

CAPITOLO 3

Livelli, protocolli e indirizzi IP

3.1 Livelli di rete: modello OSI

Tutto il sistema hardware e software che ruota attorno al mondo delle reti è regolato da norme ben precise che fanno riferimento al modello OSI (Open Systems Interconnection), introdotto nel 1984 dall'International Standard Organization (ISO). Questo modello fornisce uno standard per le interconnessioni in rete dei vari PC. Alla base del modello vi è una suddivisione delle funzioni che un sistema di rete dovrebbe svolgere affinché il processo di trasmissione dei dati venga portato a termine. Questa suddivisione comprende 7 livelli (layers).



Fig. 3.1.1 Modello OSI dei livelli di rete

3.1.1 Livello fisico

Il livello *fisico* si occupa della trasmissione dei singoli bit da un estremo all'altro dei vari mezzi di comunicazione che possono essere il doppino telefonico, il cavo coassiale, le fibre ottiche, le onde radio, i satelliti. Perché si possa avere una connessione tra PC è necessario dunque, ma non

indispensabile, un supporto fisico, composto solitamente da un cavo e da interfacce di comunicazione. La connessione tipica di una rete locale utilizza sistemi Ethernet. I cavi e le schede Ethernet appartengono a questo primo livello. Protocollo standard è il protocollo Ethernet.

3.1.2 Livello collegamento dati

Il livello del *collegamento dati* riguarda i dispositivi che gestiscono il collegamento dati da un PC all'altro della stessa rete. Controlla la correttezza delle sequenze di bit trasmesse e ne richiede eventualmente la ritrasmissione. Provvede alla formattazione delle informazioni ed alla sincronizzazione dei frame, nonché alla correzione ed al recupero dei messaggi errati. Un frame contiene, a livello di collegamento dati, l'indirizzo di destinazione e, se richiesto da un livello superiore, anche l'indirizzo di origine, e un codice per la correzione e rilevazione degli errori.

3.1.3 Livello rete

Nel livello di *rete* i messaggi vengono suddivisi in pacchetti che, una volta giunti a destinazione, vengono riassemblati nella loro forma originaria. Il livello di rete provvede inoltre a reinstradare tramite i router i pacchetti verso il PC di destinazione. Nel caso di una rete locale a banda larga con canali multipli ciò significa che è a questo livello che avviene lo smistamento dei pacchetti dati da e verso i rispettivi canali di origine o di destinazione. Il protocollo di rete più utilizzato nel livello 3 è il protocollo IP.

3.1.4 Livello trasporto

Il livello di *trasporto* gestisce la trasmissione dei pacchetti end-to-end. Ha il compito specifico di assicurare il trasferimento dei dati tra strati di sessione appartenenti a sistemi diversi, geograficamente separati, senza che sui dati vi siano errori o duplicazione. È in grado di identificare il destinatario, aprire o chiudere un connessione con il sistema corrispondente, suddividere o riassemblare un testo, controllare e recuperare gli errori, controllare la velocità con cui fluiscono le informazioni.

A questo livello l'esistenza dei livelli inferiori è completamente ignorata e ciò porta ad identificarlo come il primo dei livelli che prescindono dal tipo e dalle caratteristiche della rete utilizzata. Il protocollo standard utilizzato nel livello 4 è il TCP. Talvolta viene usato anche il protocollo UDP.

3.1.5 Livello sessione

Il livello di *sessione* gestisce la corretta sincronizzazione della corrispondenza dei dati che verranno poi visualizzati. Instaura cioè una sessione, cioè un collegamento logico e diretto tra due interlocutori, organizzandone il dialogo. Per tipo di dialogo si intende la modalità full-duplex, ovvero in entrambe le applicazioni in trasmissione e ricezione contemporaneamente (tipo telefono), o in half-duplex, che equivale a dire che mentre una stazione trasmette l'altra riceve o viceversa (tipo radiotelefono), oppure in simplex, dove una stazione può sempre e solo trasmettere e l'altra sempre e solo ricevere (come nelle trasmissioni televisive). Per sincronizzazione si intende invece la capacità di sapere sempre fino a che punto la comunicazione sia arrivata a buon fine.

3.1.6 Livello presentazione

Il livello di *presentazione* gestisce i formati di conversione dei dati, cioè effettua tutte le opportune conversioni in modo da compensare eventuali differenze di rappresentazione e di formato dei dati in arrivo e/o in partenza. Macchine diverse possono avere infatti rappresentazioni diverse. Ha anche il compito di assicurare l'opportuna compressione e/o la necessaria crittografia dei dati da scambiare.

3.1.7 Livello applicazione

Il livello di *applicazione* riguarda i cosiddetti programmi applicativi. Questo livello gestisce la visualizzazione dei dati: login remoto, file transfer, posta elettronica. Per la gestione dei PC, il problema si presenta quando due sistemi che vogliono comunicare possiedono video o tastiere diverse, e quindi non compatibili. Ad esempio, per spostare il cursore ad inizio linea o per cancellare lo schermo, ogni scheda ha i suoi comandi specifici: invece di dotare tutti i sistemi di opportuni traduttori per tutti i possibili interlocutori è evidentemente molto più semplice definire uno standard unico di un PC virtuale a cui tutti i corrispondenti dovranno adeguarsi per comunicare.

3.2 Protocolli di rete

I computer connessi ad una LAN riescono a dialogare tra loro grazie ad un protocollo di comunicazione, che riesce a gestire i flussi di dati e di informazioni dagli host verso la rete e viceversa. I protocolli utilizzati nelle reti LAN e in Internet appartengono tutti alla famiglia TCP/IP. Tale gruppo di protocolli, come si capisce dalla sigla è diviso in due livelli: TCP e IP.

Approfondimento:

Quando si trasmettono dati via Internet, la procedura di spedizione passa sempre attraverso i 7 livelli OSI appena visti. Questi livelli sono governati dalle regole dei "protocolli" che gestiscono anche il rapporto con i livelli vicini. Ogni livello rielabora il messaggio iniziale aggiungendo un header contenente informazioni per il livello successivo del ricevente

Il TCP/IP è definito protocollo a "commutazione di pacchetto", per il fatto che i dati da trasmettere vengono suddivisi in pacchetti, ognuno dei quali contiene una porzione di dati, l'indirizzo del mittente e quello del destinatario. La gestione dell'instradamento dei pacchetti è controllata dal TCP, che si occupa, inoltre, di spezzettare i dati da inviare, di controllare che tutti i pacchetti arrivino a destinazione, di riassemblare i pacchetti arrivati, ed eventualmente il TCP può anche richiedere i pacchetti che siano andati persi durante il trasporto a causa di problemi sulla rete.

La parte IP del protocollo si occupa principalmente della definizione del percorso, affinché un pacchetto arrivi a destinazione. L'IP, però non si controlla che i pacchetti arrivino a destinazione (compito del TCP, come dicevamo), e non garantisce che i pacchetti arrivino a destinazione in ordine: essi vengono spediti in ordine ma durante il trasporto le strade scelte possono essere diverse a causa di "blocchi" trovati sulla rete, motivo per cui l'ordine di arrivo non è noto.

I numerosi protocolli che compongono la suite TCP/IP prendiamo in considerazione i cinque fondamentali: HTTP, POP3, SMTP, NNTP, FTP.

I protocolli di rete sono divisi in tre categorie principali: protocolli di trasporto, protocolli applicativi e protocolli per sessioni remote, che si occupano dell'interazione tra PC di una rete, in diversi ambiti. Vediamoli nel dettaglio per non perderci tra le varie sigle che spesso si presentano parlando di LAN.

3.2.1 Protocolli di trasporto

IP - Internet Protocol

Responsabile del trasporto di pacchetti di dati da una sorgente (identificata da un indirizzo IP) ad una destinazione (identificata da un altro indirizzo IP). Se necessario questo livello del protocollo si occupa di spezzettare i pacchetti troppo grandi in pacchetti di dimensione adatta alla rete da utilizzare.

ICMP - Internet Control Message Protocol

Partner di IP con la funzione specifica di inviare, anziché dati, messaggi di controllo e diagnostici (ad esempio pacchetti ECHO).

UDP - User Datagram Protocol

Questo protocollo si trova ad un livello superiore rispetto ad IP, ed aggiunge alla semplice funzionalità di trasporto di IP la possibilità di "smistare" i pacchetti nella macchina di destinazione sulla base di un numero di porta aggiunto all'indirizzo. Viene controllata l'integrità dei dati attraverso una checksum, ma i pacchetti corrotti vengono semplicemente buttati via.

TCP - Transmission Control Protocol

Questo è il protocollo di livello superiore ad IP che viene utilizzato più di frequente. La sua caratteristica è quella di stabilire una connessione fra due applicazioni identificate, come in UDP, da un numero di porta, e di garantire la trasmissione senza errori di un flusso di dati. Se vengono ricevuti pacchetti corrotti, il protocollo richiede la ritrasmissione dei dati a partire dal primo

pacchetto corrotto identificato. TCP implementa anche un timeout per la chiusura delle connessioni interrotte o non stabilite.

PPP - Point to Point Protocol

Permette di trasferire traffico IP su una linea seriale. Creato in particolare per gestire i collegamenti transitori via modem, comprende meccanismi di auto-configurazione delle estremità del collegamento e di autenticazione.

3.2.2 Protocolli Applicativi

FTP - File Transfer Protocol

Anche questo fra i primissimi protocolli applicativi ad essere sviluppati. Consente di trasferire file fra macchine di architettura diversa. I file vengono trattati come file di testo (7 bit per carattere) oppure come file binari (8 bit per carattere). Non viene modificato o "tradotto" il contenuto dei file.

HTTP - HyperText Transfer Protocol

E' il protocollo che interconnette quella vastissima collezione di siti Internet generalmente nota come World Wide Web (WWW). Non ha molta funzionalità in più rispetto a FTP: permette in più

di richiedere l'esecuzione di procedure via rete. E' però forse oggi il protocollo di alto livello di IP più utilizzato in assoluto, perché viene utilizzato per veicolare i documenti codificati in HTML (HyperText Markup Language). E' la funzionalità di questo linguaggio, unita all'interfaccia grafica fornita dai browser, la vera ragione della praticità d'uso, e quindi del successo di WWW. **SMTP** –

Simple Mail Transfer Protocol E' il protocollo utilizzato per trasferire (fra host che "parlano" TCP/IP) i messaggi di posta elettronica.

POP - Post Office Protocol

Protocollo utilizzato per recuperare i messaggi di posta elettronica conservati su un host remoto. Nato per permettere l'accesso ai servizi di posta alle macchine non collegate direttamente ad Internet, viene recentemente sempre più spesso utilizzato anche su LAN a causa dei problemi legati alla configurazione di un server di posta "sicuro".

IMAP - Internet Message Access Protocol

Protocollo speculare rispetto a POP: permette di esaminare una casella remota di posta elettronica senza trasferire i messaggi. L'uso e la sua ragione d'essere sono sostanzialmente gli stessi di POP.

3.2.3 Protocolli per sessioni remote

TELNET

Protocollo basato su TCP (e quindi su IP), finalizzato alla creazione di una sessione interattiva su una macchina remota, del tutto simile ad una normale sessione di lavoro su un terminale collegato direttamente alla macchina remota stessa. E' stato il primo protocollo "applicativo" sviluppato nella suite di IP, ed era come l'obiettivo principale dell'intero progetto di sviluppo di IP. Viene tuttora utilizzato per ottenere sessioni remote laddove non vi sia alcuna preoccupazione riguardo alla sicurezza informatica (il protocollo non prevede infatti alcuna protezione o crittazione dei dati).

SSH - Secure Shell Versione sicura (mediante crittografia a chiave pubblica) di un precedente protocollo (rsh) che garantiva l'esecuzione di qualsiasi comando su una macchina remota. Può essere considerato come una estensione di telnet, che rappresenta il caso particolare nel quale alla macchina remota viene richiesto di eseguire un interprete di comandi. E' l'alternativa di telnet oggi raccomandata e decisamente preferibile per tutelare la sicurezza delle informazioni di login.

3.3 Indirizzamento IP

Tutti i computer connessi ad una rete devono disporre di un indirizzo, che permetta di identificare l'host in maniera univoca ed efficiente. Gli indirizzi nelle reti sono definiti per mezzo di alcune serie numeriche chiamate appunto "indirizzi IP". Un indirizzo IP è composto da quattro serie numeriche, ognuna delle quali è composta da un massimo di tre cifre, ed è compresa tra 0 e 255. Un esempio di IP potrebbe essere: 192.168.0.255.

Fig. 3.3.1 L'indirizzo IP identifica in modo univoco un host nella LAN o in Internet. Gli indirizzi privati, cioè quelli utilizzati nelle reti locali, sono assegnati dal gestore, quindi attenzione agli IP duplicati!

Per essere certi che l'identificazione sia univoca, è necessario che non esistano numeri IP uguali, per tale motivo esistono due tipi di indirizzi IP: quelli pubblici e quelli privati. Gli indirizzi privati sono assegnati ai vari host dal gestore della LAN, che deve accertarsi di non assegnare IP uguali a due PC della stessa rete. Gli indirizzi pubblici sono assegnati dal provider Internet (Internet Service Provider), in modo automatico e senza possibilità che due computer in Internet abbiano lo stesso indirizzo. Gli indirizzi IP, inoltre, possono essere sia statici che dinamici. Quelli statici, che troviamo nelle reti locali, vengono assegnati una sola volta e non cambiano ad ogni utilizzo della LAN. Gli indirizzi pubblici, invece, sono quasi sempre di tipo dinamico: ad ogni connessione il provider assegna un nuovo indirizzo al computer. In alcune situazioni particolari, gli ISP assegnano indirizzi statici, che restano quindi immutati ad ogni connessione, ma questo tipo di servizio è di solito a pagamento.

Un computer necessita di un indirizzo IP pubblico statico nel caso in cui si debba offrire un servizio Internet, come ad esempio un una macchina su cui è installato un Server Web.

Gli indirizzi IP privati sono in genere configurati dall'amministratore di rete (ossia colui che gestisce la rete) in modalità statica. In pratica, vengono assegnati manualmente e definitivamente secondo regole standard. Gli indirizzi IP privati sono dinamici se assegnati in modo automatico tramite un particolare software (Server DHCP). Essi cambiano tutte le volte che si accende il computer.

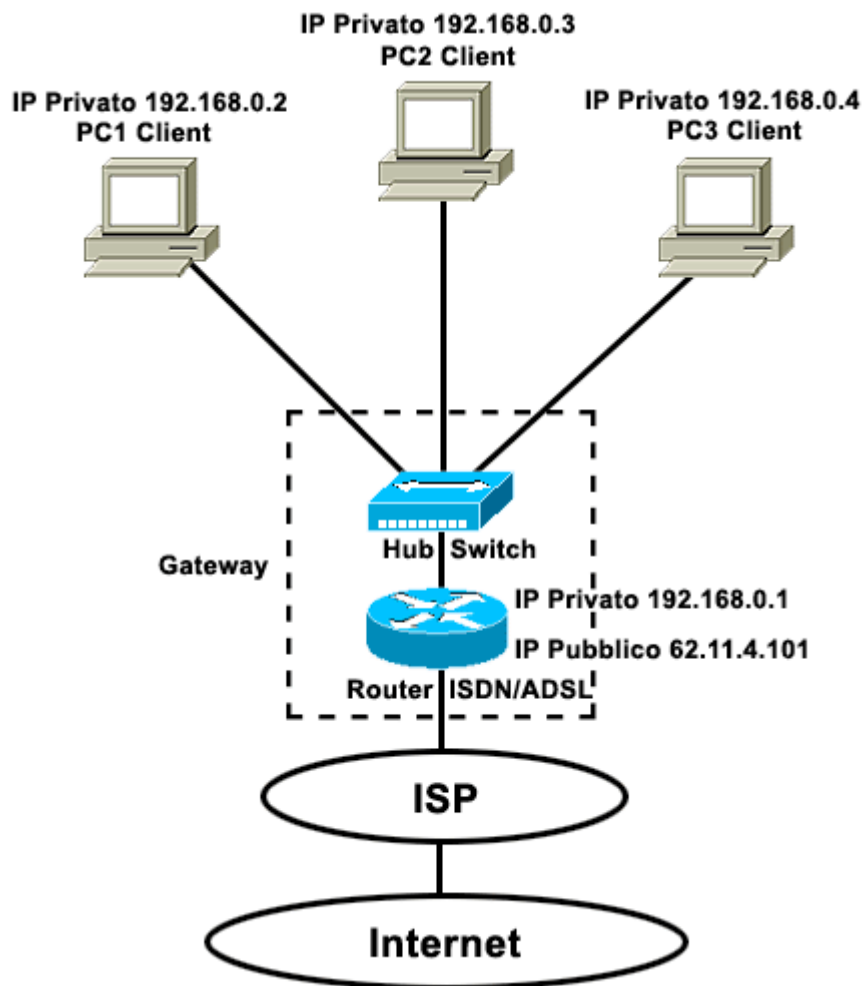


Fig. 3.3.2 Gli indirizzi statici sono utilizzati all'interno della rete locale, mentre per le connessioni ad Internet l'ISP assegna IP variabili ad ogni connessione

Tips nel testo:

Su una macchina con piattaforma Windows per conoscere l'indirizzo IP è sufficiente digitare dal prompt di MS-DOS il comando `ipconfig`. In alternativa è possibile affidarsi a programmi ad interfaccia grafica che potrai trovare in rete, sempre nei siti dedicati al networking

Gli indirizzi IP, come già menzionato, identificano un computer della rete in modo univoco. Per la verità identificano un'interfaccia di rete, quindi un host con più interfacce possiede più indirizzi IP. Allo stesso tempo, però, l'indirizzo IP indica anche la rete a cui appartiene l'host. Tali informazioni sono indispensabili per i dispositivi che effettuano le operazioni di routing, cioè di instradamento dei pacchetti nella rete. Come già accennato, l'indirizzo IP è composto da quattro serie numeriche aventi al massimo 3 cifre, ciascuna delle quali è compresa tra 0 e 255, ad esempio: 192.234.24.98. Quest'ultimo numero identifica l'indirizzo IP di un host ed è espresso in forma decimale. Ma come sappiamo, i calcolatori interpretano il sistema numerico binario (1 e 0). Infatti l'indirizzo IP è composto da 32 bit o 4 byte di otto bit ciascuno (192.234.24.98. = 11000000.11101010.00011000.01100010). Il sistema numerico decimale è utilizzato semplicemente per facilitare la gestione degli indirizzi da parte degli amministratori di rete. L'indirizzo IP è suddiviso in due campi: uno identifica la rete; l'altro l'host. Tale suddivisione ha portato alla classificazione degli indirizzi in tre classi principali (A, B, C), le quali si differenziano in funzione di quanti dei quattro bytes identificano la rete e quanti l'host.

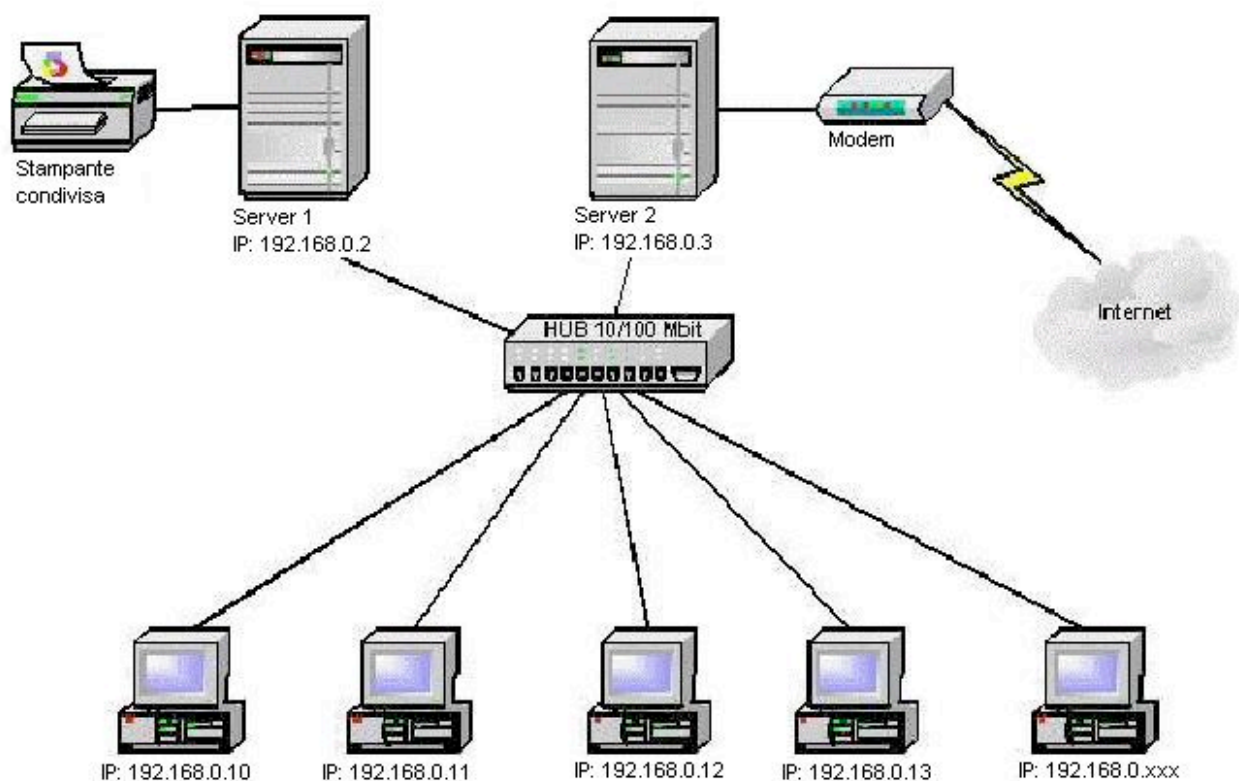


Fig. 3.3.3 Ecco un esempio di utilizzo degli indirizzi IP in una rete LAN di dimensioni ridotte

Vediamo adesso un breve schema riepilogativo. Classe A: è rappresentata dagli indirizzi IP che vanno da 1.0.0.0 a 127.255.255.255. Il primo byte identifica la rete, mentre i tre bytes successivi identificano l'host. In questo modo si possono ottenere 127 reti costituite ciascuna da 16.777.216 host. Tantissimi? In verità no, vista la crescita esponenziale di Internet.

Classe B: è rappresentata dagli indirizzi IP che vanno da 128.0.0.0 a 191.255.255.255. In questo caso, la rete è identificata nei primi due byte, mentre i due successivi fanno riferimento agli host per un totale di 16.384 reti composte da 65.536 host.

Classe C: utilizzata per le reti più piccole, è composta dagli indirizzi che vanno da 192.0.0.0 a 223.255.255.255. In questo caso, l'host è identificato solo dall'ultimo byte mentre i primi tre rappresentano la rete. Pertanto, è possibile gestire 2.097.152 reti composte da 256 host.

Classi D ed E: utilizzate per scopi particolari. Gli indirizzi di classe D non identificano nè la rete nè l'host, bensì un indirizzo multicast: sono quindi utilizzati per le trasmissioni in multicast, dove un solo host trasmette e tutti gli altri ricevono. Gli indirizzi di classe E sono invece destinati ad un utilizzo futuro.

Le reti di classe A, B e C possono essere suddivise in sottoreti. Tale operazione, denominata Subnetting, viene effettuata sia per facilitare le operazioni routing e di gestione degli indirizzi che per evitare sprechi nell'utilizzo degli indirizzi (che, come già detto precedentemente, sono una risorsa limitata con i sistemi di indirizzamento attuale, ovvero gli IPV4). La suddivisione di una rete in due o più sottoreti si esegue attraverso la netmask, che stabilisce quali indirizzi IP possono essere usati nelle sottoreti. Per la classe A, la subnet mask deve essere impostata a 255.0.0.0. Per la classe B, deve essere settata a 255.255.0.0. Per la classe C, che è la classe che sicuramente ci interessa di più, la subnet deve essere impostata a 255.255.255.0. Quindi, se gli indirizzi disponibili vanno da

192.0.0.0 a 223.255.255.255 e la nostra rete di classe C possiede, ad esempio, un indirizzo IP 192.234.24.0, la maschera di sottorete deve essere impostata a 255.255.255.192. Per quanto riguarda le due sottoreti, alla prima può essere assegnato come gateway l'indirizzo IP 192.234.24.0 (e alle macchine che la compongono gli indirizzi dal 192.234.24.1 al 192.234.24.126) mentre alla seconda può essere assegnato come gateway l'indirizzo IP 192.234.24.128 (e alle macchine che la costituiscono gli indirizzi dal 192.234.24.129 al 192.234.24.254). In questo modo, nonostante si possieda un solo indirizzo IP che identifica una rete composta al massimo da 256 host, è possibile creare virtualmente altre due reti. Una piccola precisazione: all'interno di una rete locale connessa a Internet si può assegnare tranquillamente un determinato range di indirizzi IP privati che non vengono messi a disposizione dagli ISP al momento della connessione. Tali indirizzi vanno dal 10.0.0.0 al 10.254.254.254, dal 172.16.0.0 al 172.31.254.254 e dal 192.168.0.0 al 192.168.254.254. Quest'ultimo range è il più utilizzato nelle LAN e lo ritroveremo spesso nelle trattazioni pratiche della sezione. Anche in questo caso è importante ricordare che i primi tre byte designano la rete e l'ultimo byte indica l'host.

Fig. 3.4 Da IP a nome host: i DNS

I computer di una rete locale sono generalmente visti con il nome assegnato alla macchina e non con l'indirizzo IP, molto scomodo da scrivere ed usare. Tutto ciò avviene grazie al servizio DNS (Domain Name System).

DNS è un protocollo di risoluzione dei nomi, che converte nomi di host in indirizzi IP e viceversa. Il DNS è una database la cui struttura è ad albero. La radice di tale albero capovolto si trova nella parte più alta, mentre scendendo di livello si hanno diversi sottodomini, che si diramano dalla radice.

Approfondimento:

La radice dell'albero dei domini del DNS è indicata con un punto, come generalmente accadeva con le directory del vecchio DOS

Fig. 3.4.1: L'albero capovolto che rappresenta i sottodomini di Internet, partendo dal dominio radice, posto in alto

Nelle reti locali il DNS funziona come la figura, che si riferisce a Internet, ma nell'albero si hanno le diverse zone della LAN e gli host collegati.
