche dopo un disastro nucleare, essendo costituita da moduli che mettevano un computer in grado di comunicare con un altro seguendo strade diverse: quando una strada risulta ostacolata i messaggi seguono strade alternative (instradamento delle informazioni, *routing*). L'aspetto più importante era il modo con il quale un computer comunicava con un altro. Di questo si occupa il protocollo IP (Internet Protocol), un protocollo che garantisce la comunicazione anche tra computer diversi e con sistemi operativi diversi. Questa rimane una delle caratteristiche fondamentali di INTERNET.
- Nel 1972 già veniva utilizzata la posta elettronica (e-mail) il collegamento remoto (*Remote Login*) e il trasferimento di file FTP (*File Transfer Protocol*), servizi oggi disponibili in INTERNET.
- Nel 1974 vennero ufficialmente presentati i protocolli **IP** (*Internet Protocol*) e **TCP** (*Transmission Control Protocol*).
- Nel 1979 nacque la **CSNet** (*Computer Science Research Network*), una rete progettata dai ricercatori di informatica e destinata a connettere le varie università americane.
- Nel 1980 nacque INTERNET come interconnessione tra ARPANET e CSNet tramite un gateway basato sui protocolli TCP/IP.
- Una evoluzione nella crescita di Internet si ebbe con **NSFNet** (*National Science Foundation Network*) che collegava diversi supercomputer ciascuno dei quali fungeva da server per altrettante reti locali e connessi tra di loro tramite linee telefoniche. Ciascun supercomputer era poi connesso, sempre mediante linee telefoniche, ad altri computer e centri di calcolo regionali. In tal modo ciascun computer poteva comunicare con un qualsiasi altro computer della rete. Nel 1990 NSFNet soppiantò definitivamente ARPANET e questo aprì la strada all'utilizzazione commerciale e civile della rete. Cominciarono a svilupparsi le backbone (spina dorsale), le dorsali, cioè le reti principali ad alta velocità - collegate tra di loro non da linee telefoniche, ma da linee ad alta velocità - ciascuna delle quali poi collegava, mediante linee telefoniche, le reti locali. Le velocità dei collegamenti di Internet sono così molto diverse: si va dalle poche decine di Kbps (migliaia di bit per secondo) dei modem domestici ai 45 Mbps (milioni di bit per secondo) di NSFNet.
- Nel 1990 al CERN (Centro Europeo per la Ricerca Nucleare di Ginevra) i ricercatori informatici incaricati di realizzare un sistema per la condivisione tra utenti diversi di dati sia testuali che non testuali (immagini, suoni, filmati), basandosi sul concetto di ipertesto, hanno dato origine al linguaggio **HTML** (*Hyper Text Markup Language*) che consente, oltre che a gestire informazioni di diversa natura (testuali e multimediali), anche di collegare diversi documenti tra di loro mediante opportuni link. Questo linguaggio è divenuto lo strumento più potente per distribuire informazioni in Internet ed ha introdotto quella architettura denominata WWW (*World Wide Web*), la "ragnatela di dimensioni mondiali" che consente la navigazione, cioè la consultazione semplice e veloce degli archivi e dei documenti presenti nei computer della rete.
- Nel 1993 il NCSA (Centro nazionale statunitense per il supercalcolo) realizzò **Mosaic**, il primo browser per WWW ed il primo sito a cui connettersi (un "sito" è un computer che mette a disposizione degli utenti della rete informazioni organizzate e al quale ci si può connettere per la consultazione). Attualmente i browser più diffusi sono Netscape ed Explorer di Microsoft e la comunicazione tende sempre più a passare dalla semplice consultazione ad un tipo di comunicazione interattiva, e questo grazie all'utilizzazione di linguaggi quali **Java** e **ActiveX**.
- Nel 1994 David Filo e Jerry Yang diedero vita a **Yahoo!**, il primo Motore di ricerca. Nello stesso anno arrivò il primo motore di ricerca full text di Internet, **Webcrawler**, quindi arrivarono **Lycos** e poi **InfoSeek**. Alla fine del 1995 arrivò **Altavista**, nel 1996 HotBot e nel 1998 **Google**.

- d) 1979, nascita di CSNet, rete che collega le università statunitensi;
- e) 1980, collegamento di Arpanet e CSNet, vera "nascita" di Internet;
- f) 1990, la rete NSFNet che collega supercomputer soppianta Arpanet;
- g) 1990, realizzazione, al CERN di Ginevra, del linguaggio HTML;
- h) 1993, realizzazione di Mosaic, il primo browser della rete.
- i) 1994, realizzazione di Yahoo!, il primo motore di ricerca.

Connessione e Indirizzi

La interconnessione tra due o più reti distinte avviene attraverso il **gateway** (cancello di passaggio), un dispositivo in grado di convertire i protocolli utilizzati da una rete in quelli utilizzati dall'altra rete, e viceversa. Questo permette che computer di reti diverse possano comunicare tra di loro senza che gli utenti siano tenuti a conoscere le caratteristiche fisiche delle reti.

Per i collegamenti e la trasmissione dei *messaggi* Internet utilizza la **commutazione di pacchetto**. Ogni pacchetto ha gli indirizzi (sia l'indirizzo Internet che l'indirizzo IP) del destinatario e del mittente. Ad ogni indirizzo Internet (del tipo www.repubblica.it) corrisponde un indirizzo IP (del tipo 195.130.55.10, dove ciascuno dei quattro numeri può assumere un valore da 0 a 255). Ogni host - computer o gateway - che riceve il pacchetto deve decidere cosa farne, su quale canale inviarlo; per fare ciò Internet utilizza la tecnica dell'**instradamento dinamico distribuito**: l'host decide dove instradare il pacchetto in base ad informazioni locali e a informazioni provenienti dai nodi adiacenti.

Gli indirizzi Internet sono del tipo **<host>.<dominio>**, sono cioè costituiti da un "dominio" e da un "nome dell'host" all'interno del dominio: il dominio identifica una rete (locale o estesa per un raggio di qualche decina di chilometri), mentre l'host identifica un particolare computer all'interno della rete stessa.

La traduzione da indirizzi Internet ad indirizzi IP è fatta da un servizio denominato **DNS** (*Domain Name System*) che garantisce l'univocità degli indirizzi.

Il DNS, presente sia su computer locali che sui server dei provider che su altre macchine Internet, agisce in modo gerarchico: la richiesta che non può essere soddisfatta dal DNS locale (perché non riguarda la rete locale) viene inoltrata al livello superiore di DNS.

Ad esempio **pippo.progetti.fiat.it** non sarà risolto dal DNS del nostro PC e verrà quindi inoltrato a livello superiore, al sistema di provider cui è connesso il nostro provider. Questi, se non è in grado di individuare il dominio **it**, passa a sua volta l'indirizzo al DNS superiore finché non si individua un livello DNS che sappia dove si trova il dominio **it**. A questo punto l'indirizzo viene rispedito verso il basso ai sottosistemi DNS del dominio **it** fino a scoprire che **pippo** è un computer di **progetti** appartenente alla società **fiat** che fa parte di una delle reti italiane. L'ultima parte del nome di dominio identifica o la nazione di appartenenza o il tipo di organizzazione.

Accesso

La connessione può avvenire tramite:

- normale linea telefonica analogica **PSTN** (*Public Switched Telephone Network*), con modem a 56 Kbps⁴²;

⁴² **PSTN**: la connessione tramite **modem** e **linea telefonica** è la più diffusa ed economica, ma la più lenta, con velocità di trasmissione dell'ordine delle poche decine di Kbps. Questo accesso, denominato **Dial-up connection** (*connessione tramite composizione telefonica*) prevede che venga chiamato un **ISP** (*Internet Service Provider*), una delle aziende che forniscono l'accesso a Internet, il cui computer esegue i comandi per il collegamento dell'utente a Internet e fornisce la risposta al collegamento. Il server del provider fornirà, al momento del collegamento, un indirizzo IP dinamico, tra tutti quelli a sua disposizione, che sarà l'indirizzo IP dell'utente per tutta la durata del collegamento. Generalmente l'accesso a Internet è fatto da funzioni implementate mediante il sistema operativo UNIX, ma, poiché è il computer del provider che "gira" ad Internet i comandi dell'utente non è necessario che l'utente disponga di tale sistema operativo. Una volta stabilito il

- rete pubblica **ISDN**⁴³ (*Integrated Service Digital Network*, rete numerica a integrazione di servizi) che permette accessi più veloci, di 128 Kbps;
- linea telefonica analogica con tecnologia **ADSL**⁴⁴ (*Asymmetric Digital Subscriber Line*), molto veloce, fino a 640 Kbps ed oltre;
- cavi a **fibre ottiche**, il più veloce in assoluto, fino a 10 Mbps, ma necessità di apposito cablaggio sul territorio;
- in mancanza di linea ADSL, per avere un canale a banda larga (la cosiddetta *Internet veloce*), si può utilizzare:
 - **satellite**, con l'installazione di una parabola satellitare, dell'apposita scheda di ricezione e di un convertitore, con velocità di ricezione dai 300 Kbps ai 2 Mbps;
 - "**chiavetta USB**", che sfrutta la rete della telefonia cellulare **UMTS** (*Universal Mobile Telecommunication System*);
 - collegamento **Wi-Fi** ad un ripetitore "visibile";
 - la tecnologia **WiMAX**⁴⁵

collegamento, un secondo modulo del Dial-up, il **Dial-up IP Link** (connessione fisica a seguito dell'attivazione del collegamento) connette il computer dell'utente direttamente ad Internet tramite i protocolli **SLIP** (*Serial Line Internet protocol*) per la comunicazione su linee seriali come quella utilizzata dal modem o **PPP** (*Point to Point Protocol*) per la comunicazione diretta tra due punti della rete. La connessione si può così schematizzare:



⁴³ **ISDN**: la rete ISDN (*Integrated Services Digital Network*, rete integrata di servizi digitali) permette la trasmissione di voce, fax e dati in forma digitale e non modulata. Ci sono 2 canali dati ed un canale di controllo. La velocità di trasmissione è di 64 Kbps per canale se si usano canali separati, lasciando libera la linea telefonica, o di 128 Kbps se si usano i due canali congiuntamente. Ad ogni canale possono essere associati 8 numeri telefonici. Per l'interfacciamento del computer con la linea ISDN occorre utilizzare un apposito modem ISDN, interno o estremo, o un router ISDN.

⁴⁴ **ADSL**: la tecnologia DSL (*Digital Subscriber Line*) utilizza le esistenti linee telefonica analogiche su doppiini in rame per il trasporto di dati a banda larga come i servizi video e multimediali, fornendo servizi su connessioni punto-punto. Le varie tecnologie xDSL sono: HDSL (*High bit rate DSL*), SDSL (*Single line*), RADSL (*Rate adaptive Asymmetric*), VDSL (*Very high bit rate*) e ADSL (*Asymmetric Digital Subscriber Line*). Il modem ADSL combinato con uno "splitter" sovrappone i segnali a banda larga sulle linee analogiche (PSTN) o digitali (ISDN) esistenti senza interferire con il normale traffico telefonico e la connessione è sempre attiva. È una trasmissione asimmetrica perché c'è più banda disponibile verso l'utente (downstream) e meno nella direzione opposta (upstream). La grande velocità di trasmissione (in teoria fino a 1,5 Mbps in trasmissione e fino a 16 Mbps in ricezione, ma molto dipende dallo stato delle linee, soprattutto quelle del cosiddetto "ultimo miglio") è stata ottenuta migliorando le tecnologie di filtraggio e conversione dei tradizionali modem. Le normali connessioni telefoniche sfruttano una piccola parte dello spettro di frequenza del doppiino ed il segnale telefonico viaggia ad una frequenza di 4 KHz, mentre è possibile arrivare fino ad un massimo di 1,1 Mhz. ADSL scompone tutto lo spettro di frequenza del doppiino in 256 sottofrequenze tutte indipendenti tra loro consentendo il trasporto simultaneo di una grande quantità di dati vocali e digitali. Oltre ai modem ADSL (con velocità di 128 Kbps in upload e di 640 Kbps in download, velocità 10 volte maggiori di quelle di una tradizionale linea ISDN) nel doppiino telefonico ci sono tre canali: un canale per il telefono, un canale ad alta velocità downstream e un canale duplex a media velocità.

⁴⁵ **WiMAX**: la tecnologia WiMAX (*Worldwide Interoperability for Microwave Access*) è basata sullo standard IEEE 802.16 che fornisce l'accesso alle reti di telecomunicazione a banda larga e senza cavi. La sua caratteristica principale è la capacità di copertura. Una Base Station può connettersi a Internet mediante connessioni a banda larga via cavo o ricevere connettività dal backbone (la "spina dorsale" in grado di servire una vasta area) mediante un ponte radio. WiMAX collega più Base Station mediante ponti radio e ciascuna Base Station offre via etere connettività agli utenti dell'area dotati di appositi apparati CPE (*Customer Premises Equipment*). I CPE possono essere configurati *indoor*, "da interni" (dal costo contenuto, destinati all'utenza *consumer*, operano in assenza di visibilità diretta con la Base Station) o *outdoor* "da esterni" (con prestazioni superiori, più costosi, destinati all'utenza *business*, operano in situazione di visibilità diretta con la Base Station). La velocità è di 7 Mbps in downstream (download) e di 512 Kbps in upstream (upload).

Livelli e Protocolli

Internet non si basa sul modello ISO/OSI a 7 livelli, ma sul più semplice modello TCP/IP a 4 livelli.

1-Fisico

2-Rete (IP)

3-Trasporto (TCP)

4-Applicazioni

1-Fisico: trasmissione dei bit nel canale di comunicazione; organizzazione dei messaggi in pacchetti, elaborazione delle risposte del ricevente; sincronizzazione delle diverse velocità di trasmissione / ricezione.

2-Rete/IP: il protocollo **IP** (*Internet protocol*) si occupa dell'instradamento dei singoli pacchetti in modo dinamico distribuito.

3-Trasporto/TCP: il protocollo **TCP** (*Transmission Control Protocol*) rende possibile la comunicazione tra due computer distinti collegati a reti diverse ma interconnesse, assembla i pacchetti ricevuti dal destinatario, è "orientato alla connessione" perché stabilisce una interconnessione logica tra i computer come se vi fosse un canale fisico dedicato.

4-Applicazioni: stabilisce la sessione tra i due computer coinvolti, sfrutta la bidirezionalità del canale full-duplex, si occupa della sincronizzazione dei processi, si occupa del login delle password, dei permessi di accesso, definisce le modalità di interpretazione dei dati, la sintassi e la semantica dei dati tramite il linguaggio **HTML** (*Hyper Text Markup Language*), gestisce i vari tipi di terminale, definisce il tipo di interazione con l'utente, usa i principali protocolli quali **HTTP** (*Hyper Text Transport Protocol*) e **FTP** (*File Transfer protocol*), **SMTP** (*Simple Mail Transfer Protocol*), etc.

SERVIZI

In ambiente Internet si ha essenzialmente una architettura di tipo **Client/Server**, con alcuni sistemi (**server**) dedicati alla raccolta e alla distribuzione delle informazioni a chi ne fa richiesta (**client**): un processo server resta in attesa che un processo client richieda i suoi servizi. I servizi offerti in Internet sono processi **server** residenti su alcuni potenti sistemi collegati alla rete che attendono le richieste dei processi **client** degli utenti delle varie parti del mondo.

E-Mail (posta elettronica)

La posta elettronica (*e-mail, electronic mail*) è uno dei servizi più utilizzati, forse quello che più ha contribuito alla grande diffusione di Internet.

Questo servizio consente di scambiarsi messaggi elettronici testuali e multimediali: il mittente lascia il messaggio su un server connesso alla rete all'interno della casella postale elettronica (*mailbox*) del destinatario; ogni utente, alla connessione, può controllare la propria casella postale e scaricare nel proprio sistema la posta eventualmente presente.

Insieme al messaggio è inoltre possibile inviare in allegato - **attachment** - dei file di diversa natura. I messaggi di posta sono formati da un *header* (testa) e da un *body* (corpo). L'*header* contiene le informazioni necessarie alla consegna del messaggio (*To*: indirizzo del destinatario, *From*: indirizzo del mittente, *Subject*: oggetto del messaggio, *CC*: eventuali indirizzi ai quali inviare il messaggio per conoscenza) mentre il *body* contiene il messaggio vero e proprio.

Gli indirizzi di posta elettronica sono del tipo **utente @ dominio** (dove @ - *at* - sta a significare "presso"). Ad esempio l'indirizzo veralucia@krenet.it è dell'utente "veralucia" presso il provider "krenet" che è un provider italiano "it".

I protocolli utilizzati per la posta elettronica sono: **SMTP** (*Simple Mail Transfer Protocol*, protocollo per il semplice trasferimento di posta) per la posta in uscita, supporta solo messaggi di tipo testuale; per gestire anche messaggi di tipo multimediale è stato sviluppato il protocollo **MIME** (*Multipurpose Internet Mail Extension*); **POP** (*Post Office Protocol*) per la posta in ingresso e, sempre per la posta in ingresso, il più recente e flessibile **IMAP** (*Internet Message Access Protocol*).

FTP (trasferimento file)

Il protocollo **FTP** (*File Transfer Protocol*) permette il trasferimento di file da un computer all'altro della rete. L'operazione di trasferimento dei file da una delle numerose librerie pubbliche presenti su Internet al proprio computer prende il nome di **download**, mentre l'invio di file dal proprio computer ad un altro della rete prende il nome di **upload**.

Alcuni host mettono a disposizione dei programmi **shareware** (a bassissimo costo, per essere condivisi) o **freeware** (gratuiti, distribuiti liberamente).

World Wide Web

Il **WWW** (*World Wide Web*, la "ragnatela di dimensioni mondiali") o **WEB** ("rete"), è il servizio che permette la ricerca e la consultazione di informazioni per mezzo di ipertesti (**navigazione**), di collegarsi a siti FTP, gruppi di NEWS, di usare TELNET.

Il WWW è un sistema in grado di combinare il linguaggio ipertestuale **HTML** (*Hyper Text Markup Language*) con la sintassi specifica definita tramite **URL** (*Universal Resource Locator*, allocatore universale di risorse) che, distribuito nei vari nodi della rete, consente di indirizzare qualsiasi risorsa connessa alla rete in qualsiasi punto del pianeta.

Un URL ha il seguente formato: **Risorsa : // Host . Dominio / Percorso / File**

Risorsa	può essere <u>http</u> (documento di WWW richiamato da un server http), <u>ftp</u> (documento richiamato da un servizio ftp), <u>file</u> (file ipertestuale presente nel proprio disco e richiamabile tramite browser), <u>news</u> , <u>telnet</u> , altro
Host.Dominio	è l'indirizzo Internet ove la risorsa è localizzata, formato dal nome del computer server presente nel sistema dei nomi di dominio DNS
Percorso	è il pathname del file da individuare, percorso che deve essere specificato utilizzando la sintassi UNIX ("/" al posto di "\"")

Il linguaggio HTML consente di strutturare un ipertesto (anche con un semplice editore di testi utilizzando direttamente le **tag** di formattazione del linguaggio) che può successivamente essere inserito in Internet e reso accessibile agli altri utenti per mezzo di uno dei browser per WWW. Gli indirizzi URL possono essere inseriti nell'ipertesto HTML per specificare **link** ad altri documenti ipertestuali e quindi avere un ipertesto che fisicamente risiede su computer diversi e geograficamente lontani. L'attività di consultazione di questo tipo di documenti è la cosiddetta **navigazione** nel WWW. Il protocollo di riferimento dei server web e dei browser dei client è **HTTP** (*Hyper Text Transfer Protocol*).

Telnet (accesso remoto)

Il servizio **TelNet** (*rlogin, remote login*) permette di accedere⁴⁶ ad un computer remoto come utente di quel sistema, utilizzando il proprio computer come se fosse un terminale del sistema al quale si accede. Per il collegamento è necessario avere un **account** (*permesso di accesso*) sul sistema remoto al quale poter accedere tramite una **login** e una **password** opportune.

Mailing List

La **Mailing List** (*indirizzi di posta*) è un servizio sviluppato per l'e-mail. Sono gruppi di utenti interessati ad un particolare argomento o progetto ai quali l'utente può iscriversi e ricevere nella propria casella postale tutti i messaggi inviati agli utenti della Mailing List.

News

USENET (*USEr NETwork*) identifica un servizio di posta elettronica offerto ad un certo numero di utenti che si scambiano messaggi di posta con un particolare *header* contenente un tema di discussione (*subject*) specifico: questo consente la discussione su Internet di particolari tematiche. Sono stati organizzati vari gruppi di discussione denominati **NewsGroup** (gruppi che si scambiano *news*, cioè notizie) su argomenti diversi (politica, sport, computer, religione, lavoro, tempo libero, etc.). Il protocollo di riferimento è il **NNTP** (*Network News Transfer Protocol*).

Search Engine (motori di ricerca)

In Internet sono presenti decine di milioni di documenti, per cui una delle principali necessità di un utente della rete è la ricerca. Per questo alcuni siti, denominati **motori di ricerca** (*search engine*) mettono a disposizione degli appositi programmi di ricerca che consentono di cercare i documenti che rispondono a certi requisiti di un certo argomento, che contengono una o più parole chiave date, anche combinate tra di loro mediante gli operatori logici AND e OR.

Alcuni famosi motori di ricerca sono **Yahoo**, **Google**, **Alta Vista**, **Virgilio**, **HotBot**, **Web Crawler**, **Infoseek**, e altri ancora.

Chat

I servizi di chat permettono a più utenti di dialogare in diretta inviandosi messaggi e risposte on line. I server più conosciuti sono gli **IRC** (*Internet Relay Chat*). Il metodo di comunicazione è prettamente testuale, ma le più recenti implementazioni hanno portato a integrare nel server di chat avanzate funzionalità multimediali che consentono di interagire anche in videoconferenza.

⁴⁶ **Telnet:** si può accedere direttamente ad un servizio internet utilizzando Telnet. Esempio 1: si digita, dal prompt Dos, il comando "Telnet www.virgilio.it: 80" per aprire la connessione con la porta 80 associata ad HTTP per la richiesta di pagine web; si digita il comando "Get /" e si avrà in risposta la spedizione del codice HTML che descrive la pagina e poi il messaggio del troncamento della comunicazione. Esempio 2: si digita il comando "Telnet www.virgilio.it: 110" per aprire la connessione con la porta 110 associata a POP, posta elettronica; poi si digitano i comandi "user nome" e "password password" (*nome e password* sono i nostri dati) e il server di posta fornirà numero e grandezza di ogni messaggio di posta presente nella casella postale; per leggere uno dei messaggi si può digitare il comando "retr n" (*n* è il numero del messaggio che si vuole leggere)

Videoconferenza

Disponendo dell'opportuna strumentazione (sostanzialmente una piccola telecamera da piazzare sopra il video del computer, microfono e casse) e dell'opportuno software è possibile collegarsi in **videoconferenza** con altri utenti dotati di analoga strumentazione e instaurare una videoconferenza: ognuno ha sul proprio video tutti gli altri partecipanti, ciascuno su una diversa finestra, e quello che è detto e ripreso dalle telecamere è sentito e visto da tutti.

E-qualcosa

Internet può servire, con gli strumenti ed i servizi che mette a disposizione, per molte attività:

- **e-commerce** ed **e-business** (commercio elettronico, vendita ed acquisto di prodotti)
- **e-training** (corsi di addestramento on line)
- **e-gouvernement** (accesso ai servizi della pubblica amministrazione)
- **e-banking** (accesso ai servizi bancari)

INTRANET ed EXTRANET



Intranet

Le moderne tecnologie hanno creato una forte interazione tra le LAN e Internet attraverso le cosiddette reti **Intranet**, cioè LAN che usano gli stessi protocolli e strumenti di Internet rendendo così omogeneo l'accesso alle varie informazioni e alle varie risorse, indipendentemente dal fatto che esse siano locali (stesso computer), della rete aziendale (nella LAN) o globali (in Internet).

Esistono dei web server privati (dell'azienda) che mettono a disposizione dei dipendenti, prelevandole dai propri database e dai propri applicativi aziendali (contabilità, magazzino, etc.), le informazioni in formato web. Da parte loro i dipendenti accedono a tali informazioni utilizzando semplicemente il browser del proprio PC e comunicano tra di loro utilizzando la posta elettronica.

Extranet

Parte della LAN o della Intranet aziendale può essere resa disponibile ad altre aziende dello stesso gruppo, ai clienti, ai fornitori e ai venditori dell'azienda, ad esempio per scambiare documenti, distribuire cataloghi, sviluppare progetti, addestrare il personale (*e-training*), accedere alle applicazioni aziendali). In questo caso, quando parte della rete aziendale è messo a disposizione di utenti esterni selezionati, si parla di **Extranet**, così come quando si utilizza Internet per collegare le LAN o le Intranet di sedi aziendali distanti.

In sostanza Extranet è una rete privata, geograficamente estesa, accessibile da parte di gruppi di utenti selezionati, che utilizza linee di comunicazione e protocolli pubblici (Internet).

I "linguaggi" di Internet

Molteplici sono i LINGUAGGI (di programmazione e non solo) utilizzati in Internet.

HTML (*Hyper Text Markup Language*), sviluppato nel 1990 al CERN di Ginevra da un gruppo di ricercatori (tra i quali Tim Bernes-Lee). Non si tratta di un vero e proprio linguaggio di programmazione, quanto di un "sistema di contrassegno" - linguaggio di *markup* - i cui comandi sono solo dei TAG di formattazione del documento (che consentono anche di inserire informazioni multimediali quali immagini, filmati, suoni, musica, etc.) interpretati ed eseguiti dai vari browser (Explorer, FireFox, Netscape, Opera, Chrome, etc.).

I **CSS** (*Cascading Style Sheets*), i "fogli di stile" delle pagine HTML, permettono di separare il contenuto della pagina HTML dalla sua presentazione.

JavaScript è un linguaggio di scripting basato su oggetti implementato nel 1995 per il browser Navigator 2.0 di Netscape. Oggi tutti i principali browser hanno al loro interno un interprete JavaScript. Con tale linguaggio si possono introdurre nelle pagine HTML elementi di dinamicità e di interattività. I costrutti del JavaScript sono ereditati dal linguaggio C.

Java è un linguaggio di programmazione orientato agli oggetti (OOP), i cui costrutti sono ereditati dal linguaggio C++, implementato nel 1995 da *Sun Microsystems* (acquistata nel 2010 da *Oracle*) che permette di realizzare applicazioni Internet. Java è indipendente dalla piattaforma (Windows, Linux, Apple, ...) e funziona sulla JVM (*Java Virtual Machine*) che deve essere installata sul computer ed è supportata da tutti gli odierni browser.

PHP (*Personal Home Page* o *Hypertext Preprocessor*) è un linguaggio di scripting interpretato, lato server, concepito per la programmazione di pagine web dinamiche interattive e per l'accesso ai database. L'elaborazione di codice PHP sul server produce codice HTML che viene inviato al browser dell'utente che ne fa richiesta.

PHP è supportato da web server Windows (WindowsServer, IIS) e Linux (Apache).

VBScript (*Microsoft's Visual Basic Scripting Edition*) è un sottoinsieme del linguaggio Visual Basic usato in ASP (*Active Server Pages*) come linguaggio di scripting *general-purpose* che può trovarsi sia all'interno che all'esterno di un web server. La versione di VBScript presente nel browser Internet Explorer offre le stesse funzionalità di JavaScript ma, data la sua incompatibilità con gli altri browser molti programmatori preferiscono utilizzare JavaScript.

ASP (*Active Server Pages*) e la sua evoluzione **ASP.NET** sono linguaggi di scripting lato server che hanno la stessa sintassi dei linguaggi VBScript e JScript (ASP) e VB.NET, C# e J# (ASP.NET), concepiti, come PHP, per la programmazione di pagine web dinamiche interattive e per l'accesso ai database. ASP e ASP.NET sono supportati solo da web server Windows (Windows Server, IIS).

Tutti i linguaggi di programmazione usati nel web (JavaScript, Java, PHP, VBScript, ASP, ASP.NET) hanno come base le pagine HTML nelle quali sono "ospitati".

ACRONIMI

ADSL	<i>Asymmetric DSL (Digital Subscriber Line)</i>
AP	<i>Access Point</i>
ARP	<i>Address Resolution Protocol</i>
ARPA	<i>Advanced Research Project Agency</i>
BSC	<i>Binary Synchronous Communication</i>
CERN	<i>Centro Europeo per la Ricerca Nucleare</i>
CPE	<i>Customer Premises Equipment</i>
CSMA/CD	<i>Carrier Sense Multiple Access / Collision Detection</i>
CSNET	<i>Computer Science Research Network</i>
DHCP	<i>Dinamic Host Configuration Protocol</i>
DNS	<i>Domaine Name System</i>
DSL	<i>Digital Subscriber Line</i>
EISA	<i>Extended ISA (Industry Standard Architecture)</i>
FCS	<i>Frame Check Sequence</i>
FDDI	<i>Fiber Distributed Data Interface</i>
FTP	<i>File Transfer Protocol</i>
GARR	<i>Gruppo di Autoregolamentazione delle Reti per la Ricerca</i>
GSM	<i>Global System for Mobile communication</i>
HDLC	<i>High level Data Link Control Procedure</i>
HDSL	<i>High bit rate DSL (Digital Subscriber Line)</i>
HTML	<i>Hyper Text Markup Language</i>
HTTP	<i>Hiper Text Transfer Protocol</i>
HUB	termine inglese corrispondente alla parola "perno"
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
IMAP	<i>Internet Message Access Protocol</i>
IP	<i>Internet Protocol</i>
IPV4 / 6	<i>Internet protocol Version 4 / 6</i>
IPX/SPX	<i>Internet Packed Exchange / Sequenced Racket Exchanged</i>
IRC	<i>Internet Relay Chat</i>
ISA	<i>Industry Standard Architecture</i>
ISDN	<i>Integrated Service Digital Netrwork</i>
ISO	<i>International Standard Organization</i>
ISP	<i>Internet Service Provider</i>
LAN	<i>Local Area Network</i>
MAC	<i>Media Access Control</i>
MAN	<i>Metropolitan Area Network</i>
MIME	<i>Multipurpose Internet Mail Extension</i>
NAT	<i>Network Address Translation</i>
NCSA	<i>National Center for Supercomputing Applications</i>
NETBEUI	<i>NET Bios Enanchend User Interface</i>
NETBIOS	<i>NETworc Basic Input Output System</i>
NIC	<i>Network Interface Card</i>
NNTP	<i>Network News Transfer Protocol</i>
NSFNET	<i>National Science Foundation Network</i>
OSI	<i>Open System Interconnection</i>
PCI	<i>Peripheral Component Interconnect</i>
POP	<i>Post Office Protocol</i>

PPP	<i>Point to Point Protocol</i>
PSTN	<i>Public Switched Telephone Network</i>
RIP	<i>Routing Information Protocol</i>
SLIP	<i>Serial Line Internet Protocol</i>
SMB	<i>Server Message Block</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
SNMP	<i>Simple Network Management Protocol</i>
STP	<i>Shielded Twisted Pair</i>
TCP	<i>Transfer Control Protocol</i>
TFTP	<i>Trivial FTP (File Transfer Protocol)</i>
UDP	<i>User Datagram Protocol</i>
UMTS	<i>Universal Mobile Telecommunications System</i>
URL	<i>Universal Resource Locator</i>
USENET	<i>USEr NETwork</i>
UTP	<i>Unshielded Twisted Pair</i>
VDSL	<i>Very high bit rate DSL (Digital Subscriber Line)</i>
WAN	<i>Wide Area Network</i>
WI-FI	<i>Wireless Fidelity</i>
WiMAX	<i>Worldwide Interoperability for Microwave Access</i>
WT	<i>Wireless Terminal</i>
WWW	<i>World Wide Web</i>