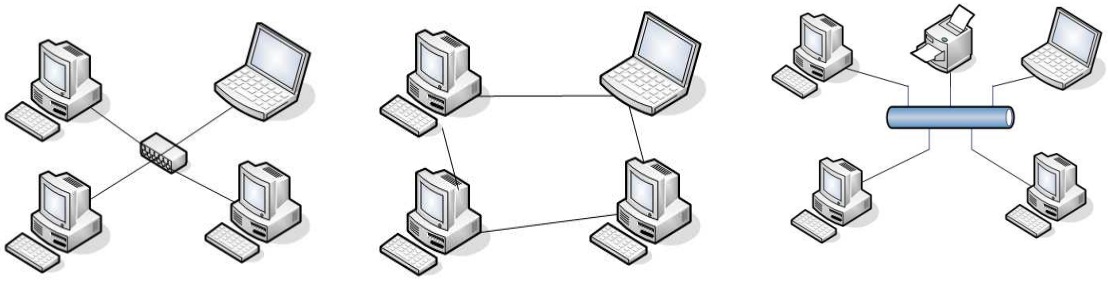
Protocolli e reti di computer
(prof. Ettore Panella)

Topologia delle reti locali

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



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

Dispositivi di Rete

I dispositivi necessari per realizzare una rete di PC sono:

- Computer (con software per gestione della rete) dotati di schede di rete
- Cavi (UTP, fibre ottiche, doppino telefonico)
- Hub e/o Switch (nodo di smistamento dei dati)
- Router (consente di connettere host appartenenti a reti diverse)
- Access Point Wireless (consente all'utente mobile di collegarsi ad una rete *wireless*)

Ogni scheda di rete possiede un indirizzo univoco, denominato **MAC Address**, impostato in fabbrica dalla casa costruttrice. Non esistono due schede al mondo con MAC uguali tra loro. Il MAC è composto da 6 byte (48 bit) espressi in notazione esadecimale (ad esempio: 00-E0-18-FF-59-7F). I primi 3 byte individuano la casa costruttrice, gli altri il numero di serie.

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.

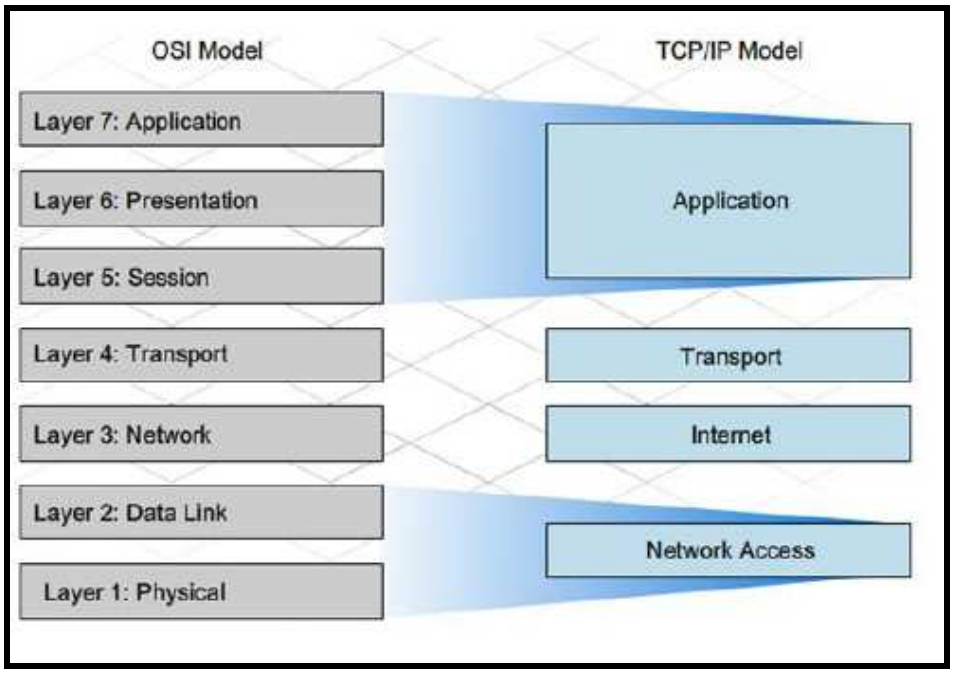
Tecnica CSMA/CD (Collision Detection)
Utilizzata nelle reti Ethernet e pubblicata come standard IEEE802.3, differisce dalla precedente durante la trasmissione dei dati; infatti, nella tecnica precedente, il nodo inizia la trasmissione se rileva il canale libero e non si cura più dell'ascolto del canale.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

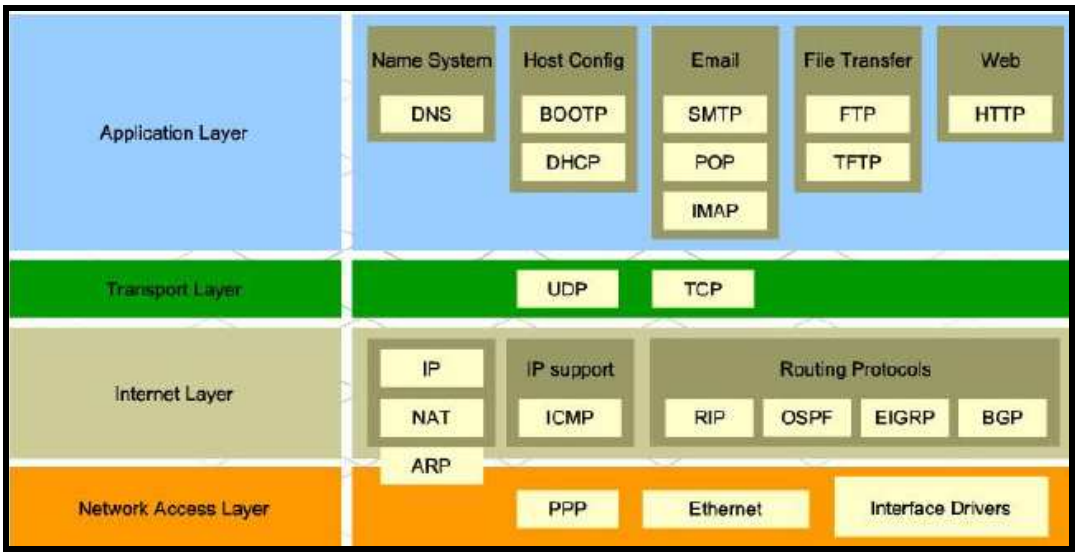
Tecniche di accesso a domanda

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.

Modello ISO/OSI e modello TCP/IP

La tecnica di trasmissione utilizzata da internet è a ***commutazione di pacchetto***. 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.
Il protocollo ISO/OSI è un modello generale a 7 livelli. Il protocollo TCP/IP è un modello a 4 livelli riconducibile al modello generale.



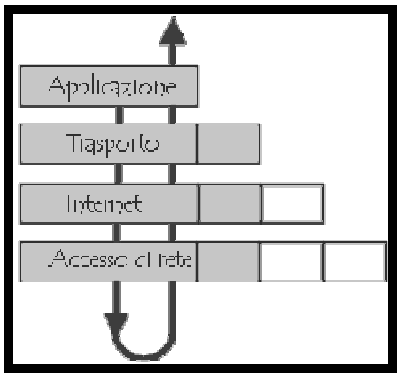


Il **quarto livello**, il più alto, è quello nel quale gira la specifica applicazione (TELNET, FTP, SMTP, HTTP, ecc.).
Il **terzo livello**, corrispondente al quarto livello del modello OSI (trasporto), è utilizzato dal protocollo TCP che ha il compito di garantire che i pacchetti giungano a destinazione 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

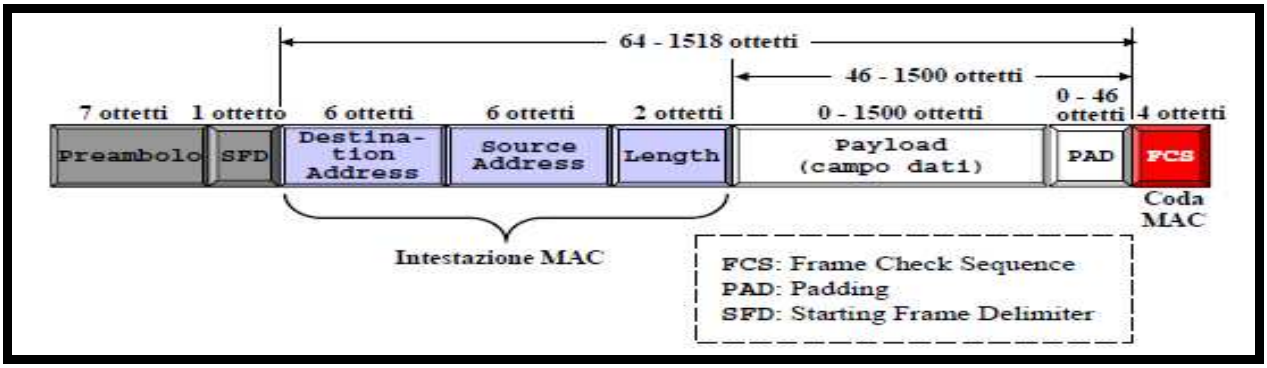
Nel transitare dal livello di applicazione a quello fisico l'informazione da trasmettere (messaggio) modifica il suo formato, dato che gli si aggiunge un'intestazione, e quindi le denominazioni cambiano seguendo i livelli.

- 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



Formato delle trame Ethernet a livello fisico

Il *formato del pacchetto* prevede otto campi, di seguito elencati:



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 SFD**. 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 o Length**. 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 Payload**. È costituito da una lunghezza che va da 0 a 1500 byte.
7. **Campo riempitivo PAD**. 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 FCS**. 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.

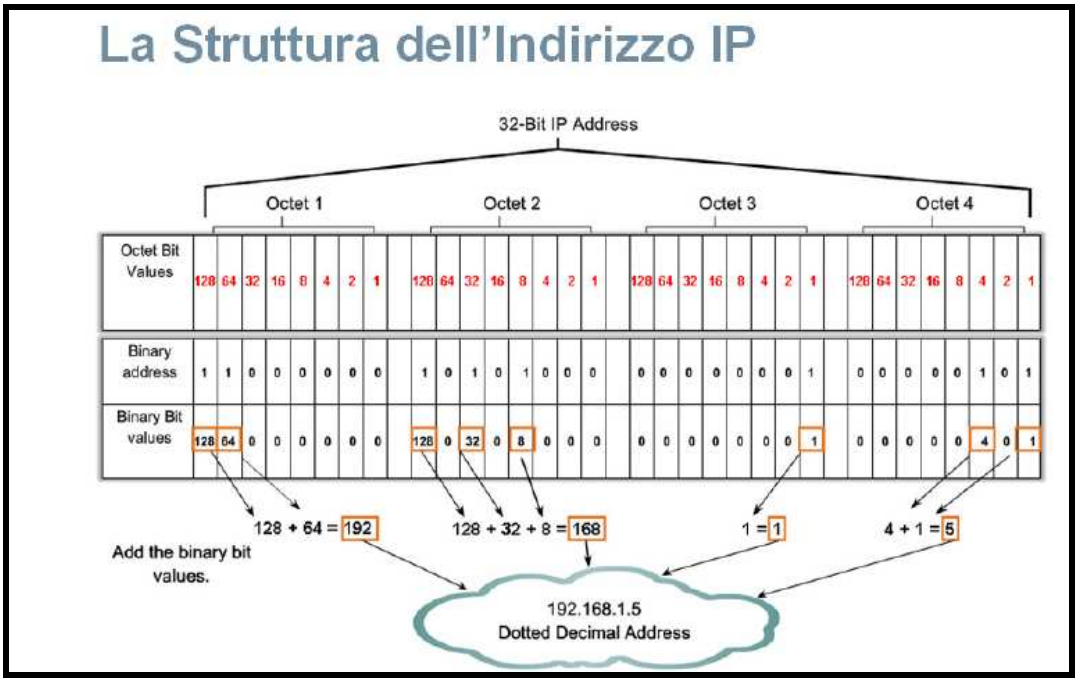
Assegnazione degli IP

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.
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)

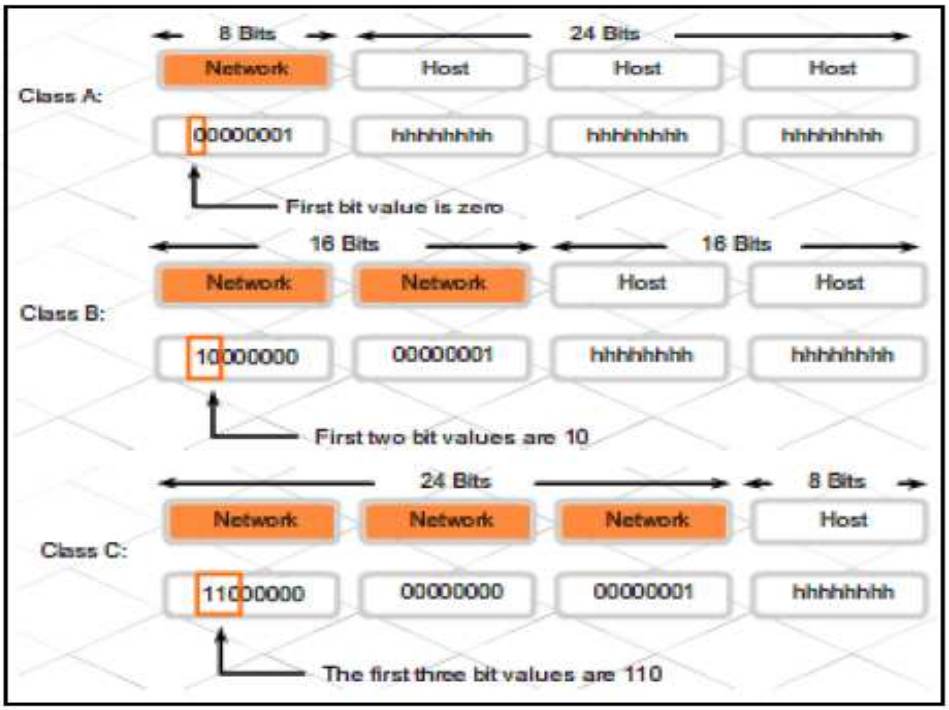
Per poter inviare e ricevere messaggi su una rete IP ogni host di rete deve possedere un unico indirizzo IP a 32 bit fornito in "**notazione decimale puntata**" (dotted-decimal notation). In questo formato, ognuno dei quattro ottetti (quattro gruppi di otto bit) viene convertito in un numero decimale separato da un punto. Esempio:

Notazione Binaria	Notazione Decimale puntata
11000000.10101000.00000001.01101010	192.168.1.106



Per creare un maggior numero di reti, lo spazio di indirizzamento a 32-bit è stato organizzato in cinque classi. Tre di queste classi, A, B e C, forniscono indirizzi che possono essere assegnati ai singoli host o alle reti. Le altre due classi, D ed E, sono stati riservati per il multicast e per uso sperimentale. La classe di una rete è indicata dal valore dei primi bit dell'indirizzo IP.

- Se il primo bit è 0, la rete è di classe A, e i primi 8 bit, o primo ottetto, rappresenta l'ID di rete.
- Se i primi due bit sono 10, la rete è di classe B, e i primi 16 bit rappresentano l'ID di rete.
- Se i primi tre bit sono 110, la rete è di classe C e i primi 24 bit rappresentano l'ID di rete.



Gli indirizzi unicast, broadcast e multicast

Gli indirizzi IP sono anche categorizzati in**: unicast** (per messaggi uno a uno), broadcast (**uno a tutti**) e multicast (uno a molti). Gli indirizzi unicast sono i più comuni, usati sempre come sorgente di un messaggio, e come destinazione se essa è uno specifico host (ad es. il Client 192.168.1.5 chiede una pagina al WebServer 192.168.1.200; il pacchetto con la richiesta viene incapsulato in una trama con gli indirizzi MAC della sorgente e della destinazione: IP e MAC collaborano per la consegna dei messaggi).

Destination MAC	Source MAC	Destination IP	Source IP	User data	FCS
00-07-E9-42-AC-28	00-07-E9-63-CE-53	192.168.1.200	192.168.1.5	xxxx	yyyy
		|<----------	Pacchetto	----------\>|	
<----------		Trama Ethernet		----------\>	

Gli indirizzi **broadcast** contengono tutti i bit a “1” nel campo host, ed i relativi pacchetti sono letti ed interpretati da tutti gli host della rete. Molti protocolli, come ARP e DHCP, li usano.
Gli indirizzi broadcast di Classe C hanno l’ultimo byte = 255 (1111 1111), ad es. 192.168.1.255. Quelli di Classe B hanno 255 negli ultimi due bytes (172.16.255.255), mentre quelli di Classe A hanno 255 negli ultimi tre (10.255.255.255), che sono sempre i campi host delle rispettive Classi. Un Pacchetto broadcast viene incapsulato in una trama con indirizzo MAC broadcast, con 48 “1”.

Destination MAC	Source MAC	Destination IP	Source IP	User data	FCS
FF-FF-FF-FF-FF-FF	00-07-E9-63-CE-53	192.168.1.255	192.168.1.5	xxxx	yyyy

Gli **indirizzi multicast** (da 224.0.0.0 a 239.255.255.255) permettono ad un mittente di inviare messaggi ad un gruppo di host della sua rete, previamente configurati per riconoscerli. Questo può servire in caso di videoconferenze, giochi di gruppo in remoto, ecc.

I Pacchetti multicast vengono incapsulati in trame multicast. Di solito il MAC multicast è costituito da una prima metà (sezione OUI di 24 bit) data da 01-00-5E, mentre la seconda metà sono gli ultimi tre bytes dell'indirizzo IP (15.100.197 = 0F-64-C5).

Destination MAC	Source MAC	Destination IP	Source IP	User data	FCS
01-00-5E-0F-64-C5	00-07-E9-63-CE-53	224.15.100.197	192.168.1.5	xxxx	yyyy

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

Indirizzi IP privati

Oltre a creare classi separate, l' IETF (Internet Engineering Task Force) ha deciso di riservare una parte dello spazio di indirizzi Internet ad esclusivo utilizzo di reti private. Le reti private non hanno alcun collegamento alle reti pubbliche, infatti gli indirizzi di reti private non possono essere instradati su Internet. Questo permette a più reti ubicate in varie località di poter utilizzare lo stesso schema di indirizzamento privato, senza creare conflitti di indirizzi IP. L'utilizzo dello spazio di indirizzamento privato riduce enormemente il numero di indirizzi IP univoci registrati (gli IP pubblici per intendersi) da rendere disponibili alle organizzazioni che vogliono collegarsi ad Internet.

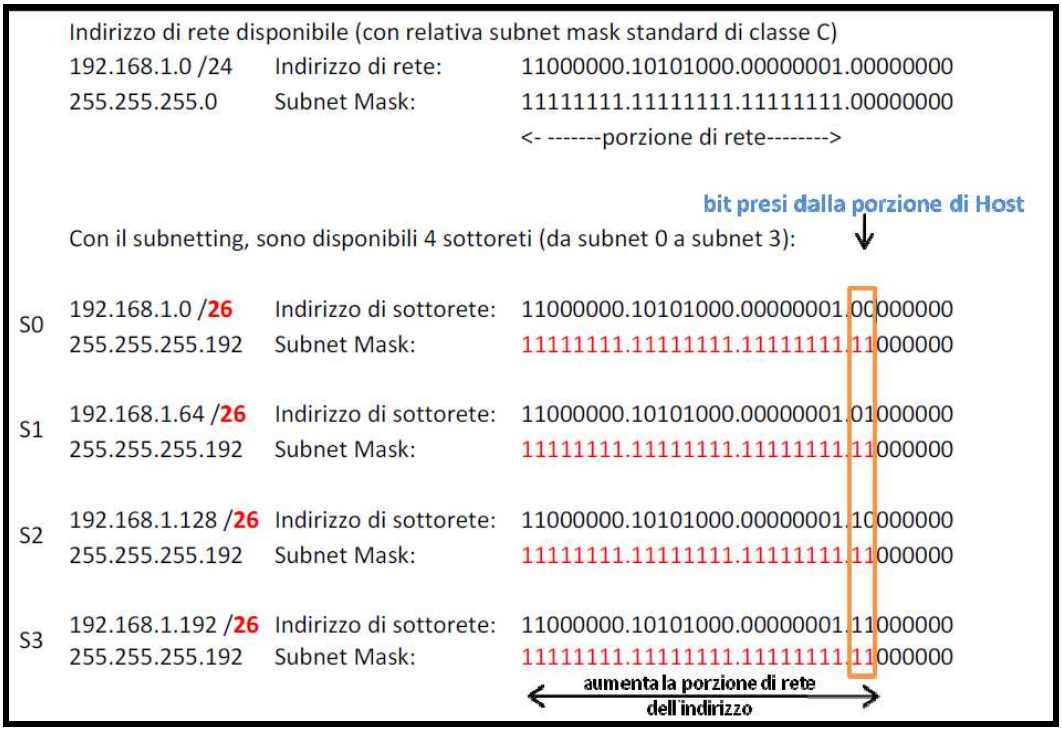
Class	Private IP Addresses (RFC 1918)	Default Subnet Mask	Number of Networks	Hosts per Network	Total Hosts
A	10.0.0.0 to 10.255.255.255	255.0.0.0	1	16,777,214	16,777,214
B	172.16.0.0 to 172.31.255.255	255.255.0.0	16	65,534	1,048,544
C	192.168.0.0 to 192.168.255.255	255.255.255.0	256	254	65,024

Maschere di sottorete personalizzate

Volendo realizzare due o più sottoreti di una stessa rete locale è necessario utilizzare maschere di sottorete personalizzate.
Una **subnet mask standard** e una **modificata** differiscono tra loro, in quanto quella standard cambia soltanto al confine dell'ottetto. In altre parole è composta solamente dai valori decimali 255 e 0, perché ogni ottetto è interamente composto o da tutti 1 o da tutti 0. Per esempio, la subnet mask

standard per una rete di classe A è 255.0.0.0. Le maschere di sottorete modificate prendono alcuni bit dalla porzione di host di in un indirizzo IP (con valore 0) trasformandoli in bit di rete (con valore 1), aumentando di fatto la quantità di 1 rispetto alla subnet mask standard della rispettiva classe. In altre parole, su uno solo degli ottetti si avrà un misto di 1 e 0 e il corrispettivo valore decimale non potrà più essere né 255, né 0.
Per esempio, se partiamo da un indirizzo di classe C, come il 192.168.1.0, ci sono soltanto otto bit della porzione di host che possiamo prendere in prestito per personalizzare la subnet mask. Ogni bit può essere soltanto 1 o 0. Supponendo di volere tre sottoreti, almeno due degli otto bit devono essere presi in prestito. Questo crea la possibilità di avere un totale di quattro sottoreti:

- 00 – prima sottorete
- 01 – seconda sottorete
- 10 – terza sottorete
- 11 – quarta sottorete



Nell'esempio, 2 bit sono stati presi in prestito ($2^2 = 4$), per cui sono state create quattro sottoreti. Se fossero state necessarie dalle cinque alle otto sottoreti, i bit da prendere in prestito dalla porzione host, sarebbero stati 3 ($2^3 = 8$). Il numero di bit scelti per identificare la maschera di sottorete influenza sia il numero di sottoreti possibili che il numero di host per ogni sottorete. All'aumentare del numero di reti, diminuisce il numero di host per ogni sottorete e viceversa.

In altre parole, 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 diventa: 255.255.255.19210 = $(11111111.11111111.11111111.11000000)_2$
Indirizzo della rete fisica: 192.168.1.0

Sottorete 0: da 192.168.1.0 a 192.168.1.63
Sottorete 1: da 192.168.1.64 a 192.168.1.127
Sottorete 2: da 192.168.1.128 a 192.168.1.191

Sottorete 3: da 192.168.1.192 a 192.168.1.255

Poiché ogni sottorete ha **due indirizzi di host che sono riservati**, quello con i bit di host tutti a 0 e quello con i bit di host tutti a 1 (rispettivamente indirizzo di rete e di broadcast), per determinare il numero di host disponibile in ogni sottorete si deve applicare la formula: $\mathbf{2^n - 2,}$ dove n è il numero di bit della porzione host. In definitiva, per l'esempio proposto, si sono realizzate 4 sottoreti ciascuna delle quali dispone di 62 indirizzi IP.

Esempio

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 = $(11111111.11111111.11111111.11100000)_2$
Indirizzo della rete fisica: 192.168.1.0

Sottorete 0: 192.168.1.0 - 192.168.1.31
Sottorete 1: 192.168.1.32 - 192.168.1.63
Sottorete 2: 192.168.1.64 - 192.168.1.95
Sottorete 3: 192.168.1.96 - 192.168.1.127
Sottorete 4: 192.168.1.128 - 192.168.1.159
Sottorete 5: 192.168.1.160 - 192.168.1.191
Sottorete 6: 192.168.1.192 - 192.168.1.223
Sottorete 7: 192.168.1.224 - 192.168.1.255

Ogni sottorete dispone di 5 bit di indirizzo di host ovvero di 2^5=32 indirizzi IP di cui solo 30 sono utilizzabili (si escludono il primo e l'ultimo).

Quando una rete è suddivisa in sottoreti, ogni sottorete è in realtà una rete completamente separata. Pertanto, se un dispositivo in una sottorete deve comunicare con un dispositivo su un'altra sottorete, è necessario un **router per interconnettere le due reti**.
Quando si determina il numero di host per ogni sottorete, è necessario includere l'interfaccia del router, o gateway, e i singoli dispositivi host. Ogni interfaccia del router deve avere un indirizzo IP nella stessa sottorete degli host a cui è collegata.

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).

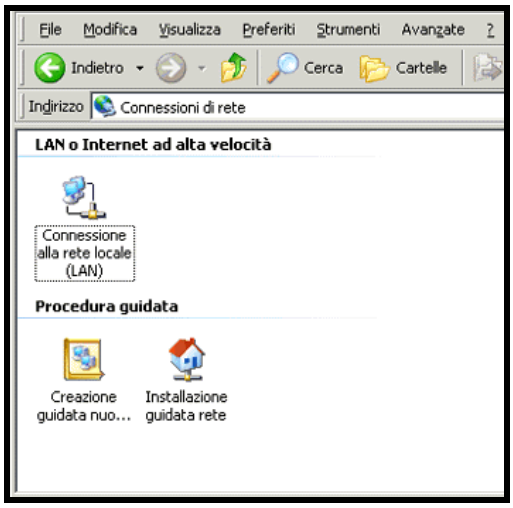
Protocolli per la risoluzione degli indirizzi

Il **protocollo ARP** (Address Resolution Protocol) 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.

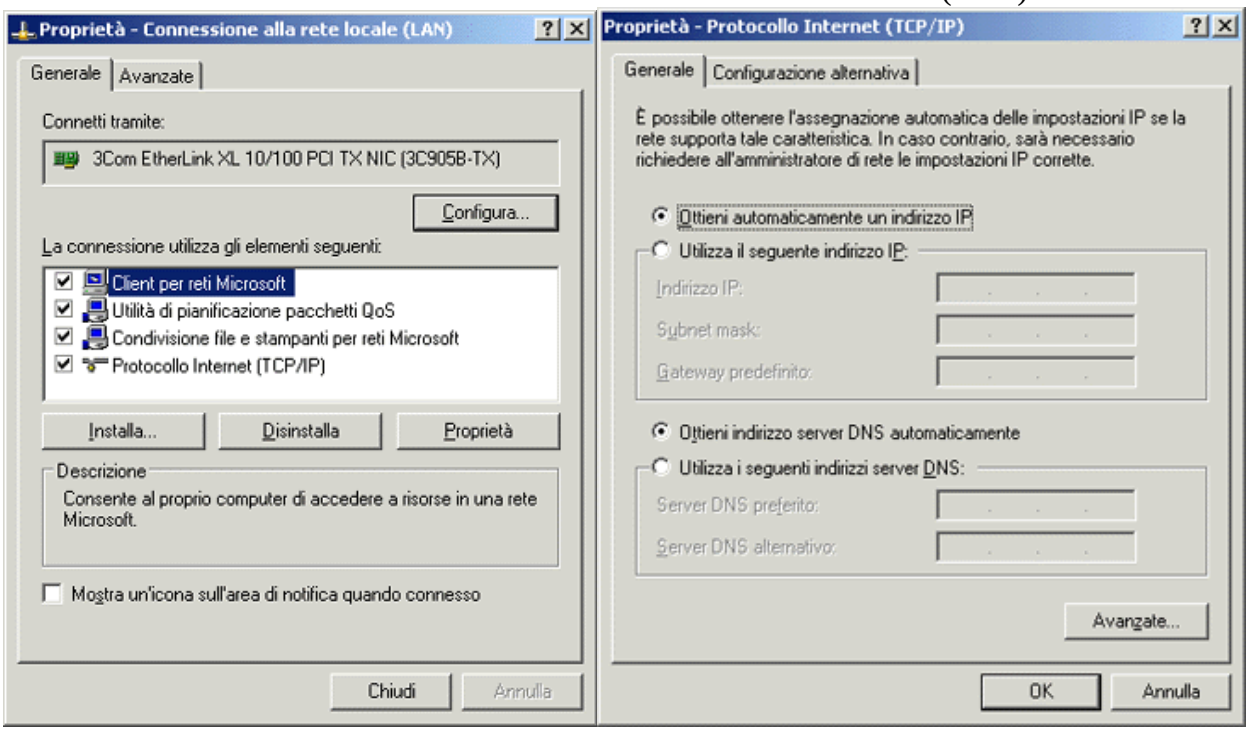
LAN con Router

Configurazione dei PC

Una volta installata correttamente la scheda di rete dovrebbe comparire nel desktop una nuova icona (Risorse di rete).



Click con il tasto destro del mouse sull'icona "Connessione alla rete locale (LAN)" si ha:

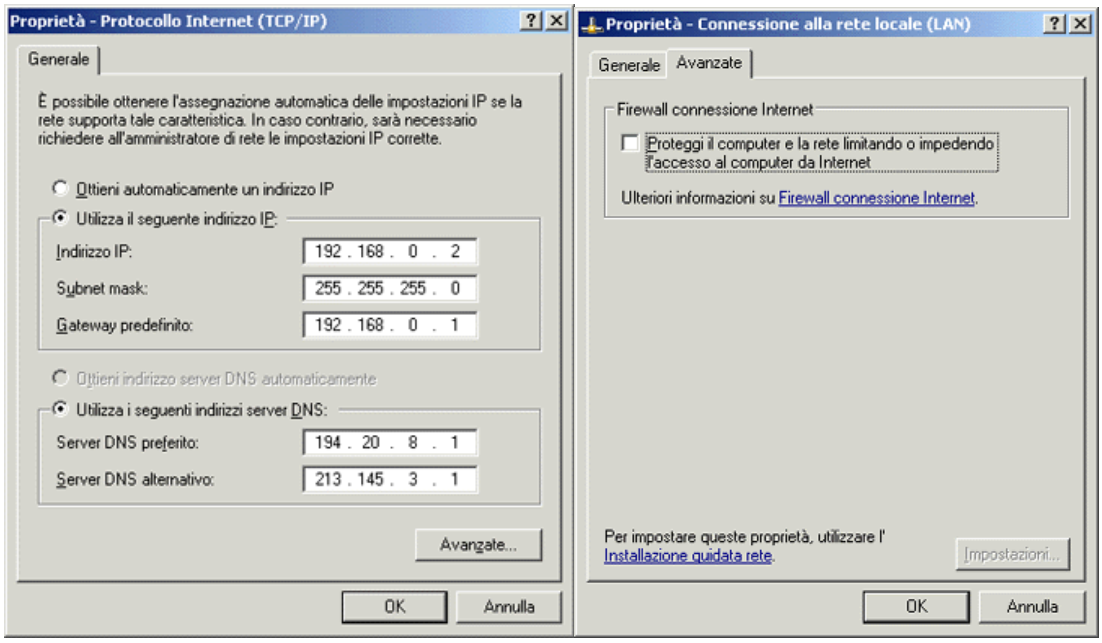


Click sulla voce "Protocollo Internet (TCP/IP)" e poi sul pulsante Proprietà. Comparirà una schermata come la precedente a destra.

Click sulla voce "Utilizza il seguente indirizzo IP" e configuriamo le prime voci. Ad esempio:

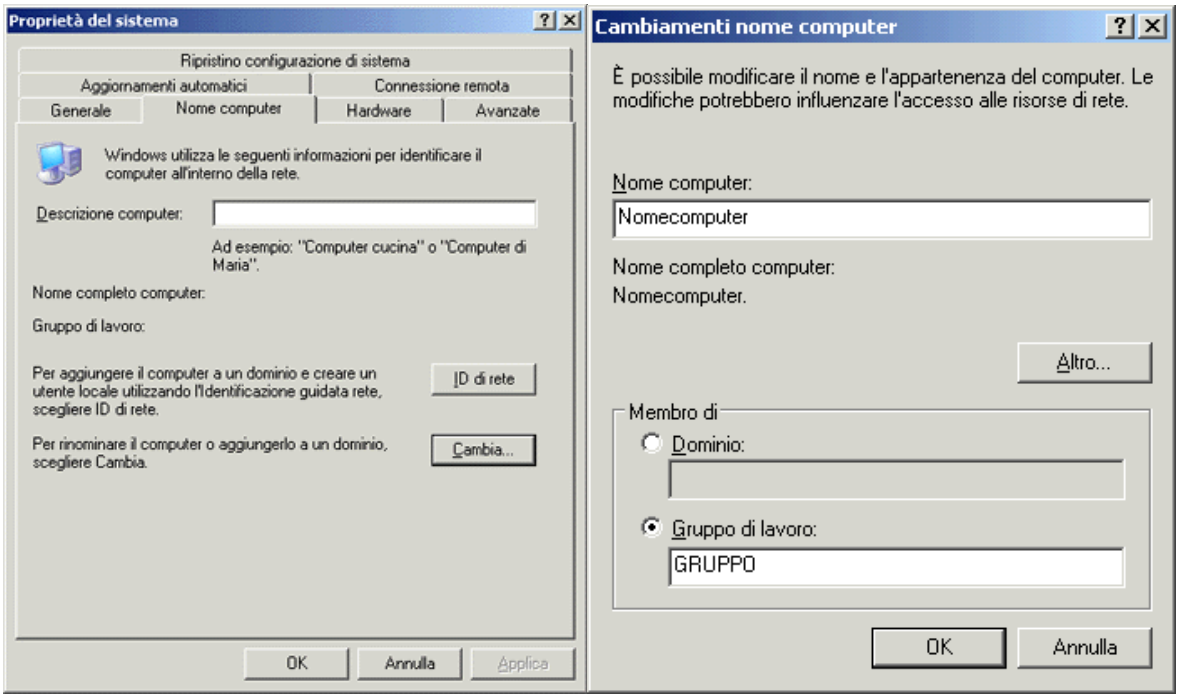
Come indirizzo IP si pone 192.168.0.2. Si è posto questo indirizzo perché la rete 192.168.x.x è privata e si pone come ultimo numero 2 perché spesso i Router ADSL hanno con l'indirizzo 192.168.0.1 (controllare nel manuale del Router).

Inserire il numero 255.255.255.0 nella voce Subnet Mask (questo permette di avere 254 numeri da poter usare per i nostri PC collegati).
Inseriamo l'indirizzo 192.168.0.1 nella casella **Gateway predefinito**.
Il Gateway è l'indirizzo IP con cui i PC usciranno su Internet (quindi l'indirizzo IP del router).
Nell'area di configurazione dei DNS si devono inserire gli IP dei DNS (Primario e secondario) del Provider (anche se possiamo inserire i numeri IP dei DNS di qualsiasi Provider). Si ha:



Click sul bottone OK e ritornare alla schermata principale delle proprietà di rete.
Click su "Avanzate" comparirà la schermata precedente a destra.
L'opzione ci consente di attivare/disattivare la funzione "Proteggi il computer e la rete limitando o impedendo l'accesso al computer da Internet". Questa funzione è indispensabile per chi si collega via modem, ma quasi inutile se il collegamento avviene tramite router, in quanto lo stesso ha già incorporati dei filtri che impediscono le intrusioni da Internet verso il PC.

Si deve impostare il nome da dare al PC (nome con cui verrà visto nella rete locale) ed il gruppo di lavoro.
Click con il tasto destro del mouse sull'icona "Risorse del computer" e quindi sulla voce "Proprietà". Click sulla voce "Nome computer" e successivamente su “Cambia”, si ha:

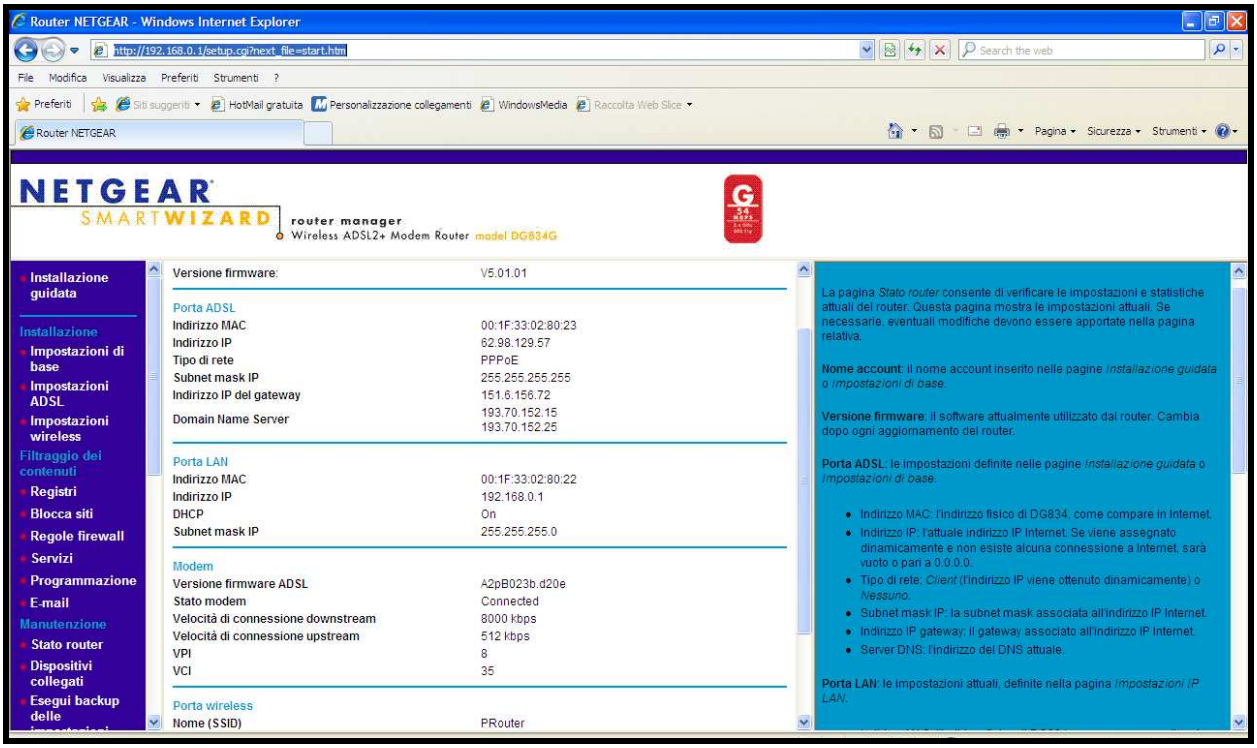


Nella voce "Descrizione computer" (facoltativa) si può inserire una descrizione del PC.
Il nome del gruppo di lavoro che deve essere uguale per tutti i PC collegati alla rete locale.
Una volta effettuata la configurazione di tutti i PC la rete dovrebbe cominciare a funzionare.

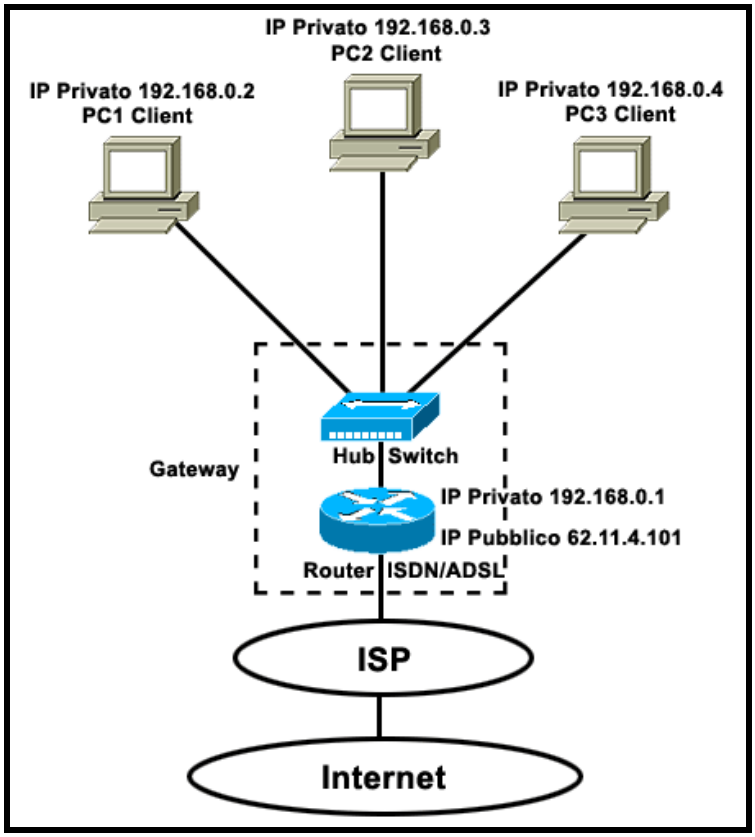
Impostazioni del Router

Si devono seguire le istruzioni e le procedure fornite dal costruttore. Normalmente si collega il PC al router con cavo RJ45 e si accede mediante indirizzo IP del tipo: **http://192.168.0.1** e si accede alla configurazione del dispositivo inserendo nome e password. La credenziali del produttore hardware sono standard: spesso **admin** come username e password come **password.**

Si ottiene una schermata del tipo.



Per configurare la propria connessione ADSL e le impostazioni fondamentali del router, è possibile servirsi del "wizard" che guida l'utente passo-passo. Le impostazioni per la connessione Internet sono visionabili cliccando sulla voce **Impostazioni di base**. Qui vanno inseriti i dati forniti dal provider con cui si è stipulato il contratto di abbonamento al servizio ADSL. Il primo dato da fornire riguarda il tipo di incapsulamento dei dati: PPPoA (Point to Point Protocol Over ATM), IPoA (IP Over ATM) e PPPoE (Point to Point Protocol Over Ethernet) sono quelli più utilizzati. Dal punto di vista prestazionale i protocolli PPPoA (RFC 2364) e PPPoE (RFC 2516) sono praticamente identici (in PPPoE si usano 8 byte in più di intestazione e si usa un livello di incapsulamento in più: il pacchetto Ethernet viene incapsulato nella trama PPP quindi in quella ATM): PPPoA è solo leggermente più efficiente. Oggi praticamente tutti gli apparati dei gestori telefonici sono configurati in modalità "autosense" così da riconoscere automaticamente il metodo di incapsulamento impostato dall'utente sul suo modem/router.
Per fare in modo che gli altri sistemi della rete locale possano accedere ad Internet tramite il router è indispensabile verificare di aver **attivato la funzione NAT**. I nodi ATM smistano il traffico sulla rete in base ad una coppia di parametri detti VPI/VCI (Virtual Path/Circuit Identifier) della cella e della porta d'ingresso. Quando configuriamo il router è necessario inserire il parametro VPI/VCI assegnato dal provider. In Italia VPI è sempre 8 mentre VCI 35. L'indirizzo IP assegnato al router e, di conseguenza, quelli assegnati agli host della LAN, possono essere liberamente modificati portandosi all'interno del menù Impostazione IP della LAN.
Cliccando sulla voce **Stato del router** si possono ottenere tutta una serie di utili informazioni sulla configurazione del dispositivo, sulla connessione ADSL, sui parametri della linea. In particolare, vengono restituiti indirizzo IP del server gateway del provider, l'indirizzo MAC del router, il suo indirizzo IP, i server DNS di riferimento.
E' necessario connettere il router alla presa telefonica tramite il cavo RJ-11.
Esempio



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.