GUIDA ALLE RETI DI PC
Prof. Ettore Panella
www.ettorepanella.com

Reti locali

Le reti locali, note col termine **LAN** (Local Area Network), sono reti private ad alta velocità di piccole estensioni utilizzate per la trasmissione dei dati tra due o più apparati che, generalmente, sono computer localizzati in un'area limitata.
La tecnologia più affermata è la Ethernet nella quale la massima velocità di trasmissione dei dati è di 10Mbps, 100Mbps nella Fast Ethernet e di 1Gbps nella Gigabit Ethernet.
Il tasso di errore di trasmissione è assai basso: 10^{-8} - 10^{-9}, ovvero un errore medio di un bit ogni 100 milioni – 1 miliardo di bit trasmessi correttamente.
Si rammenta che l'architettura di una rete locale è costituita da un insieme di **nodi** collegati tra di loro attraverso i **rami**.
Il nodo può essere un punto terminale di un ramo, cioè un punto della rete dove risiedono le risorse che si intendono condividere, o un punto di congiunzione in cui confluiscono due o più rami, cioè un apparato di rete come, ad esempio, Hub o Switch.
Una rete WAN che utilizza le onde radio per la connessione è detta WLAN (Wireless LAN)

Reti WAN

Le reti Wide Area Networks (WAN) sono reti che connettono LAN che si trovano in località geograficamente separate. L'esempio più comune di una WAN è Internet. Internet è una grande WAN composta da milioni di LAN interconnesse. Per interconnettere queste LAN che si trovano in località differenti vengono utilizzati i Telecommunications Service Providers (TSP) Nel caso della rete internet noti anche come ISP.

Dispositivi di Rete

Ci sono molti dispositivi che possono essere usati all'interno di una rete per fornire connettività. Il dispositivo che verrà usato dipenderà da quante periferiche si connetteranno, dal tipo di connessione che utilizzano e dalla velocità alla quale i dispositivi operano. Questi sono i dispositivi di rete più comuni:

- Computer
- Hub
- Switch
- Router
- Access Point Wireless

I dispositivi di rete si scambiano informazioni attraverso **rami** che rappresentano i mezzi trasmissivi, le cui caratteristiche ne determinano anche le modalità d'uso.

HUB

Un hub rappresenta un **concentratore**, un dispositivo di rete che funge da nodo di smistamento di una rete di comunicazione dati organizzata prevalentemente a stella. Nel caso delle reti Ethernet, un hub è un dispositivo che inoltra i dati in arrivo da una qualsiasi delle sue porte su tutte le altre. Per questa ragione può essere definito anche un "ripetitore multiporta". La conseguenza del

comportamento dell'hub è che la banda totale disponibile viene ridotta ad una frazione di quella originaria, a causa del moltiplicarsi dei dati inviati.

SWITCH

Uno switch (commutatore) è un dispositivo di rete che inoltra selettivamente i frame ricevuti verso una porta di uscita. Come con un hub, due nodi possono comunicare attraverso uno switch come se questo non ci fosse, ovvero il suo comportamento è trasparente. A differenza però di quanto farebbe un hub, uno switch normalmente inoltra i frame in arrivo da una qualsiasi delle sue porte soltanto a quella cui è collegato il nodo destinatario del frame. Uno switch possiede quindi l'intelligenza necessaria a riconoscere i confini dei frame nel flusso di bit, immagazzinarli, decidere su quale porta inoltrarli, trasferirli verso una porta in uscita, trasmetterli. Normalmente uno switch opera al livello datalink del modello di riferimento ISO/OSI.

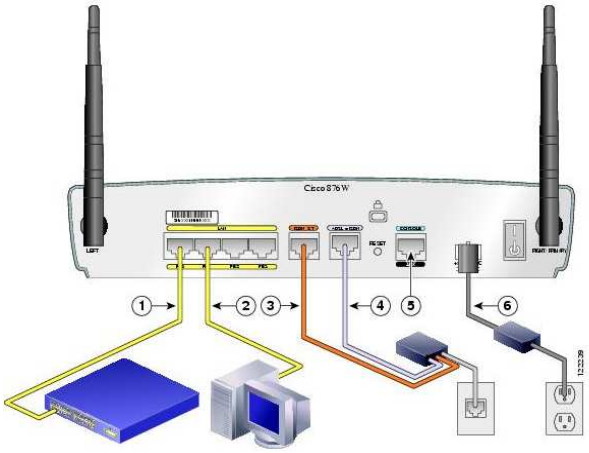
ROUTER

Il Router (instradare) e' un dispositivo elettronico utilizzato per interconnettere reti di computer tra di loro. La funzione primaria di un router e' quella di indirizzare correttamente i **pacchetti di informazioni** di host appartenenti a reti diverse. L'uso fondamentale del router è il collegamento di una rete locale ad internet.

Hub

Switch

Access Point



Router

Fig. 1. Esempi di dispositivi di rete

I mezzi trasmissivi in cavo utilizzati per realizzare una rete sono:

- **Doppino Intrecciato** (Twisted pair).

È un mezzo economico; consente notevoli velocità di trasmissione per distanze fino a circa 100 metri. Ci sono due tipologie di base di cavi twisted pair:

1. **UTP (Unshielded Twisted Pair) –** Consente la cancellazione delle interferenze grazie agli intrecci delle coppie di fili che limita il degrado del segnale causato dall'interferenze elettromagnetiche (EMI) e dalle interferenze radio (RFI). L'UTP è il tipo di cablaggio più comunemente utilizzato nelle reti. I cavi UTP hanno un raggio d'azione di circa 100m
2. **STP (Shielded Twisted Pair) -** Ogni coppia di conduttori è avvolta in una lamina metallica per meglio schermare i fili dal rumore. Le quattro coppie di conduttori sono successivamente avvolte in un unico nastro o lamina metallica. L'STP riduce il rumore elettrico dall'interno del cavo. Riduce anche EMI ed RFI provenienti dall'esterno del cavo.

Esistono diverse categorie di UTP che dipendono da:

a) Il numero di conduttori all'interno del cavo
b) Il numero di avvolgimenti per coppia

Categoria 3 è il cablaggio utilizzato per gli impianti telefonici e per le reti Ethernet a 10 Mbps. La Categoria 3 ha quattro coppie di fili.

Categoria 5 e Categoria 5e hanno quattro coppie di conduttori con una velocità di trasmissione di 100Mbps. Quelli di Categoria 5 e 5e sono i cavi di rete più comunemente utilizzati. Il cavo di Categoria 5e ha più avvolgimenti per unità di lunghezza rispetto a quello di Categoria 5. Un numero di torsioni più elevato minimizza maggiormente le interferenze dovute a fonti esterne e agli altri conduttori interni al cavo.

Categoria 6 utilizzano un divisore di plastica per separare le coppie di fili ed impedire le interferenze. Le coppie hanno più torsioni rispetto ai cavi di Categoria 5e.

I Doppini telefonici

Il doppino è formato da una coppia di fili metallici ricoperti da materiale isolante: è il mezzo più diffuso nelle reti geografiche per il suo utilizzo nella costruzione di delle linee telefoniche.

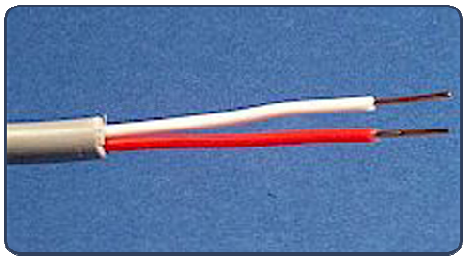
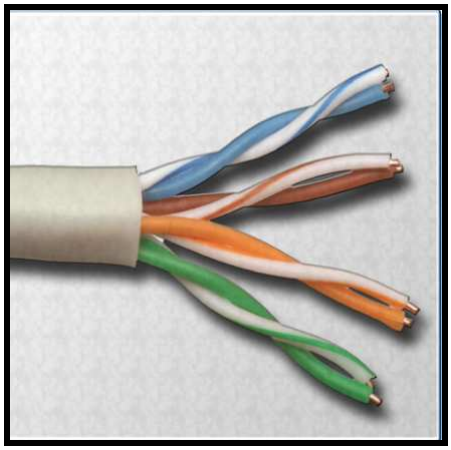


Fig. 2. Doppino telefonico

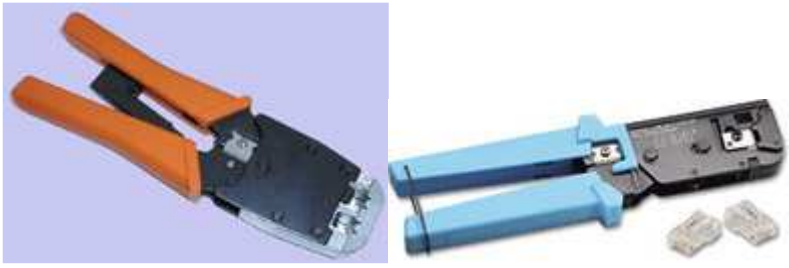
Cavi di rete ethernet UTP - connettore RJ45

Un **Cavo incrociato ethernet o crossover** è un tipo di cavo di rete usato per connettere assieme dei dispositivi di computer direttamente.

Il **cavo ethernet dritto** (anche detto Patch) con connettori RJ-45 permette di collegare il proprio computer o notebook ad uno SWITCH o HUB di rete in pochi secondi.
Il cavo è utilizzabile anche per collegare stampanti o dispositivi conformi allo standard di rete a routers ed access point.

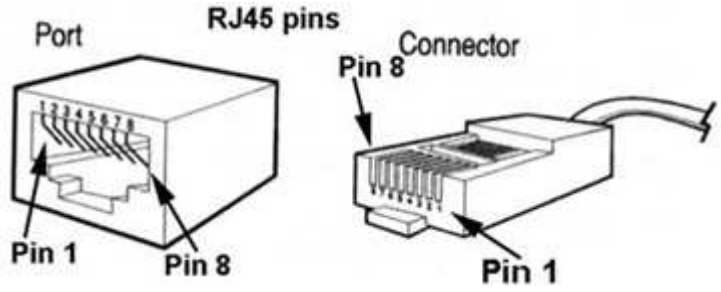


Cavo Twisted Pair



Due esempi di pinza a crimpare.

Un tipo di tester per cavi RJ45 ed una busta di connettori RJ45.



Connettore RJ45

Fig. 3. Cavi e e connettori di rete

- **Cavo Coassiale**

Un cavo coassiale è un cavo con un nucleo di rame circondato da una robusta schermatura. Il cavo coassiale viene utilizzato per collegare i computer in una rete; per la sua elevata larghezza di banda consente elevate velocità per distanze di diversi chilometri.. Ci sono diversi tipi di cavi coassiali:

a) **Thicknet 10BASE5** - Cavo coassiale utilizzato nelle reti, operante a 10 megabit al secondo su distanze massime di 500 metri
b) **Thinnet 10BASE2** - Cavo coassiale utilizzato nelle reti, operante a 10 megabit al secondo su distanze massime di 185 metri
c) **RG-59** - Più comunemente utilizzato per la televisione via cavo in America
d) **RG-6** - Di qualità superiore rispetto al cavo RG-59, con una maggiore larghezza di banda e meno sensibilità alle interferenze

In questa rete ogni PC deve avere una scheda di rete con connessione BNC per **cavo coassiale** con relativi driver installata correttamente; ad ogni scheda di rete è attaccato un connettore a T.
Si possono mettere quindi in serie tra loro più computer. Lo svantaggio di questa rete è che se si rompe un cavo coassiale la rete è rotta a metà. Dai due pc che stanno alle estremità di questa rete partono altri due cavi coassiali che devono terminare con un tappo terminatore da 50 ohm.
Il cavo coassiale è simile a quello usato per i televisori, solo che non è a 75 Ωma a 50Ω.

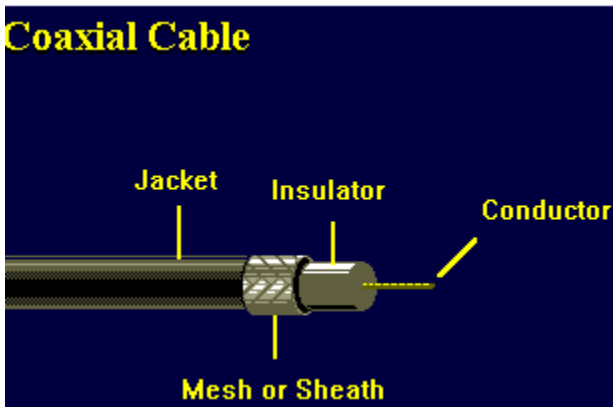


Fig. 4. Cavo coassiale

- **Fibra Ottica**

Una fibra ottica è un conduttore di vetro o di plastica che trasmette informazioni utilizzando la luce.;presenta una totale immunità al rumore elettromagnetico e consente velocità di trasmissione fino a 12Gbit/s avendo una larghezza di banda di oltre 10GHz. I segnali sono convertiti in impulsi di luce per entrare nel cavo, e convertiti in segnali elettrici quando escono dal cavo.
Vi sono due diverse tipologie di cavo in fibra ottica:

a) **Multimode** - Cavo con nucleo di diametro (tipico 50μm) maggiore rispetto a un cavo single-mode. È più facile da costruire, economica e può usare semplici sorgenti luminose (LED). Funziona bene su distanze di pochi chilometri .
b) **Single-mode** - Cavo con un nucleo molto sottile (tipico 9.5 μm). Utilizza il laser come sorgente di luce, e può trasmettere segnali fino ad una decine di chilometri. È più complessa nella costruzione e risulta poco economica.

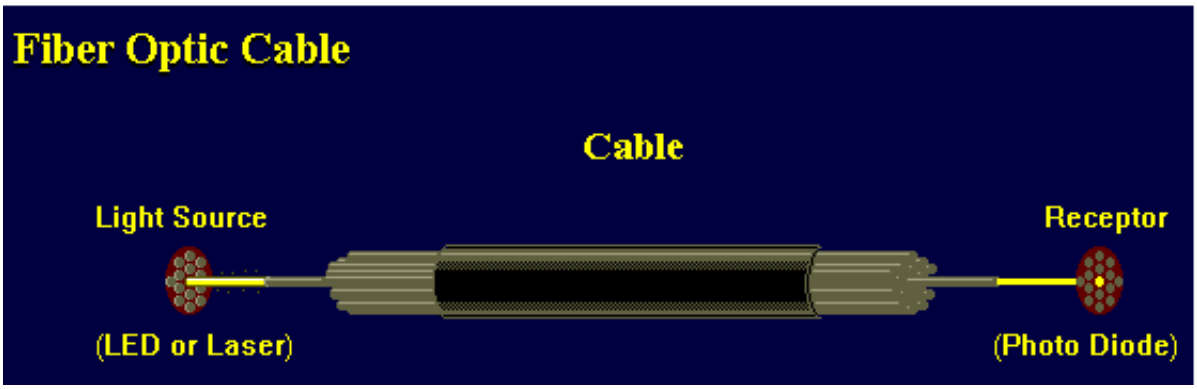


Fig. 5. Cavo in fibra ottica

- **Rete Powerlan o Rete PLC**

Utilizza la normale rete elettrica presente negli edifici per collegare i computer alla rete locale. La distanza massima tra i computer è dell'ordine di 100m. e la velocità di trasmissione è intorno a 10Mbit/s.
La tecnica **Powerline** (**Power Line Communication** o **PLC**) o sistema ad **onde convogliate** è una tecnologia per la trasmissioni di voce o dati che utilizza, come mezzo di collegamento tra computer, i cavi della rete elettrica presente in un locale, in un appartamento, in un edificio, in una città.
Una tecnologia Powerline molto diffusa in tutto il mondo ed anche in Italia è quella basata sul protocollo LonWorks ora anche standard ISO/OSI-14908-1-2-3-4, infatti su questo protocollo è basato il contatore che Enel installa da qualche anno che è in grado di fare la tele-lettura e le modifiche contrattuali da remoto.

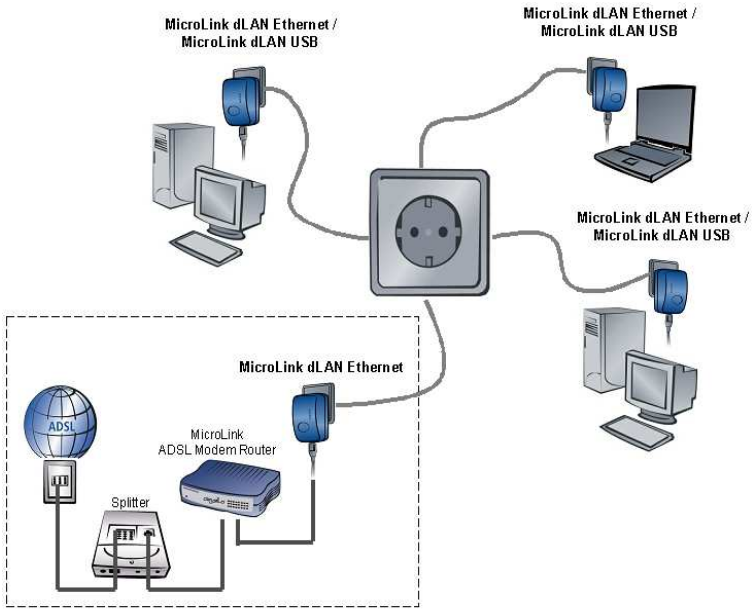


Fig.6. Esempio di rete powerlan costituita da 3 PC connessi ad internet via router ADSL. Servono 4 adattatori powerlan, ad esempio il MicroLink dLAN della "Devolo".

- **Reti Wireless o senza fili**

I mezzi trasmissivi che sfruttano l'etere per il trasporto delle informazioni si dividono:

- *a radiofrequenza (ponti radio, satelliti, onde radio al suolo);*
- *a infrarossi.*

Le reti wireless (senza fili) consentono la trasmissione dei dati per reti locali attraverso le onde radio. I primi risultati rispondono alle specifiche IEEE 802.11 approvate nel 1999.
Gli altri sistemi di trasmissione dati a breve distanza che utilizzano le onde radio sono i collegamenti ad *infrarossi*, sostanzialmente impiegati nei telecomandi, e la tecnologia *Bluetooth* utilizzata principalmente per i bassi costi di trasmissione e soprattutto per la possibilità di far comunicare qualunque tipo di dispositivo wireless attraverso onde radio.
La frequenza di lavoro è di 2.4GHz nella banda denominata ISM (Industrial, Scientific and Medical) che non richiede specifiche autorizzazioni di impiego.
La portata va da 30m a 100m in ambienti interni e da 100m a 500m in esterno. I valori dipendono dal dispositivo preso in esame. La presenza di ostacoli come muri, scaffali, tavoli, armadi, piani diversi, limita la portata delle onde radio.

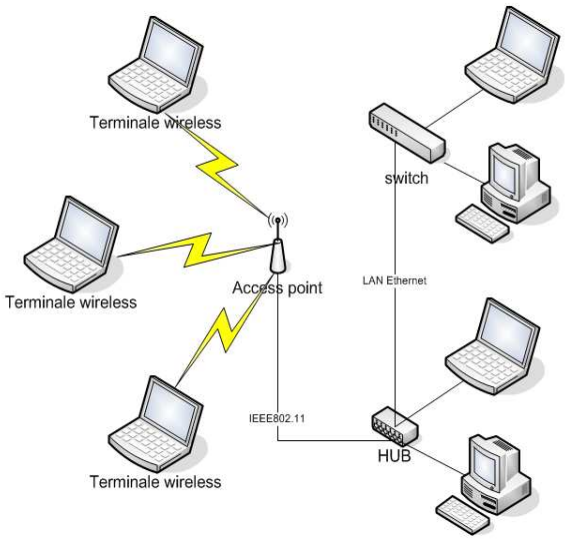


Fig. 7. Esempio di rete wireless

Tabella 1 - Principali caratteristiche degli standard wireless

standard	frequenza portante	velocità dei dati	tipo di modulazione
802.11a (Wi-Fi 5)	5.8GHz	54Mbps	OFDM
802.11b (Wi-Fi)	2.4GHz	11Mbps	DSSS
802.11g	2.4GHz	54Mbps	OFDM
802.11n	2.4GHz	108Mbps	

Legenda:
OFDM = Orthogonal Frequency Division Multiplexing
DSSS = Direct Sequence Spread Spectrum
Wi-Fi 5 = Il 5 rappresenta il valore della frequenza portante.

Confronto tra reti cablate e wireless

Tabella 2 - Confronti tra la Ethernet cablata e senza fili

	Wired Ethernet	Wireless Ethernet
Ingombro	predisposizione tracce e canalette per la posa dei cavi e punti rete	nessuna predisposizione o tracce e canalette solamente per le dorsali
Costi	costosa predisposizione del cablaggio, costo contenuto dei dispositivi di rete	costo contenuto del cablaggio, costi contenuti dei dispositivi di rete
Efficienza	velocità elevate, poco soggette a disturbi elettrici	velocità contenute, soggette a interferenze elettromagnetiche
Sicurezza	sicurezza maggiore data dalla necessità di possedere accesso fisico alla struttura	livello di sicurezza inferiore (i dati vengono trasmessi in radiofrequenza). Il livello di accesso alla rete può però essere autenticato e crittografato

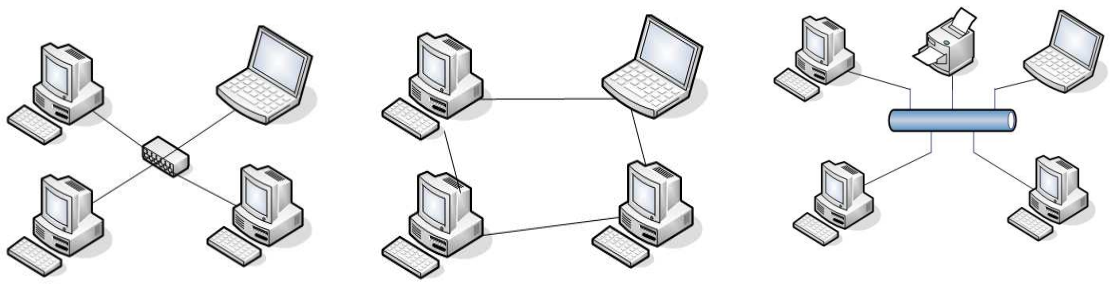
Topologia delle reti locali

Le strutture delle reti sono numerose ma tutte riconducibili a tre tipiche configurazioni fondamentali che sono:

- rete a stella;
- rete ad anello;
- rete a bus;
- Rete mista.

Per ciascuna di esse è possibile scegliere il mezzo trasmissivo da utilizzare, la tecnica di modulazione, il metodo di accesso alla rete ed il relativo tipo di controllo.

Nella **rete a stella** si individua un nodo centrale a cui sono collegati gli altri nodi attraverso trasmissioni bidirezionali. Il centro stella spesso è un apparato di rete come **Hub o Switch**.



a) Rete a stella **b) Rete ad anello** **c) Rete a bus**

Fig.8. – Tipologie delle reti.

Nella **rete ad anello** ogni nodo risulta connesso ai due nodi adiacenti da rami con collegamento punto-punto unidirezionale.

Una **rete a BUS** è costituita da un'unica linea multipunto a cui risultano collegati, tramite cavo coassiale.

Nella **rete mista** al bus principale, denominato ***dorsale***, sono collegate delle bretelle ognuna delle quali porta al centro di una sotto-rete locale a stella come si mostra in fig.2. Il centro stella è un dispositivo concentratore, di normalmente uno SWITCH, che ha il compito di dirigere il traffico di rete e di individuare eventuali problemi.

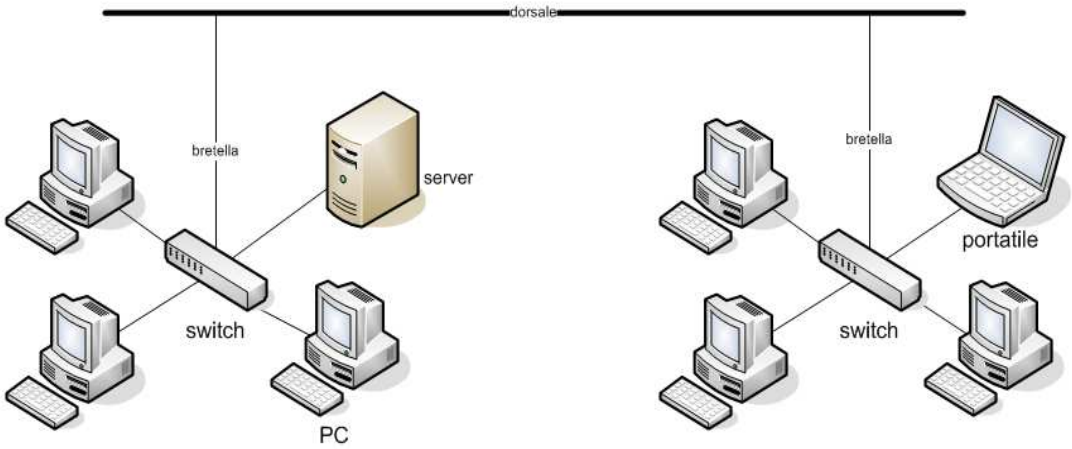


Fig.9 – Esempio di rete locale mista.

Reti peer-to-peer

La rete peer-to-peer (o P2P), cioè **rete paritaria**, è una rete di computer o qualsiasi rete informatica che non possiede nodi centralizzati come client o server fissi ma un numero di nodi equivalenti (peer). In particolare:

- Non vi è alcuna gestione centralizzata della rete, ciò rende difficile stabilire chi controlla le risorse della rete.
- Non vi è alcuna centralizzazione della sicurezza. Ogni computer deve utilizzare misure di sicurezza separate per la protezione dei dati.
- La rete diventa sempre più complessa e difficile da gestire, quando aumenta il numero di computer in rete.
- Non ci può essere la centralizzazione del backup dei dati.

Rete client/server

In una rete client/server, il client richiede le informazioni o i servizi da un dispositivo centralizzato detto **server**. Il server fornisce al client le informazioni o il servizio richiesti. Il server di una rete client/server esegue normalmente lavori di elaborazione per le macchine client; ad esempio, l'ordinamento di un database prima di fornire solo i record richiesti dal client. Risulta:

- rete sicura
- database centralizzato
- backup centralizzato (server)

Il software *server*, oltre alla gestione logica del sistema, deve implementare tutte le tecniche di gestione degli accessi, allocazione e rilascio delle risorse, condivisione e sicurezza dei dati o delle risorse.

Ad esempio un *server* di posta elettronica è paragonabile ad un qualunque ufficio postale. Gli utilizzatori per accedere via *client* alla loro cassetta di posta elettronica devono essere stati autorizzati. In modo analogo un utente deve possedere la chiave della cassetta sita presso un ufficio postale dalla quale vuole prelevare la corrispondenza.

Tecniche di accesso alla rete

Le tecniche di accesso descrivono le modalità con le quali i nodi terminali utilizzano il mezzo trasmissivo al fine di realizzare una corretta trasmissione delle informazioni.

L'obiettivo delle tecniche di accesso è quello di gestire in modo ottimale il traffico all'interno di una rete locale ovvero nella capacità di smaltire velocemente il traffico dati.

Esse si possono suddividere in due grandi categorie:

- **accesso a contesa**;
- **accesso a domanda**.

La **tecnica di accesso a contesa** è di tipo casuale e consente a ciascun nodo, in modo asincrono, di iniziare la trasmissione.

La **tecnica di accesso a domanda** cede ad un nodo il diritto di trasmettere sulla rete in determinati periodi di tempo.

Tecniche di accesso contesa

Tecnica CSMA (Carrier Sense Multiple Access)

La tecnica CSMA (accesso multiplo a rilevazione di portante) è una tecnica che consiste nell'*ascolto* del canale prima di passare alla trasmissione dei dati.

Se il canale è libero si procede alla trasmissione dei dati senza più preoccuparsi del controllo del canale.

Se il canale è occupato sono possibili due attività:

- aspettare che il canale si liberi prima di trasmettere;
- riascoltare il canale dopo un dato tempo di ritardo.

Questa tecnica non elimina del tutto la possibilità di collisione tra i dati trasmessi simultaneamente da due nodi perché potrebbe verificarsi il caso in cui due o più nodi, trovando il canale libero, inizino contemporaneamente la trasmissione generando, così, la collisione dei dati.

Tecnica CSMA/CD (Collision Detection)

Utilizzata nelle reti Ethernet e pubblicata come standard IEEE802.3, differisce dalla precedente durante la trasmissione dei dati; infatti, nella tecnica precedente, il nodo inizia la trasmissione se rileva il canale libero e non si cura più dell'ascolto del canale.

Nella tecnica CSMA/CD (CSMA a **rivelazione di collisione**) il nodo continua l'ascolto del canale anche a trasmissione avviata: in caso di collisione la comunicazione in corso viene sospesa, il nodo trasmettitore genera una stringa binaria di 4-6 byte, nota come "sequenza di jamming", che permette a tutte le stazioni di rilevare la collisione e di scartare i bit ricevuti come frutto della collisione.

Il nodo trasmettitore ripete la procedura di inizio trasmissione dopo un intervallo di tempo di attesa pseudocasuale To.

In questo modo difficilmente i due nodi potranno rientrare in conflitto.

Questo metodo consente di ridurre fortemente la possibilità di collisione rendendo, così, la trasmissione più efficiente.

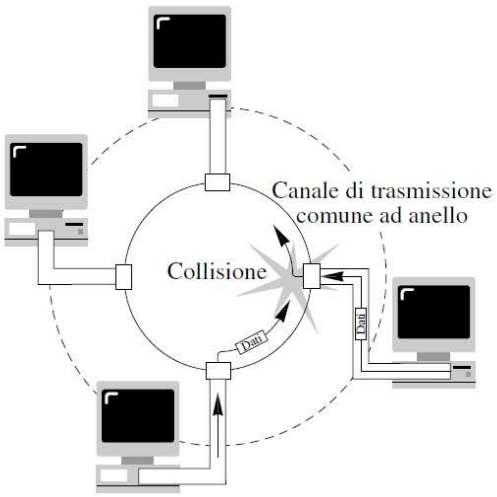


Fig. 10. Tecnica CMSA/CD

Tecniche di accesso a domanda

Le tecniche di accesso a domanda si possono utilizzare nelle reti locali ad anello e a stella e consistono nell'interrogazione ciclica dei nodi oppure nell'inserire nella rete una stringa (**token**) che fornisce al nodo che la riceve il consenso o il diniego all'accesso alla rete. Le reti che adottano queste tecniche di accesso non hanno il problema della contesa del mezzo trasmissivo e, di conseguenza, non sono soggette a collisioni.

Tecnica di Polling/Selecting

È utilizzata nelle reti a stella e ad anello in cui un nodo svolge la funzione di controllore.
Nella tecnica di *polling* il controllore effettua una interrogazione ciclica ai nodi della rete: un nodo potrà trasmettere dati al nodo controllore solo quando quest'ultimo glielo consente.

Tecnica Token-ring

Sviluppata dalla IBM e successivamente pubblicata come standard IEEE802.5, è utilizzata nelle reti ad anello ed è in grado di stabilire l'ordine e il momento in cui un nodo può trasmettere le informazioni.
Il nodo controllore trasmette in rete una particolare configurazione di bit nota col nome di **token** (**gettone**) che consente, a chi lo riceve, di avviare la trasmissione, ammesso che abbia qualcosa da trasmettere. Se il nodo che ha catturato il token non ha alcun dato da trasmettere, rimette in rete il token che giungerà al successivo nodo.
Il nodo che desidera trasmettere, subito dopo aver catturato il token, avvia la trasmissione dei dati, dell'indirizzo del destinatario ed, infine, del token.
Il token, in questa tecnica, soddisfa alcune regole:

- è uno solo in tutta la rete;
- non può essere usato da un nodo due volte consecutivamente.

Protocolli TCP/IP

Va sotto il nome di TCP/IP (Transmission Control Protocol/Internet Protocol) un insieme di circa 100 protocolli che consentono di dar vita ad *internet*, la rete delle reti.
L'obiettivo di internet è quello di assicurare la comunicazione di dati digitali dalla postazione di una rete locale alla postazione di un'altra rete, anche tecnologicamente diversa dalla prima, attraverso collegamenti che danno vita ad una particolarissima e sconfinata rete geografica. Vi sono, pertanto,

particolari dispositivi di rete, di nome ***gateway,*** che hanno appunto il compito di stabilire il percorso che devono compiere i dati nel transitare da una rete locale all'altra.
La tecnica di trasmissione utilizzata da internet è a *commutazione di pacchetto* con servizio a datagramma.
Il file da trasmettere viene suddiviso in frammenti ognuno dei quali prende il nome di *pacchetto*. Ogni pacchetto è autonomo poiché contiene tutte le informazioni necessarie: indirizzo IP del mittente e del destinatario, numero di sequenza, tipo di applicazione, ecc. Ogni pacchetto, per raggiungere la destinazione, prende un percorso autonomo che può essere diverso da quello attraversato da altri pacchetti.
Anche l'ordine di arrivo può essere differente per cui il protocollo TCP/IP del destinatario deve poter mettere "nella giusta sequenza" i pacchetti pervenuti.
Al TCP/IP appartengono, separatamente, anche il protocollo TCP e il protocollo IP.
Il TCP/IP è organizzato a livelli; in ciascuno di questi vengono svolti compiti specifici correlati a quelli dei livelli adiacenti attraverso interfacce.
I livelli del TCP/IP sono 4 e corrispondono in parte a quelli del modello ISO/OSI.

Tabella 3

ISO/OSI		**TCP/IP**	
Applicazione		Applicazione	
Presentazione			HTTP, FTP, SMTP, TELNET
Sessione			
Trasporto		Trasporto	TCP, UDP
Rete		Rete	IP, ICMP, ARP, RARP
Linea		Linea + Fisico	IEEE 802, EIA232, X21, ISDN, ecc.
Fisico			

Il **quarto livello**, il più alto, è quello nel quale gira la specifica applicazione (TELNET, FTP, SMTP, HTTP, ecc.).
Il **terzo livello**, corrispondente al quarto livello del modello OSI (trasporto), è utilizzato dal protocollo TCP che ha il compito di garantire che i pacchetti giungano a destinazione e che vengano opportunamente e ulteriormente suddivisi per consentire il passaggio su particolari rami della rete.
Il **secondo livello**, corrispondente al livello di rete del modello OSI, è utilizzato dal protocollo IP che ha il compito di instradare le informazioni al ricevitore.
Il **primo livello**, o **Data link** corrispondente ai primi due livelli del modello OSI, è relativo alle interfacce fisiche che consentono il reale trasferimento dei segnali elettrici. È responsabile dell'inoltro dei datagrammi IP su uno specifico tipo di rete (es. Ethernet, ATM, PPP, HDLC etc..)

Incapsulamento dei dati

Durante una trasmissione, i dati attraversano alcuni degli strati al livello del terminale emittente. Ad ogni livello, un'informazione viene aggiunta al pacchetto di dati, si tratta di un' intestazione, un insieme di informazioni che garantisce la trasmissione. A livello del terminale ricettore, al momento del passaggio in ogni livello, l'intestazione viene letta, poi cancellata. Così, alla ricezione, il messaggio è nel suo stato originale…

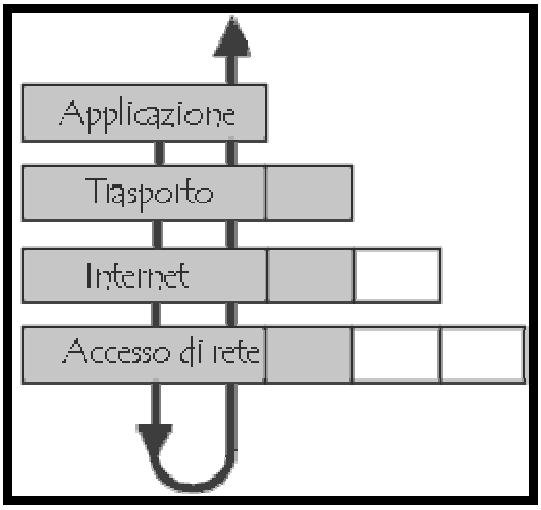


Fig. 11. Incapsulamento dei dati

Ad ogni livello, il pacchetto cambia d'aspetto, dato che gli si aggiunge un'intestazione, e quindi le denominazioni cambiano seguendo i livelli :

- Il pacchetto di dati è detto **messaggio** al livello Applicazione
- Il messaggio in seguito è incapsulato sotto forma di **segmento** nel livello Trasporto
- Il segmento, una volta incapsulato, nel livello Internet prende il nome di **datagramma**
- Infine, si parla di **trame** sul livello Accesso di rete

Il formato delle trame Ethernet, o PDU-Protocol Data Units *di Livello 2*.
Il *formato del pacchetto* prevede otto campi, di seguito elencati:

n.byte	7	1	6	6	2	0-1500	0-46	4
campo	**Preambolo**	**Inizio trama**	**MAC address ricevitore**	**MAC address trasmettitore**	**Tipo**	**Dati**	**Riempitivo**	**CRC**

1. **Preambolo**. È costituito da 7 byte uguali dal codice binario 10101010 (HEX: AA) e serve per la sincronizzazione dei nodi ricevitori; se la rete funziona a 10Mbps, la durata del preambolo è pari a 5.6µs (7byte · 8bit · 0.1µs).
2. **Inizio trama**. È costituito dal byte 10101011 (HEX: AB) e segnala la fine del preambolo e quindi l'inizio del pacchetto dati vero e proprio.
3. **MAC Address** del nodo di destinazione. È costituito da 6 byte. Se tutti i bit sono a 1 i dati vengono inviati a tutti i nodi;
4. **MAC Address** del nodo di origine. È costituito anch'esso da 6 byte;
5. **Tipo**. È costituito da 2 byte. Se minore o uguale a 1500 indica la lunghezza del campo dati. Se maggiore di 1500 contiene informazioni di servizio che cambiano di significato in funzione dell'ambiente in cui ci si trova.
6. **Campo dati**. È costituito da una lunghezza che va da 0 a 1500 byte.
7. **Campo riempitivo**. È di lunghezza variabile in funzione della quantità di dati del precedente campo dati. Questo campo garantisce che la lunghezza della trama complessiva sia almeno di 64byte anche in assenza di dati da trasmettere. In questo ultimo caso la lunghezza di tale campo è di 46byte.
8. **Campo controllo CRC**. È costituito da 4 byte. Contiene il codice ciclico di ridondanza (CRC) dei campi indirizzo del nodo di destinazione, di origine e del campo dati. I 18 byte del campo di intestazione sono la somma dei byte occupati nei campi MAC address, tipo e campo di controllo.

Indirizzi IP

Le reti collegate ad internet attraverso i protocolli TCP/IP utilizzano un indirizzo a 32 bit (oltre 4 miliardi di configurazioni numeriche), secondo lo standard RFC 791 (Request For Comments) http://www.faqs.org/rfcs/rfc791.html per individuare un computer e la rete nella quale è inserito il computer. Il formato di tale indirizzo è:

Indirizzo IP = Indirizzo di rete + Indirizzo di host

L'indirizzo è rappresentato da 4 byte ognuno dei quali espresso in forma decimale da 0 a 255 e separato dagli altri con un punto. Tale protocollo è noto come IPV4.
Il gruppo di lavoro IETF (Internet Engineering Task Force) ha messo a punto la versione 6 del protocollo IP coniando il termine IPV6 che utilizza 6 byte per gestire gli indirizzi.. In tal modo si metterebbe a disposizione un numero sconfinato di possibili indirizzi IP (2^{128}).
Sono consentiti quattro tipi di formati di indirizzo IP indicati con classe A, classe B, classe C e classe D.
NOTA: Si escludono quegli indirizzi IP che hanno indirizzo di rete costituito da tutti 0 e da tutti 1 e, analogamente, si escludono quelli con indirizzo di host costituito da tutti 0 e da tutti 1. Quando l'indirizzo di host è costituito da tutti 0 l'indirizzo IP esprime l'indirizzo di rete. Quando l'indirizzo di host è costituito da tutti 1 si ha il broadcast a tutti i PC della rete.

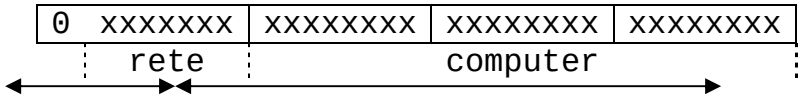
Tabella 4

Classe	bit iniziali	indirizzo rete (in bit)	indirizzo host (in bit)	reti individuabili	host disponibili
A	0	7	24	128	16.777.216
B	10	14	16	16.384	65.536
C	110	21	8	2.097.152	254
D	1110	Indirizzo Multicast a 28 bit (268.435.456 indirizzi)			
E	11110	Riservato per usi futuri a 27 bit (134.217.728 indirizzi)			

IP è un protocollo di strato di rete che svolge le funzioni di:
- indirizzamento;
- instradamento;
- frammentazione;
- aggregazione.

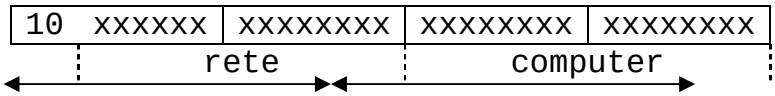
Classe A

È il formato di indirizzo per reti aventi un numero elevatissimo di host. Le reti disponibili sono 126 (da 1 a 126; i numeri 0 e 127 sono riservati). Il campo per individuare un host è di 24 bit corrispondente ad un numero massimo superiore a 16 milioni. Il primo numero dell'indirizzo IP va da 1 a 126 ed individua la rete; i restanti 3 numeri (24 bit) individuano l'host all'interno della rete. Gli host individuati da tutti 0 e da tutti 1 non sono utilizzabili.
L'intervallo dei valori consentiti va da 1.0.0.1 a 126.255.255.254.

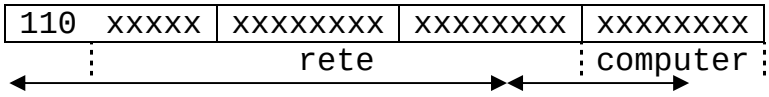


Si riportano alcune società che hanno indirizzi IP in classe A:
Hewlett Packard (15.0.0.0), Apple Computer (17.0.0.0), Stanford University (36.0.0.0), Posta Americana (56.0.0.0).

Classe B
Gli indirizzi di classe B sono utilizzati dalle reti di dimensioni intermedie. Le reti individuabili sono oltre 16000 (14 bit) e il numero massimo di host di ciascuna rete è superiore a 64000 (16 bit). I primi due numeri dell'indirizzo IP vanno da 128.1 a 191.254 ed individuano la rete (al solito si escludono il primo e l'ultimo indirizzo cioè 128.0 e 191.255); i restanti due numeri individuano l'host all'interno della rete. Gli host individuati da tutti 0 e da tutti 1 non sono utilizzabili.
L'intervallo dei valori consentiti va da 128.1.0.1 a 191.254.255.254.



Classe C
Gli indirizzi di classe C sono utilizzati da reti molto piccole. Le reti individuabili sono oltre due milioni (21 bit) ed il numero massimo di host di ciascuna rete è di 254 (si escludono 0 e 255). I primi tre numeri dell'indirizzo IP vanno da 192.0.1 a 223.255.254 ed individuano la rete; l'ultimo numero, da 1 a 254, individua l'host all'interno della rete.
L'intervallo dei valori consentiti va da 192.0.1.1 a 223.255.254.254.



Esempio

Individuare il tipo di rete, l'indirizzo di rete e di host per il seguente indirizzo IP:

195.32.115.9 (1)

Risoluzione

L'indirizzo IP assegnato corrisponde al seguente numero binario a 32 bit:
11000011 00100000 01110011 00001001

L'indirizzo di rete si ottiene dalla (1) eliminando i bit che individuano la classe (110 per la classe C) e gli ultimi 8 bit che rappresentano l'indirizzo di host.

$00011\ 00100000\ 01110011_2 = 204915_{10}$.

L'indirizzo interno dell'host è: $00001001_2 = 9_{10}$.

Sottoreti

Una rete locale fisica può suddividersi in una o più sottoreti locali logiche. Per far questo si utilizza una particolare maschera costituita da 32 bit, suddivisa in 4 numeri separati da punti, come l'indirizzo IP, nota come ***subnet mask*** (maschera di sottorete).
I computer con stessa subnet mask appartengono alla stessa sottorete.

La subnet mask individua la sottorete. Il computer con subnet mask 255.255.255.0 ed indirizzo IP 192.168.0.5 appartiene alla rete di classe C 192.168.0.0. Qualsiasi computer i cui primi tre numeri dell'indirizzo IP sono pari a 192.168.0 appartiene alla rete. Per individuare una sottorete si utilizzano due o più bit da sottrarre all'indirizzo di host. Nella subnet mask devono essere posti ad uno i bit omologhi ai seguenti campi:
bit iniziali, indirizzo di rete, indirizzo di sottorete.
In pratica l'indirizzo IP di un nodo della rete è costituito da 4 campi:

bit iniziali	indirizzo di rete	indirizzo di sottorete	indirizzo di host

Volendo realizzare due o più sottoreti della rete locale in classe C 192.168.0.0, il quarto numero della subnet mask dovrà essere diverso da 0.

Esempio 1

Ponendo a 1 i primi due bit del quarto numero della subnet mask, si individuano 4 sottoreti (4 combinazioni degli omologhi bit degli indirizzi IP dei computer della rete: 00, 01, 10, 11).
Subnet mask: $255.255.255.192_{10}$ = $11111111.11111111.11111111.11000000_2$
Indirizzo della rete fisica: 192.168.0.0
Sottorete 0: da 192.168.0.0 a 192.168.0.63
Sottorete 1: da 192.168.0.64 a 192.168.0.127
Sottorete 2: da 192.168.0.128 a 192.168.0.191
Sottorete 3: da 192.168.0.192 a 192.168.0.255

Ogni sottorete dispone di 64 indirizzi IP di cui solo 62 sono utilizzabili (si escludono il primo e l'ultimo di valore 0 e 63, come al solito). Infatti, potendo gestire 6 bit di indirizzo di host si possono individuare un massimo di 2^6=64 host da cui sottrarre il primo e l'ultimo (64-2=62).

Esempio 2

Ponendo a 1 i primi 3 bit del quarto numero della subnet mask, posso individuare 8 sottoreti.

La subnet mask vale: 255.255.255.224 e le sottoreti sono:
Sottorete 0: 192.168.0.0 - 192.168.0.31
Sottorete 1: 192.168.0.32 - 192.168.0.63
Sottorete 2: 192.168.0.64 - 192.168.0.95
Sottorete 3: 192.168.0.96 - 192.168.0.127
Sottorete 4: 192.168.0.128 - 192.168.0.159
Sottorete 5: 192.168.0.160 - 192.168.0.191
Sottorete 6: 192.168.0.192 - 192.168.0.223
Sottorete 7: 192.168.0.224 - 192.168.0.255

Ogni sottorete dispone di 32 indirizzi IP di cui solo 30 sono utilizzabili (si escludono il primo e l'ultimo). Infatti, potendo gestire 5 bit di indirizzo di host si possono individuare un massimo di 2^5=32 host da cui sottrarre il primo e l'ultimo (32-2=30).

Si mostra in fig. 12 una rete fisica suddivisa in 2 sottoreti logiche. Il quarto numero della subnet mask di ciascun PC vale 192 che, in binario, corrisponde a 1100000. Si possono individuare 4 sottoreti, come nell'esempio 1. Alla sottorete 1 appartengono i PC con indirizzi di host 100 e 101; alla sottorete 2 appartengono i rimanenti 3 PC con indirizzi di host 130, 131 e 132.

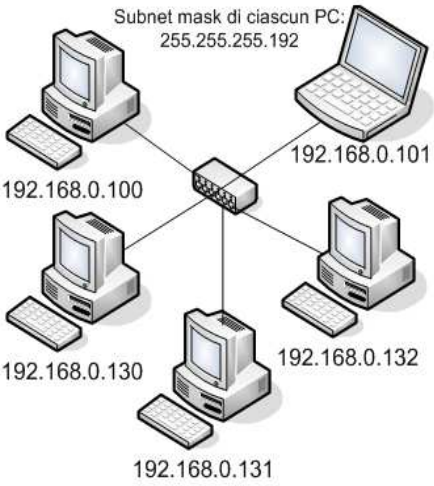


Fig.12. – Rete fisica suddivisa in due sottoreti logiche.

Assegnazione degli IP

Una rete locale può utilizzare il protocollo TCP/IP per lo scambio dei dati tra gli elementi della LAN. In tal caso ciascun nodo deve possedere un **indirizzo IP che può essere fisso** oppure **assegnato dinamicamente** come, ad esempio, viene attribuito dal **servizio DHCP** (Dynamic Host Configuration Protocol), se attivato, del sistema operativo di rete Windows Server.
Il (DHCP) è un programma di utilità software utilizzato per assegnare dinamicamente gli indirizzi IP ai dispositivi di rete.
Le informazioni di indirizzamento IP che un server DHCP può assegnare ad un PC:

- Indirizzo IP
- Subnet mask
- Default gateway
- Valori opzionali, come ad esempio un indirizzo del server DNS (Domain Name System)

Funzionalità APIPA (Automatic Private IP Addressing)

APIPA è un meccanismo che permette di assegnare un indirizzo IP ad un client senza ricorrere né alla configurazione statica (manuale) né ad un server DHCP.

Quando un client ha necessità di un indirizzo IP in mancanza di indirizzo statico ed in assenza di server DHCP, il protocollo APIPA in funzione su ogni singolo client auto-assegna un indirizzo IP nel range 169.254.0.0 e 169.254.255.255 con subnet mask 255.255.0.0.
Dopo la generazione dell'indirizzo il protocollo prevede la verifica di unicità dell'indirizzo generato tramite un broadcast. Se nessun altro client ha tale indirizzo trasmesso in broadcast, quest'ultimo diventa effettivo
Il processo si ripete finché l'indirizzo assegnato è univoco. Periodicamente (circa 5 minuti) il client ricerca la presenza di un server DHCP, in assenza del quale continuerà ad utilizzare l'indirizzo assegnato da APIPA.

Indirizzi IP privati

Esistono particolari **intervalli di indirizzi privati IP** destinati ai nodi delle reti locali e non accessibili da internet. Ciò consente una certa protezione dei dati che circolano all'interno della LAN lontano da occhi indiscreti.

Nella seguente tabella 5 si forniscono gli intervalli di indirizzi privati utilizzabili dalle postazioni LAN. Essi possono essere di classe A, di classe B e di classe C. La scelta che l'amministratore di rete dovrà compiere è funzione della dimensione della rete locale.

Tabella 5. – Indirizzi IP privati utilizzabili nelle reti LAN

Classe	Intervallo di indirizzi
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

In genere si preferiscono gli indirizzi di classe C poiché quasi tutte le reti locali sono costituite da meno di 254 nodi. In particolare si sceglie la rete con indirizzo 192.168.0.0.
Il computer server normalmente ha indirizzo 192.168.0.1 e nella rete si possono individuare fino a 254 nodi. Quello con indirizzo IP più alto è 192.168.0.254.
Un altro indirizzo IP particolare è 127.0.0.1 che individua il computer locale (**localhost**), la macchina, cioè, su cui si sta lavorando.

DNS

Poiché non è facile ricordare a memoria l'indirizzo IP numerico del server al quale ci si desidera collegare, si è pensato di utilizzare un indirizzo mnemonico da porre in corrispondenza biunivoca con l'indirizzo numerico IP attraverso una tabella.
L'insieme degli indirizzi mnemonici è denominato DNS (Domain Name System).
La scelta dell'indirizzo mnemonico non è del tutto arbitraria perché deve seguire una logica che consente, seppur in minima misura, di riconoscere la natura del sito: università (edu), militare (mil), governativo (gov), commerciale (com), italiano (it), inglese (uk), svizzero (ch), francese (fr), europeo (eu), ecc. e il tipo di protocollo: ftp, www, mail, news, ecc. I vari nomi che compongono l'indirizzo sono separati tra loro da un punto. La documentazione è disponibile nella RFC 1034 http://www.faqs.org/rfcs/rfc1034.html

Ad esempio, i seguenti DNS individuano, rispettivamente:
http://www.tiscali.it un server *Wide World Web italiano* di nome *tiscali*.
http://www.sony.com un server *Wide World Web commerciale* di nome *sony*.
ftp://ftp.libero.it/pub/ la sottodirectory *pub* del server *ftp italiano* di nome *libero*.

I prefissi http (HyperText Transfer Protocol) ed ftp (File Transfer Protocol) individuano il tipo di applicazione da utilizzare.

Protocolli per la risoluzione degli indirizzi

Il **protocollo ARP** (Address Resolution Protocol, RFC 826, reperibile sul sito http://www.faqs.org/rfcs/rfc826.html) consente di determinare l'indirizzo univoco di scheda di rete (MAC address) a partire dall'indirizzo IP del destinatario del pacchetto. Il protocollo funziona nel seguente modo: viene inviata a tutti i nodi della rete LAN una richiesta del tipo "a chi appartiene questo indirizzo IP?"; risponde solo il nodo che ha tale indirizzo fornendo anche il MAC address.
Vi sono alcune stazioni di lavoro senza disco fisso che non conoscono il proprio indirizzo IP.
Per ottenere l'indirizzo IP la stazione invia a tutti il proprio MAC address e solo il **server RARP** (Reverse Address Resolution Protocol) è in grado di trasmettere l'indirizzo IP conoscendo quello fisico. Il server RARP, quindi, esegue l'operazione inversa rispetto al protocollo ARP.

LAN con Router

Un **Router** è un'apparecchiatura che permette la comunicazione tra reti eterogenee (ad esempio: rete locale con rete internet) svolgendo funzioni nel livello fisico OSI, di collegamento dati e di rete.

In particolare un router:

- Nei livelli fisico e data link, deve essere in grado di trasformare frame, creati con tecnologie differenti;
- Nel livello network, instrada i pacchetti generati dai computer di reti differenti.

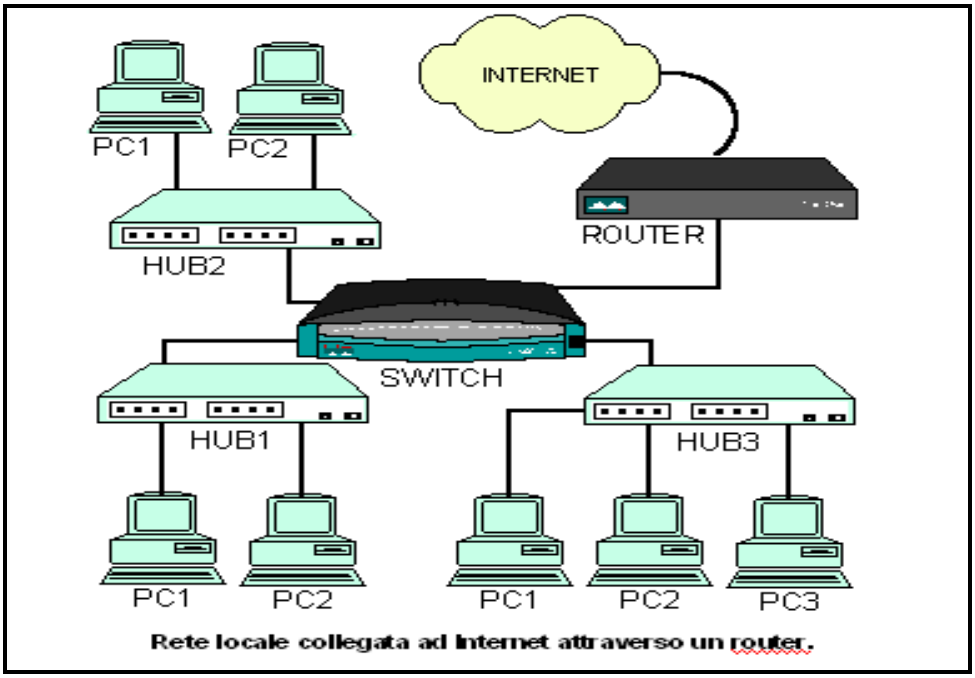


Fig. 12. Rete con router

Il router collegato ad Internet è il **Server/Gateway**: un piccolo computer (senza tastiera e mouse) che offre la condivisione dei servizi Internet alle altre macchine della rete e mette in collegamento con Internet la mini LAN interna. L'hardware di rete necessario per realizzare la piccola LAN è costituito, oltre che dal Router, dalle schede di rete, da un concentratore, Hub o Switch, che distribuisce fisicamente i dati (a meno che il router non svolga anche la funzione di concentratore) e, naturalmente, dai cavi di rete (Twisted Pair) da collegare al concentratore e alle schede di rete.

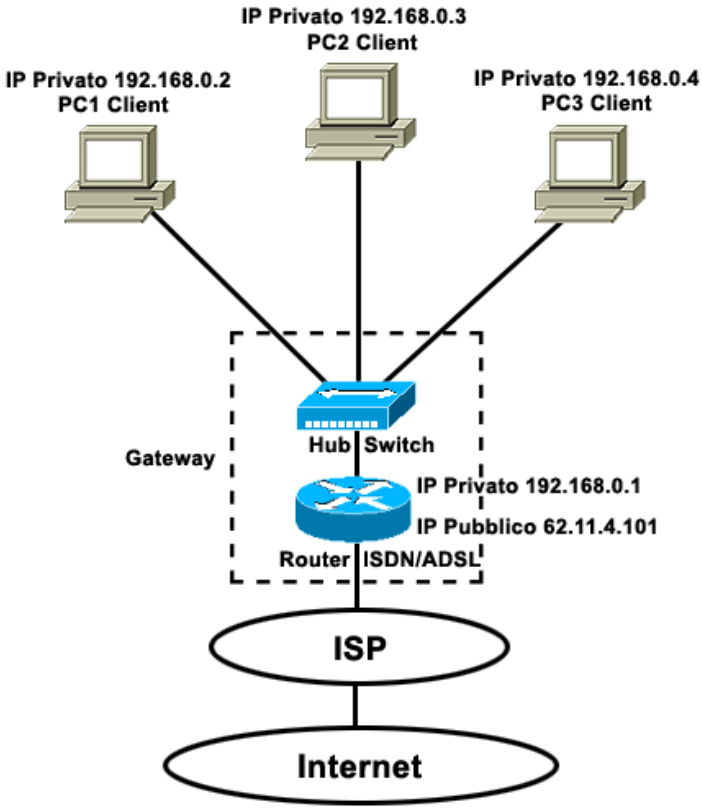


Fig. 13. Rete con router

Osservando lo **schema della rete,** si deduce chiaramente che l'architettura è, in questo caso, del tipo Client/Server; la topologia **fisica a stella** e quella **logica Ethernet**.
Nella tecnica utilizzata dal router, è necessario precisare che i PC Client dispongono di un indirizzo IP privato, mentre il router gateway possiede sia un indirizzo IP privato che un IP pubblico (vedi figura sopra).
L'utilizzo di un router al posto di un computer che funge da Server/Gateway è una soluzione ideale se non si dispone di un computer a cui devolvere tale funzione.

Il protocollo ICMP (Internet Control Message Protocol)

Il protocollo IP fornisce un meccanismo di trasferimento dei pacchetti dal mittente al destinatario secondo un approccio best-effort (letteralmente: sforzo migliore). Questo vuol dire che l'IP non è in grado di garantire la consegna dei pacchetti (chiamati "datagrammi" in analogia con i telegrammi) al destinatario, ma esegue dei tentativi di consegna, al meglio delle possibilità di cui dispone, e non si fa remore di ignorare i datagrammi che per qualche motivo non riesce a gestire. Si dice che quei datagrammi vengono "dropped on the floor", cioè "lasciati cadere in terra", persi per sempre. Per questo motivo è benvenuto un meccanismo che consenta un error-reporting, offerto appunto dall'ICMP, che sta per Internet Control Message Protocol (Protocollo per i Messaggi di Controllo in Internet). Il protocollo ICMP è descritto dall'RFC 792.
ICMP, come TCP e UDP, utilizza i servizi del livello IP, tuttavia viene ritenuto generalmente parte integrante del protocollo IP (ICMP è incluso nelle specifiche del protocollo IP).

Comandi TCP/IP

PING (Packet Internet Groper) è un tipo comando che fa uso del protocollo ICMP

Il ping è uno strumento di troubleshooting utilizzato per determinare la connettività a livello IP.

Durante le attività di risoluzione dei problemi è possibile utilizzare il comando **ping** per inviare una richiesta echo ICMP a un nome host o a un indirizzo IP di destinazione. Utilizzare il comando **ping** quando è necessario verificare se un computer host è in grado di connettersi alla rete TCP/IP e alle risorse di rete. È inoltre possibile utilizzare il comando **ping** per individuare problemi hardware della rete e configurazioni non compatibili.
Il miglior modo di procedere consiste in genere nel verificare che esista una route tra il computer locale e un host di rete utilizzando innanzitutto il comando **ping** e l'indirizzo IP dell'host di rete al quale si desidera connettersi. Provare a eseguire il ping sull'indirizzo IP dell'host di destinazione per controllare se risponde, come illustrato di seguito:
ping *indirizzo_IP*

Quando si utilizza il comando **ping**, si consiglia di procedere come segue:

1. Eseguire il ping sull'indirizzo di loopback per verificare che TCP/IP sia configurato correttamente nel computer locale: **ping** 127.0.0.1
2. Eseguire il ping sull'indirizzo IP del computer locale per controllare che sia stato aggiunto alla rete in modo corretto.
   ping localhost
3. Eseguire ping sull'indirizzo IP del gateway predefinito per controllare che sia funzionante e che sia possibile comunicare con un host locale sulla rete locale.
   ping *indirizzo_IP_gateway_predefinito*
4. Eseguire ping sull'indirizzo IP di un host remoto per controllare che sia possibile comunicare tramite un router. Esempio:
   ping www.ettorepanella.com

IPCONFIG

Quando si utilizza il comando **ipconfig** con l'opzione **/all**, viene creato un rapporto dettagliato sulla configurazione per tutte le interfacce, incluse le eventuali porte seriali configurate. Con il comando **ipconfig /all** è possibile reindirizzare l'output del comando su un file e incollare il testo in altri documenti. È inoltre possibile utilizzare questo output per verificare la correttezza della configurazione TCP/IP di ogni computer della rete o per indagare ulteriormente sui problemi di rete relativi a TCP/IP.

TRACERT

TRACERT consente di stampare un elenco ordinato dei router nel percorso che ha restituito il messaggio ICMP di tempo scaduto. Se l'opzione -d viene utilizzata (indicando TRACERT non esegua una ricerca DNS in ciascun indirizzo IP), verrà restituito l'indirizzo IP di interfaccia dei router. TRACERT è utile per la risoluzione dei problemi di reti di grandi dimensioni in cui è possibile eseguire più percorsi per arrivare allo stesso punto o in cui sono coinvolti molti sistemi intermedi (router o bridge).

Esempio: **tracert 11.1.0.1 oppure**

tracert www.libero.it