NETWORKING

Internet è una rete di reti: un insieme di reti collegate tra loro. Le reti sono organizzate in livelli, ciascuno costruito sopra il precedente. Lo scopo di un livello è quello di offrire certi servizi ai livelli più alti, nascondendo i dettagli su come tali servizi siano implementati.
Per creare un collegamento a Internet è necessario disporre sul proprio computer del software **TCP/IP**, il quale si basa su uno schema detto a **commutazione di pacchetti**. Questo significa che ogni file inviato su Internet è suddiviso in parti più piccole chiamate pacchetti seguendo le regole del **protocollo IP**. Ogni pacchetto è etichettato, includendo anche l'indirizzo numerico di destinazione, detto **indirizzo IP**.
Se si effettua un collegamento a Internet (che sia in linea commutata o meno), si ha bisogno di un host number che serve per identificare univocamente ogni computer connesso alla rete Inernet. I singoli programmi in esecuzione su questa macchina saranno identificati da un altro numero, il port number, in modo che il computer sappia distinguere i pacchetti diretti a ciascuno di essi. Se il collegamento è permanente, l'host number è attribuito una volta per tutte; altrimenti, il software TCP/IP otterrà questo numero dal computer del provider ogni volta che l'utente si collega a Internet. I computer speciali che collegano le viarie parti della rete e instradano i pacchetti nelle diverse zone sono chiamati **router**. Il nome di un computer non è equivalente all'host number, poiché non basta a identificare univocamente una macchina; per questo il sistema assegna a ogni calcolatore anche un dominio. Il nome di dominio serve per identificare un intero gruppo di computer collegati a Internet. Un dominio più grande (.it, .com, …) può comprenderne altri più piccoli (sottodomini). Ogni volta che si digita un nome, viene interpellato un apposito programma, il **Domain Name System**, per eseguire la traduzione in numero.
I router sono macchine collegate a due o più reti, che hanno il compito di far passare i pacchetti da una rete in modo da avvicinarli alla loro destinazione (i pacchetti diretti a una macchina collegata alla stessa rete del mittente arrivano a destinazione senza bisogno dei router). I router di Internnet hanno un compito semplice: inoltrare i pacchetti che ricevono alla loro destinazione, passandoli da router a router. Per inoltrare i pacchetti fino all'ultima fermata si crea una catena di router, ognuno dei quali sa l'indirizzo del successivo sulla rete grazie a tabelle costantemente aggiornate. L'instradamento viene fatto pacchetto per pacchetto.
Un **BBS** ovvero Bulletin Board System è un programma speciale che risiede su un certo computer e consente che altri computer si colleghino a lui via telefono. Per usare il servizio telematico, l'utente deve installare nel suo computer un dispositivo di comunicazione, detto modem, e collegare il modem alla linea telefonica. Poi userà un programma di comunicazione per connettersi al BBS.

RETI INTRANET

Il collegamento in rete permette

- la condivisione delle informazioni, ad esempio l'accesso contemporaneo ad un archivio di dati, sempre aggiornato e con la possibilità di trasmettersi l'uno con l'altro qualsiasi tipo di documento. L'archivio ovviamente deve risiedere in un disco rigido su uno dei computer collegati alla rete
- a condivisione di dispositivi hardware come dischi rigidi, ottici, stampanti, modem fax

CARATTERISTICHE TECNICHE

La creazione di una rete avviene con l'inserimento di una scheda all'interno di ciascun computer, con la sistemazione di un cavo che le unisca e l'installazione di un apposito programma di gestione della rete (sul server). Le reti si suddividono per:

- localizzazione delle postazioni
- topologia
- metodologia
- tecnologia
- protocollo
- sistema operativo di rete

LOCALIZZAZIONE DELLE POSTAZIONI

LAN (Local area Network) sono il tipo di rete più ampiamente diffuso negli uffici. Sono possedute da organizzazioni private. Esse si estendono su un piano di un edificio, o su un intero edificio (qualche chilometro). Non possono, di norma, posare cavi su suolo pubblico. Una LAN si può anche arrivare ad estendersi su più edifici vicini. Tutti i siti sono vicini tra di loro, ampia velocità di trasmissione, bassa frequenza di errori, costi alti.

Sono in generale broadcast con tipologia bus (IEEE 802,3, chiamato impropriamente Ethernet) o ring.

MAN (Metropolitan area Network) sono reti che collegano aree metropolitane quali Pubbliche amministrazioni, Università, Reti civiche, Agenzie di servi. Sono caratterizzate da alte velocità di trasmissione, costi elevati.

WAN sono nella maggior parte la combinazione di una serie di reti su area locale (LAN) opportunamente connesse tra di loro mediante collegamenti aggiuntivi per permettere la comunicazione tra loro. Sono nate per collegare tra loro siti di ricerca distanti tra loro e sono caratterizzate da costi bassi, velocità basse. Utilizzano linee telefoniche standard come mezzo di comunicazione principale (IEEE 802,6 i DDB).

WAN (Wide area Network)

- Si estendono a livello di una nazione o pianeta
- Sono costituite da due componenti:
- un insieme di elaboratori (host)
- una subnet che connette gli hot tra loro

  La subnet consiste di due componenti:
- linee di trasmissione (circuiti, canali, trunk)
- elementi di commutazione (switching element)

  Non esiste una terminologia standard per identificarli. Termini sono: sistemi intermedi, nodi di commutazione pacchetti, router. Molte topologie di interconnessione possono essere usate tra i router: a stella, anello, albero, magliata, completamente connessa.

La connessione non può essere messa in opera direttamente con cavi, ma viene realizzata tramite collegamenti telematici attraverso linee telefoniche ordinarie, lineee dedicate o servizi telematici pubblici o privati. Una WAN può essere anche realizzata in maniera mista: in parte cablata, in parte basata su radio o satellite.

L'**INTERWORK** è un insieme di più reti, anche non omogenee, collegate per mezzo di un gatway.

TOPOLOGIA

Nell'implementazione di una rete locale, bisogna prendere in considerazione diversi aspetti della rete, tra cui la collocazione del computer, l'ubicazione dei cavi, l'hardware richiesto per la connessione. Le postazioni di lavoro appartenenti alla stessa rete possono essere collegate in modi diversi.

Al momento attuale si utilizzano comunemente quattro topologie di rete:

- Reti a bus
- Reti a stella
- Reti ad anello
- Reti a doppio anello

Rete a bus
La rete a bus è il metodo più semplice per permettere la connessione tra più computer.
Consiste di un singolo cavo che connette tutti i computer. Il cavo parte dal server (o dall'hub) e si innesta in ciascuna postazione e dalla stessa riparte per la successiva. Quando un host deve comunicare con un altro host immette sulla rete i propri dati.
Questi dati arrivano a tutti computer sulla rete e ciascuno di essi quindi, li esamina per invididuare se sono diretti a lui. Se non lo sono le scarta, e così via fino a quando non raggiungono l'host destinatario.
Se più host iniziano l'invio contemporaneamente avviene una ***collisione***
e gli host lo possono scoprire.
Per il collegamento di host su una rete a bus si utilizzano i connettori BNC.
Uno degli svantaggi di questo tipo di rete, è che la disconnessione di un computer dalla rete può portare al blocco dell'intera rete.
La rete inoltre deve essere sempre terminata da un apposito ***terminatore*** (volgarmente ***tappo***) per impedire che la rete lasciata aperta si blocchi. È probabilmente il tipo di rete più economico, ma supporta un numero limitato di host.

Reti a stella
Tipo LAN centralizzata in cui i nodi, costituiti da stazioni (workstation) di lavoro, sono collegati a un computer centrale o hub. Dal serve (o dall'hub) partono tanti cavi quante sono le postazioni. I costi di collegamento sono più elevati rispetto ad altre topologie di rete; inoltre, dato che tutti i messaggi passano attraverso l'hub, in caso di un suo malfunzionamento l'intera rete va fuori uso.
Rispetto alla rete a bus ha però il vantaggio che la disconnessione di un singolo computer non comporta alcun impatto sul buon funzionamento della rete.

Reti ad anello
Le reti ad anello sono un tipo di rete locale decentralizzata i cui nodi, costituiti da stazioni di lavoro periferiche condivise e server di file, sono collegati da un cavo chiuso ad anello (un unico cavo circolare). Il cavo parte dal server (o hub), si innesta in ciascuna postazione e dalla stessa riparte per la successiva, e così via fino a quando non ritorna allo stesso server chiudendo il cerchio.
Ciò permette una maggiore velocità di trasferimento dati (data transfer rate) rispetto a una rete a bus , che raggiunge 16 MBPS (contro i 10 dello standard Ethernet).
I segnali sono inviati in senso orario lungo il circuito chiuso passando attraverso ciascun computer che funge da ripetirore e ritrasmette il segnale potenziato al computer successivo.
I dati viaggiano sulla rete con un metodo chiamato a passaggio di testimone o di gettone (token-ring).
Il token (gettone) viene trasferito da un computer al successivo finché non raggiunge quello su cui sono disponibili dati da trasmettere. Il token viene modificato dal computer trasmittente che aggiunge al dato l'indirizzo del destinatario e quello del mittente e lo rinvia lungo l'anello. I dati passano attraverso ciascun computer finché raggiungono quello il cui

indirizzo corrisponde a quello indicato sui dati. Questo computer restituisce un messaggio di conferma al computer trasmittente il quale crea un nuovo token e lo immette nella rete.
Nelle reti token ring, a differenza di altre, un computer malfunzionante viene automaticamente escluso dall'anello consentendo agli altri di continuare a funzionare regolarmente in rete. In altri tipi di reti ad anello, un computer che non funziona può provocare la caduta di tutta la rete.
Non sono reti basate su un mezzo trasmissivo broadcast. Non possono verificarsi collisioni.

Reti a doppio anello
Le reti a doppio anello sono simili a quelle ad anello, avendo la sostanziale differenza di utilizzare due anelli anziché uno:

- un anello primario e
- un anello secondario

Una uleriore differenza è l'utilizzo di fibre ottiche (FDDI – Fiber Distributed Data Interface).

Nelle normali condizioni i dati fluiscono solo sull'anello primario, utilizzando il secondario solo in caso di guasto del primario.

Ogni computer deve ovviamente essere connesso ad entrambi gli anelli, per poter commutare dal primario al secondario in caso di guasto.

Generalmete in questo tipo di rete non tutti i computer sono collegati ad entrambi gli anelli.

Tipologia ad anello a stella
E' una combinazione della rete a Stella ed ad Anello. Anche detta ad Anello con cablaggio a stella, è simile alla tipologia a bus a stella, ma in questo caso gli hub non sono collegati tra loro tramite cavi bus lineari ma attraverso un hub principale secondo un modello a stella.

Tipologia a bus a stella
E' una combinazione della tipologia a Bus e a Stella. Più reti a stella sono collegate tramite cavi a bus lineari. Il malfunzionamento di un computer non influenza il resto della rete. In caso di mancato funzionamento di un hub, tutti i computer connessi a qell'hub saranno esclusi dalla rete. Se l'hub a sua volta è collegato ad altri hub anche queste connessioni saranno interrotte.

METODOLOGIA

Per metodologia si intende il metodo con il quale ciascuna postazione di lavoro invia e riceve i dati. Le metodologie usate sono due:

- **CSMA/CD** (Carrier Sense Multiple Access/Collision Detection) che sta per Accesso multiplo con rilevamento della portante e riconoscimento delle collisioni.
  La portante (carrier) è il segnale elettrico che passa sul cavo trasportando i dati. Ciascuna postazione, prima di trasmettere i suoi dati sul cavo, rileva se sul cavo è già presente una portante o meno. Se non la rileva, trasmette i dati; se la rileva si ferma per riprovare dopo una frazione di secondo.
  Ogni scheda di rete segue questa tecnica quando deve spedire un messaggio che permette ad un computer di usare la rete solo se nessun altro la stava già usando. Dunque questo protocollo ha la caratteristica implicita di permettere ad un solo dispositivo di comunicare in un dato momento. Quando due dispositivi cercano di

comunicare simultaneamente, tra i pacchetti trasmessi si verifica una collisione che viene rilevata dai dispositivi trasmittenti. I dispositivi cessano quindi di trasmettere e si mettono in attesa prima di inviare nuovamente i loro pacchetti. Tutto ciò fa parte del normale funzionamento per le reti Ethernet e Fast Ethernet. Questo protocollo ha il compito di rilevare la collisione.

- **TOKEN PASSING** cioè passaggio di contrassegno.
  L'accesso alla trasmissione dei dati viene concessa ad ogni postazione di lavoro secondo un turno prestabilito. Il token è un segnale di contrassegno che viene inviato dal server alla prima postazione della rete. Se questa postazione ha necessità di trasmettere dati, lo può fare ed ha la temporanea proprietà esclusiva della rete. Al termine della trasmissione, o se la postazione non ha nulla da trasmettere, passa il contrassegno alla postazione immediatamente successiva nel turno. Il token viene passato da postazione a postazione, fino all'esaurimento del turno e d un nuovo inizio. Con questo sistema sono evitate le collisioni di dati. La metodologia CSMA/CD consente però una migliore ottimizzazione della rete, in quanto ciascuna postazione può utilizzare i tempi morti delle altre.

TECNOLOGIA

La tecnologia di rete si riferisce alle regole di comunicazione fra server, postazioni di lavoro e periferiche. Ciascuna tecnologia di rete utilizza esclusivamente una metodologia e una topologia ben definite.
Alcune fra le più diffuse sono:

- Ethernet (metodologia a CSMA/CD e topologia a bus).
  Fra le diverse tecnologie di rete le più diffuse, attualmente, sono **Ethernet** e **Fast Ethernet**. Queste sono abbastanza simili e la differenza maggiore è rappresentata dalla velocità con cui trasferiscono le informazioni. Ethernet funziona a **10 Megabit** per secondo (Mbps) e Fast Ethernet a **100 Mbps** per secondo. Ethernet è il tipo di rete locale più diffuso nel mondo. L'estensione che Ethernet può coprire varia da circa 200 m a 2,5 km a seconda delle varie versioni, con velocità di trasmissione di 10Mbit/s, 100, fino a 1000 Mbit/s di Gigabit Ethernet. Possiede una struttura eletrica (il segnale tocca tutti i nodi passando per un solo percorso) a bus: il segnale raggiunge tutti gli altri nodi seguendo un solo percorso. La struttura fisica invece può essere a bus o a stella, in cui i nodi si collegano ad un punto centrale. Il cavo che connette le varie stazioni è un cavo coassiale o un doppino (con otto fili al suo interno). Il cavo può essere anche a fibre ottiche.
  Ethernet fu la prima LAN utilizzata per trasportare i datagrammi IP, dopodiché fu modificata e trasformata in fast Ethernet. Originariamente la comunicazione era basata su un cavo coassiale. Ethernet è una tecnologia LAN che usa il protocollo TCP/IP.
  Fast Ethernet usa un frame così composto:

Destination Phisical address	Source Phisical address	Protocol type	IP datagram	FCS
	o MAC (Media Access Control)			
Address fild Usa 46 bit per distinguere indirizzi locali da globali. 0 indica indirizzi ordinari, 1 gruppi di indirizzi.				

Fast Ethernet e 802,3 sono due tecnologie di una LAN. Ulteriori tecnologie LAN sono 802,4 (rete bus), 802,5 (token ring), FDDI (tonken ring a fibre ottiche).

- **IBM Token ring** (metodologia a Token passing e topologia ad anello)
- Appletalk (metodologia a CSMA/CD e topologia a bus)
- **StarLAN**
- **FDDI** Una FDDI è una rete, come una token ring, ad anello. A differenza della token ring, Lo standard FDDI prevede l'utilizzo della fibra ottica per la realizzazione del canale multiaccesso. Ciò permette di utilizzare una FDDI sia come dorsale per LAN più lente, che come MAN.
  Un'altra differenza sostanziale da una token ring è che il traffico è suddiviso in due classi di priorità.
  Anche l'FDDI, come la token ring così come l'abbiamo descritta, usa trasmettere un free token subito dopo la trasmissione del pacchetto e ciò, come si può far vedere, garantisce ad una FDDI un throughput maggiore rispetto allo standard token ring dell'IEEE nel caso di alto traffico nella rete.
  Nell'FDDI distinguiamo due tipi di frame:
  * Token frame, che implementa il free token che abbiamo introdotto nella token ring.
  * Data frame, che implementa il pacchetto vero e proprio.

  I tipi di traffico previsti nello schema utilizzato da un'FDDI sono:
  * Traffico ad alta priorità, che può essere spedito subito da un nodo non appena il nodo riceve il token.
  * Traffico a bassa priorità, che può essere spedito subito da un nodo solo se non c'è congestione.

  Nell'FDDI è ritenuto opportuno imporre una limitazione sulla quantità di traffico ad alta priorità che può essere spedito. Il motivo è che si deve assicurare che entro un tempo ben definito un nodo possa trasmettere il traffico ad alta priorità che ha da trasmettere
- **ISDN** (**velocità variabile dai 64 Kbps ai 128 Kbps – il modem tradizionale va a 64 Kbps**) soffre di una grave limitazione che ne inficia le ottime caratteristiche: la limitazione di banda. Essa offre velocità di accesso da un minimo di 64 Kbps ad un massimo di 2 Mbps assegnabili ai servizi secondo multipli di 64 Kbps. ISDN rappresenta un passo significativo ma non è ancora sufficiente per raggiungere una piena integrazione dei servizi a causa della banda limitata e assegnabile in maniera poco flessibile.
  ITU, prendendo atto dei suddetti limiti, decise quindi di reingegnerizzare ISDN al fine di farla evolvere verso una rete a larga banda capace di gestire in modo flessibile il maggior numero possibile di servizi di telecomunicazioni. Nacque così il concetto di Broadband ISDN (**B-ISDN**).
  (ADSL è un accesso digitale (non analogico) ad alta velocità attraverso il doppino telefonico. Una nuova tecnologia modem, trasforma le normali linee telefoniche a doppino in percorsi di accesso per la comunicazione dati ad alta velocità di tipo multimediale. La velocità di trasmissione ADSL supera i 6 Mbit al secondo dalla centrale all'utente e può arrivare fino a 640 Kbit al secondo in senso contrario. Velocità di questo livello espandono la larghezza di banda delle linee telefoniche esistenti di un fattore di 50 o più volte superiore senza necessità di nuovi cablaggi. Nell'aprle 1997 l'ADSL Forum ha annunciato di aver approvato una raccomandazione tecnica per far transitare il traffico ATM su ADSL. Le piccole sedi remote possono entrare a far parte della rete geografica (WAN) aziendale mentre le loro reti locali (LAN), soprattutto quelle che utilizzano la tecnologia ATM, diventeranno pienamente integrate; gli utenti che operano dalle sedi remote potranno accedere alle Internet aziendali e scaricare da esse a velocità molto elevate).

- **ATM** Asynchrons Transfer Mode
  E' la tecnica di trasferimento delle informazioni che l'International Telecommunications Union (UTI) ha scelto per realizzare l'infrastruttura trasmissiva della Broadband Integrated Service Digital Network (**B-ISDN**), ovvero la **rete di telecomunicazioni** che nel prossimo futuro rappresenterà la piattaforma comune ad una pluralità di servizi tra cui telefonia, broadcasting televisivo ad alta definizione, Video onDemand (VoD), trasmissione dati, ecc.
  Questa tecnologia è stata sviluppata per l'invio veloce di voce, video e dati attraverso la rete, sia pubbliche che privata. I segmenti ATM sono molto veloci e sono suddivisi in unità chiamate CELLE. Le celle sono trasmesse attraverso la rete attraverso servizi chiamati switches, i quali analizzano le informazioni nell'intestazione per trasmettere le celle all'esterno. I frame sono segmentati in celle all'inizio e riassemblati in frame, una volta arrivati a destinazione da ATM Adaption Laer (AAL). Ci sono diversi AALs, ma l'unico rilevante per la trasmissione dei datagrammi IP è AAL5.
  ATM differenzia il contenuto delle celle nell'intestazione per dare priprità al traffico in tempo reale, ovvero fonia o video, rispetto alla trasmissione di dati. La sua velocità è di 155 Mbit al secondo e ciò ne fa la tecnologia ideale per il traffico multimediale, garantendo nel contempo prestazioni elevate anche alla trasmissione dati e ad altri tipi di traffico.
  Nonostante ATM sia stata concepita come una tecnologia di supporto alle telecomunicazioni su larga scala, non vi è alcun impedimento al suo impiego anche in ambiti ristretti quali le Local Area Network (LAN).
  Una rete ATM consente a numerosi utenti di condividere la larghezza di banda. Ciasun utente vede solo la propria rete ma, a differenza di una rete dedicata vera e propria, gli utenti possono aggiungere larghezza di banda per far fronte ai picchi di traffico, anche all'interno di una determinata connessione, confidando nel fatto che altri utenti non stanno utilizzando in quel momento la banda loro allocata. Si tratta di una modalità networking ad alte prestazioni economiche sia per l'utente sia per l'operatore.
  Gli switch ATM sono collegati tra loro attraverso linee di connessione numeriche di tipo punto a punto, tipicamente in fibra ottica, per realizzare la rete vera e propria secondo una topologia a maglia arbitraria.

PROTOCOLLO

Un protocollo è l'insieme di regole che governano il formato e il significato delle informazioni. Reti con diverse tecnologie possono avere lo stesso protocollo, mentre reti con la stessa tecnologia potrebbero usare diversi protocolli.

- TCP/IP (richiesto dal Ministero della Difesa degli Stati Uniti, viene adottato da tutte le tecnologie di rete);
- IPX/SPX (sviluppato dalla Novell, una casa produttrice del più diffuso sistema operativo di rete operante sui personal computer);
- NetBIOS e SDLC (sviluppati dalla IBM ed utilizzati per i propri elaboratori e personal).
  NetBEUI/NetBIOS
  NetBEUI è l'acronimo di NetBjos Extended User Interface, cioè, interfaccia utente estesa di NetBIOS. NetBIOS a sua volta significa Network Basic Input Output System, ossia, sistema input/output di base di rete. Infine SMB sta per Service Message Block, blocco messaggio server.
  Più che un protocollo, il NetBIOS, che lavora al livello Sessione, è un'API, cioè un'interfaccia di programmazione che, attraverso un set di comandi standard, unisce l'SMB con i protocolli di trasporto ed instradamento sottostanti, come TCP/IP o IPX/SPX.

NetBEUI è invece un protocollo, ed ingloba in modo nativo sia l'interfaccia NetBIOS, sia una semplice funzionalità di trasporto. Quindi, mentre il NetBIOS può lavorare solo se è abbinato ad un protocollo di trasporto, NetBEUI non ha bisogno ne di protocolli di trasporto, né di interfacce verso SMB.

- PROTOCOLLO SMB

Creato dall'IBM a metà degli anni '80 e successivamente adottato e modificato dalla Microsoft, si tratta di un importante protocollo, la cui implementazione è presente in quasi tutti i sistemi Windows. Si tratta di un protocollo di più alto livello, al di sotto del quale si può trovare il NetBEUI oppure il NetBIOS (quest'ultimo a sua volta su un protocollo di trasporto quale il TCP/IP o IPX/SPX). Il suo funzionamento è client-server, del tipo richiesta-risposta. Essenzialmente il lavoro di questo protocollo è quello di rendere possibile la condivisione di file e stampanti, incluse tutte le operazioni che comunemente vengono fatte su queste risorse (per es: aprire, chiudere, leggere, scrivere, creare, cancellare …). Ad ognuna di queste operazioni corrisponde un certo messaggio SMB (open, read, write, close …). Fa parte del protocollo SMB anche quel particolare elemento che permette di disporre delle risorse remote come se fossero locali. Il nome di questo componente è "redirector". Tramite il redirector ad esempio, è possibile vedere undisco di un altro computer come se fosse un disco sul proprio computer.

Per adattare meglio l'SMB ai vari ambienti sotto cui può lavorare, sono state create diverse varianti di questo protocollo. Per questo, quando due computer iniziano una connessione SMB, la prima cosa che viene fatta è decidere quale variante usare. Il modo per mettersi d'accordo è di inviare come primo messaggio, un SMB particolare chiamato "negprot" (negozia protocollo), che contiene le varianti conosciute dal mittente. Il ricevente risponderà indicando una cerca variante oppure, se non ne conosce nessuna tra quelle elencate dal mittente, risponderà con un numero speciale che indica l'errore. Successivamente ha luogo l'autenticazione, che avviene spedendo al server un nome utente e una password. In questo caso l'SMB usato è "sesssetupx". Se il login ha successo, viene inviato come risosta al richiedente un numero, l'UID, che dovrà essere reinviato al server in tutte le successive connessioni con esso. Infine, per accedere ad una risorsa condivisa, si fa uso dell'SMB "tconx" a cui segue in risposta un altro numero, il TID da usare inmodo analogo all'UID nei successivi accessi a quella risorsa. Il protocollo SMB è in grado di gestire due livelli di CIFS, o Common Internet File System, è una novità su cui sta lavorando Microsoft insieme ad altre società. Si tratta di un protocollo basato su SMB, ma orientato verso Internet e mira ad aggiungersi ai sistemi classici di accesso ai file (FTP, HTTP, NFS). Le specifiche sono aperte: l'intento è che diventino un RFC e vengono implementate su tutte le piattaforme, incluse quelle Microsoft e Unix. I vantaggi dichiarati consisterebbero in un accesso multiplo in scrittura ai file senza perdita di integrità, robustezza, buona velocità, sicurezza negli accessi, supporto dei caratteri in formato Unicode, uso di nomi con significatività globale per i file.

All'epoca l'obiettivo era quello di creare un protocollo su misura per le LAN di dimensioni contenute, quindi doveva essere piccolo, semplice, veloce e doveva permettere di assegnare nomi umani alle risorse invece dei complessi indirizzi usati dal TCP/IP. Inoltre NetBIOS è stato progettato perché usasse intensamente i broadcast (messaggi uno a tutti), piuttosto che interrogare un'entità centralizzata.

La diffusione di Internet ha messo subito in luce quali sono i limiti di NetBIOS e del suo socio NetBEUI quando la rete cresce di dimensioni.

Il degrado prestazionale sulle WAN dovuto all'uso dei broadcast, il problema dell'unicità di nomi. Dato che due computer non possono usare due nomi uguali nella stessa rete, bisognerebbe trovre un nome diverso per ogni computer connesso, cosa

non banale in una rete geografica. In secondo luogo, sempre a causa dei nomi, NetBEUI non permette il routing. Cioè, dato un nome NetBIOS, è impossibile sapere quale sia la strada per raggiungerlo. Un ultimo problema, forse il più importante, è che i router di Internet non permettono il propagarsi deibroadcast, tanto cari al NetBIOS quando cerca di localizzare un nodo.

Per evitare che il NetBIOS affondasse, invece di navigare in Internet, tornò molto comodo a Microsoft il fatto di poter abbinare l'interfaccia NetBIOS ad un protocollo molto più flessibile del NetBEUI, come il TCP/IP, e limitando l'impiego del NetBEUI nell'ambito delle reti locali tra sistemi Microsoft. In questo modo ogni messaggio elaborato da NetBIOS viene incapsulato in unmessaggio TCP/IP, che non soffre delle limitazioni di cui sopra.

- IBM SNA (architettura ancora molto diffusa soprattutto nelle grandi aziende dotate di sistemi informativi IBM
- Digital Decnet Phase IV
- Appletalk
- Standard IEEE 802 per reti locali
- Architettura OSI
- Decnet Phase V (conforme allo standard OSI)

SISTEMA OPERATIVO DI RETE

Il programma che gestisce la rete ed amministra tutte le postazioni di lavoro e le periferiche collegate, è per la rete l'equivalente del sistema operativo per il singolo computer. Su di lui risiede la responsabilità del funzionamento dell'intera rete, della trasmissione dei dati da una postazione ad un'altra, da una postazione ad una periferica, da un disco ad una postazione e viceversa. Il programma di rete deve risiedere in un computer dedicato a questa sola funzione, chiamato server, e deve sempre essere in esecuzione. Spesso il sistema operativo di rete è in grado di gestire reti con metodologie, topologie, tecnologie e protocolli diversi. Parallelamente deve essere presente un programma di amministrazione della rete, a volte in esecuzione sullo stesso server, altre volte da una postazione di rete. L'accesso al programma di amministrazione della rete viene concesso esclusivamente, tramite una parola d'ordine, al network manager, figura essenziale in qualsiasi tipo di rete, piccola o grande che sia.

COMPONENTI DELLA RETE

Altri componenti fisici o logici della rete, oltre al sistema operativo, sono:

- Server
- Nodo
- Pacchetto
- Cavi
- Repeater
- Bridge
- Router
- Gatway

SERVER

E' il computer sul quale è in esecuzione il sistema operativo di rete. Non è importante la sua collocazione fisica nell'ambito della rete, se non nella topologia a stella. In quelle a bus o ad anello può essere una qualsiasi delle postazioni. La maggior parte dei programmi di rete richiede che il server sia adibito a questo scopo esclusivo, e quindi quella postazione non può essere utilizzata per l'ordinario lavoro.

NODO
Il termine si riferisce a qualunque apparecchiatura sia connessa alla rete, sia una postazione che una periferica, sia un server che bridge o router. I nodi sono identificati dal sistema operativo di rete con un numero assegnatogli all'atto dell'installazione della singola apparecchiatura. Il numero identificativo del nodo costituisce l'indirizzo dell'apparecchiatura.

PACCHETTO
Il pacchetto è il più piccolo blocco di dati che il protocollo utilizzato dalla rete è capace di trattare. I documenti inviati da un nodo ad un altro vengono suddivisi in pacchetti. In ciascun pacchetto, oltre ai dati, sono presenti i numeri dei nodi di destinazione e di partenza e il numero progressivo del pacchetto all'interno dell'intera trasmissione. Ciò consente al protocollo CSMA/CD, di identificare i pacchetti persi per collisione e di effettuarne la ritrasmissione.

CAVI
La scelta dei cavi con i quali effettuare la trasmissione deve essere effettuata in considerazione non solo del costo dei cavi e delle loro installazione, ma soprattutto delle dimensioni che la rete deve avere, delle tecnologie utilizzate e del traffico prevedibile di dati. I tre tipi di cavi più utili sono:

- **Doppino telefonico**: filo a due poli, spesso non schermato, utilizzato per le normali linee telefoniche (il costo è molto basso, l'efficienza buona e la capacità di traffico mediocre);
- **Cavo coassiale**: filo a due poli, uno interno ed uno esterno che funziona anche da isolante per interferenze elettriche esterne. Offre un miglior isolamento rispetto al doppino e quindi consente velocità di trasmissione maggiori su distanze superiori. E' costituito da un conduttore centrale in rame circondato da uno strado isolante all'esterno del quale vi è una calza metallica. E' ormai sostituito quasi ovunque dalla fibra ottica. Rimane usato per la TV via caso e in molte LAN. Il sistema category è uno standard per il tipo di cavi di rame e va da 1 a 5 (il costo è medio, l'efficienza buona e così anche la capacità di traffico).
- **Cavo ottico (fibre ottiche):** è uno dei mezzi più recenti. Le fibre ottiche sono fatte di un sottilissimo cilindro centrale il vetro (core) circondato da uno strato esterno (cladding) di vetro avente diverso indice di rifrazione e da una guaina protettiva. Sono quindi raggruppate insieme in una guaina contenitrice esterna. Le fibre ottiche sfruttano il principio della deviazione che un raggio di luce subisce quando attraversa il confine fra due materiali diversi (core e cladding). Hanno prestazioni strepitose: è raggiungibile una velocità di trasmissione di 50,000 Gbps.
- **Trasmissione senza fili:** Un tipo di collegamento attualmente in sperimentazione prevede il collegamento senza l'utilizzo di cavi. Due sono i metodi:
- con infrarossi: ciascun nodo è dotato di un sensore ricevente e di un emettitore di infrarossi. Ciascun nodo, però, deve trovarsi a portata visiva di un altro e il contatto non deve interrompersi, quindi non deve essere disturbata da oggetti, da apertura o chiusura di porte o passaggio di persone;
- con onde radio: le onde elettromagnetiche, create dal movimento degli elettroni, viaggiano nello spazio alla velocità della luce e possono indurre una corrente in un dispositivo ricevente (antenna). La velocità di trasmissione è in funzione dell'ampiezza di banda utilizzata. I nodi possono trovarsi anche in posti diversi di un palazzo, od in palazzi adiacenti. Utilizzando frequenze radio diverse, vicine a quelle delle normali radio ricetrasmittenti, ci si può collegare alla rete pur trovandosi in una qualunque parte

della città. Soluzione studiata per i rappresentanti commerciali o per i dirigenti impegnati in riunioni fuori dalla sede dell'azienda.

REPEATER

Ciascuna tecnologia di rete ha una distanza massima oltre la quale i dati non possono essere trasmessi. Il segnale arriva, a quella distanza, ai limiti della comprensibilità, deteriorato e affievolito dal passaggio del cavo. Un repeater amplifica e ritrasmette il segnale, aumentando così la distanza massima raggiungibile dalla rete. Attraverso il repeater passa tutto il traffico di dati, non solo quello destinato alla parte opposta della rete, in modo da trasmettere la portante del segnale nelle metodologie CSMA/CD per occupare la rete, o il contrassegno di turno nelle metodologie token passin.

BRIDGE

Un bridge consente il collegamento tra due reti, in modo che le due reti ne formino una sola e che ciascun nodo della prima rete possa ricevere o trasmettere dati scambiandoli con un nodo della seconda rete. Il bridge è collegato ad entrambe le reti ed esamina tutti i pacchetti in circolazione nelle due reti. Quando riconosce, in un pacchetto di una rete, l'indirizzo di un nodo appartenente all'altra rete, lo smista in modo totalmente invisibile per gli altri utenti. Il normale traffico di dati all'interno di ciascuna rete continua ad avvenire in modo del tutto indipendente e separato. Quindi il suo lavoro consiste nel fare in modo che i dati generati da una rete rimangano separati dall'altra, salvo quando il destinatario non appartenga all'altra rete Il bridge può servire per

- connettere fra loro LAN distinte (es. Ethernet e Token ring)
- se si vuole una LAN la cui lunghezza superi i limiti massimi consentiti per Ethernet
- se si desidera, nel caso di una LAN contenente molti host, suddividerla in molteplici LAN.

Il bridge lavora al livello 2 del modello ISO/OSI, cioè al livello data link. Ciò significa che la loro operatività è basata esclusivamente sulle informzioni contenute nelle buste di livello due, mentre non vengono prese in considerazione quelle di livello tre. Questa è la caratteristica fondamentale che li differenzia dai router, che invece agiscono a livello tre. Questo comporta che l'indirizzo in base al quale si decide se inoltrare o meno un messaggio, è un indirizzo di scheda di rete Ethernet a 48 bit.

SWITCH E' un'evoluzione del bridge. Come quest'ultimo, il suo compito consiste nel far passare i dati solo ai segmenti interessati. A differenza del bridge, possiede diverse porte, ognuna collegata ad un segmento. Il traffico di un segmento viene propagato solo al segmento interessato. In pratica, è come se in uno switch fossero presenti tanti bridge.

ROUTER E' quel dispositivo che, in una rete TCP/IP determina quale sarà il prossimo nodo a cui inoltrare un pacchetto giunto in input, in modo da fargli raggiungere la sua destinazione. Un pacchetto può passare attraverso diversi router prima di raggiungere il nodo finale. **Il più comune router è il router IP**. Se una od entrambe queste reti sono connesse ad altre tramite altri router, anch'esse sono connesse tra loro. I dati possono essere scambiati anche fra nodi di reti non adiacenti, attraverso il passaggio di router diversi. Il router riconosce l'indirizzamento del pacchetto, e lo inoltra a destinazione attraverso diverse reti e diversi router seguendo la strada più conveniente. Nel caso che questa strada sia interrotta per traffico eccessivo di una delle reti intermedie o del suo blocco per malfunzionamento, il router cerca di inoltrare i dati seguendo percorsi alternativi. Il normale traffico di dati all'interno di ciascuna rete continua ad avvenire in modo del tutto indipendente e separato.

GATWAY Mette in connessione due o più reti intervenendo all'ultimo livello, il settimo, del modello ISO/OSI. In questo senso, il suo scopo non è tanto quello di connettere reti differenti, ma di mettere in connessione i servizi di due o più ambienti che altrimenti

sarebbero incompatibili. E' dunque usato per le comunicazioni tra differenti NOS (Network Operating System) es. Windows NT e IBM SNA. Permette inoltre la connessione fra due reti che utilizzano diversi protocolli di trasmissione, traducendo i pacchetti di dati da unprotocollo all'altro. Il gatway è tipicamente usato per connettere una rete costituita da personal computer ed una costituita da un mainframe ed i suoi terminali. I Gatway tolgono dai pacchetti le informazioni di protocollo e li ri-impacchettano per essere interpretati dalla rete di destinazione. Un Gatway può essere un dispositivo hardware o un software. Converte protocolli diversi, unisce reti diverse come Windows e UNIX.

TECNOLOGIA TRASMISSIVA

Le tipologie di rete sono fondamentalmente due:reti broadcast e reti punto a punto.

Nelle **reti broadcast** i vari elaboratori comunicano tra di loro attraverso la trasmissione di piccoli impulsi elettrici (chiamati pacchetti), che utilizzando un unico canale di comunicazione che è condiviso da tutti.

Brevi messaggi chiamati pacchetti, inviati da un elaboratore sono ricevuti da tutti gli altri elaboratori. Un indirizzo all'interno del pacchetto specifica il destinatario. Quando un elaboratore riceve un pacchetto, esamina l'indirizzo di destinazione. Se questo coincide col proprio indirizzo il pacchetto viene elaborato, altrimenti viene ignorato. Le reti broadcast, consentono anche di inviare un pacchetto a tutti gli altri elaboratori, usando un opportuno indirizzo (BROADCASTING). In tal caso tutti prendono in considerazione il pacchetto. Un'altra possibilità è quella di inviare il pacchetto ad un sottoinsieme degli elaboratori (MULTICASTING). In tal caso solo gli elaboratori di questo sottoinsieme lo prendono in considerazione, gli altri lo ignorano. Nelle reti broadcast il problema principale consiste nel decidere quale elaboratore (stazione) ha diritto di usare il mezzo trasmissivo quando c'è competizione. Si deve evitare che molte stazioni trasmettano contemporaneamente, perché i relativi segnali si disturberebbero a vicenda. I protocolli per decidere chi è il prossimo a trasmettere su un canale broadcast (detto anche multi access channel) appartengono ad un sottolivello del livello data link, detto anche sottolivello MAC.

Questo tipo di trasmissioni sono usate soprattutto nelle LAN, ma anche nelle parti di WAN basate su satelliti.

Nelle **reti punto a punto (PPP: Point to Point Protocol)**, i vari elaboratori utilizzando dei dispositivi intermedi per arrivare dalla sorgente alla destinazione. In queste reti l'instradamento (**routing**) ha un ruolo molto importante.

HDLC Hight Level Data link control è lo standard per la trasmissione di dati nelle reti punto a punto. I dati sono spezzettati in pacchetti, chiamati frame. Un frame include vari campi.

Flag	Dest. Adr.	Control	Data	Frame Chek Frequence FCS	Flag
Header				Trailer	
	Questo valore è espresso in numeri binari o esadecimali.	Questo campo contiene informazioni necessarie per trasmettere il frame sulla rete e informazioni relative al tipo di dato da trasmettere.		Campo utililizzato per determinare errori di trasmissione. Se l'indirizzo di provenienza e destinazione non sono correti, oppure qualche bits è alterato, il frame viene scartato.	Questo campo delimita il frame all'inizio e alla fine. Contiene la pattern 01111110. Questa sequenza di bit deve essere uguale nel flag iniziale e finale. Quando il datagramma arriva, viene rimosso lo 0

					davanti all’1.

Molti venditori hanno implementato la propria versione dell’interfaccia PPP HDLC, quindi questo non è uno standard pulito. Inoltre non riesce ad operare nelle comunicazioni multiprotocollo.
Per molto tempo non c’è stato un protocollo standard per le comunicazioni punto a punto. Così IETF (Internet Engineering Task Force) ha settato un protocollo standard: il PPP. Esso supporta multipli protocolli come IP, IPX, DECnet, OSI.
Include anche molti subprotocolli per esempio responsabili del set up, test, configurazione e chiusura della comunicazione. La struttura dei frame PPP è la seguente:

Flag	Address	Control	Protocol	Datagram	FCS	Flag
	Supporta la compressione. Si può utilizzare quella Van Jacobson					

PPP permette l’autenticazione usando due protocolli PAP (password authentication protocol) e CHAP (challenge handshake autentication protocol).
Nel protocollo PAP, messaggio, userid e password sono inviati assieme;
nel protocollo CHAP viene validata l’identità di chi stabilisce la connessione.
I dati possono essere inviati a connessioni lente, veloci, ISDN e fibre ottiche.
In generale le reti geograficamente localizzate tendono ad essere broadcast, mentre le reti molto estese tendono ad essere punto a punto.

unicast L'indirizzo unicast riguarda un'interfaccia di rete singola; in altri termini, un indirizzo unicast serve per raggiungere un'interfaccia di rete in modo univoco. Identifica l'indirizzamento punto-punto
anycast L'indirizzo anycast serve per essere attribuito a più interfacce di rete differenti (in linea di principio, queste dovrebbero appartenere ad altrettanti componenti di rete distinti). Si tratta di un indirizzo che ha le stesse caratteristiche esteriori di quello unicast, che però viene attribuito a diverse interfacce di altrettanti nodi, con lo scopo di poter raggiungere semplicemente quello che risponde prima (quello più vicino in base al protocollo di instradamento). Per la precisione, i pacchetti inviati a un indirizzo anycast dovrebbero raggiungere un'unica interfaccia di rete. identifica anch’esso un gruppo di stazioni, ma il pacchetto viene inviato alla prima (più vicina) di tali stazioni.
multicast L'indirizzo multicast serve per essere attribuito a più interfacce di rete differenti (in linea di principio, queste dovrebbero appartenere ad altrettanti componenti di rete distinti). I pacchetti inviati a un indirizzo multicast dovrebbero raggiungere **tutte** le interfacce di rete a cui questo indirizzo è stato attribuito. identifica un gruppo di stazioni: il pacchetto viene inviato a tutte le stazioni
MBONE e' la contrazione di Multicast Back bONE e cioe' una dorsale di rete con protocollo TCP/IP che usa l'indirizzamento Multicast piuttosto del normale indirizzamento Unicast.
Non e` una "nuova" rete ma semplicemente una nuova funzionalita` di Internet.
L'indirizzamento Unicast lo conosciamo bene, e' il normale indirizzo Internet di un computer in rete. Tutti gli applicativi Internet che conosciamo, dal telnet al Web, usano un indirizzamento di tipo Unicast.
L'indirizzamento Multicast usa gli indirizzi dal 224.0.0.0 (oltre la classe C) riservati per la sperimentazione.

L'indirizzo Multicast non appartiene ad un singolo computer ma a un gruppo di computer. Questo significa che un computer che sfrutta MBONE, o in genere un indirizzo Multicast, possiede almeno due indirizzi: il suo indirizzo Unicast e l'indirizzo del gruppo Multicast. Se un calcolatore si unisce a piu` gruppi Multicast avra' n indirizzi di rete.
La sperimentazione Multicast e' nata per esigenze multimediali e soprattutto di video conferenza. Il concetto e' semplice: se dieci persone stanno comunicando tra loro con un indirizzo Unicast e tutti devono avere le stesse informazioni, in rete circoleranno 90 pacchetti. Ognuno dei 10 partecipanti invia il proprio pacchetto ad ognuno degli altri 9.
Ma se tutti i 10 partecipanti appartengono allo stesso gruppo Multicast, i pacchetti che circolano in rete saranno solo 10, perche' ogni calcolatore che appartiene ad un gruppo sara' in grado di ricevere i pacchetti che portano l'indirizzo del gruppo.
Tutti i pacchetti che appartengono ad un gruppo Multicast hanno lo stesso indirizzo di destinazione anche se provengono da calcolatori diversi e arriveranno a calcolatori diversi.
La video conferenza, per essere decente, sfrutta larghissime bande di rete, limitare la decuplicazione dei pacchetti, identici e quindi inutili, e' la finalita' dell'indirizzamento Multicast.
La teoria appena esposta puo` non avere problemi se la applichiamo ad una rete locale ma cosa accade su rete geografica? (Chiaramente una video conferenza ha senso su scala geografica perche' su spazi paragonabili ad un campus universitario, puo` essere un gioco divertente ma nulla di piu`).
Quando la sperimentazione ebbe inizio, nessuno dei routers che collegava le varie reti locali, ad Internet, era in grado di gestire il Multicast.
Finalmente un limite!
Ma come resistere al fascino di un'idea nuova ed aspettare?. Impossibile!
Il rimedioe` stato semplice: esiste una frontiera? Bene espatriamo in modo clandestino. I routers non supportano Multicast? Creiamo software non per i routers ma per i computers, piu' flessibili, lo chiamiamo Mrouter. colleghiamo i vari Mrouters nel mondo con tunnel Unicast per scavalcare i routers.
E' nato MBONE.
Proprio in questi mesi, i routers, ma soprattutto i loro costruttori :-), hanno deciso di frenare l'espatrio clandestino di pacchetti Multicast e di gestirne, finalmente, il traffico. Non e' solo un problema formale: se i pacchetti vengono gestiti tra le frontiere e non sulle reti locali, il traffico diminuisce ulteriormente.

LE DOMANDE A CUI RISPONDERE

Quando una rete aumenta di dimensioni, le prestazioni peggiorano in modo proporzionale. Per ridurre al minimo questa tendenza è possibile suddividere appropriatamente la rete in diversi segmenti, inserendo dispositivi come **hub, switch o router**, a cavallo tra essi. A differenza degli hub, che si limitano a ritrasmettere i dati su tutte le porte esattamente come sono arrivati, i bridge, gli switch e i router sono in grado di smistare il traffico tra i vari segmenti, permettendo che i dati si propaghino fuori dal segmento solo se il destinatario dei dati trasmessi appartiene ad un segmento diverso da quello del mittente. Si prevengono così probabili intasamenti della rete quando mittente e destinatario appartengono allo stesso segmento.
E’ necessario conoscere alcuni elementi di base relativi alle reti prima di poter trovare delle risposte e prendere delle decisioni. E’ meglio usare cavi Category 3 o 5, fibra multimode o single-mode, Ethernet, Fast Ethernet, hub, sitch, hub in fribra ottica, Gigabit Ethernet, ATM, VoIP (Voice over IP), oppure LAN wireless?
Nella scelta della tecnologia più adatta alla propria azienda, è opportuno prendere in considerazione e trovare le risposte alle seguenti domande.

Quanto a lungo si rimarrà nello stesso edificio? Quanti utenti si prevede di avere in rete? (deve essere prevista la scalabilità ovvero la possibilità di aumentare le prestazioni del sistema aumentando il numero di elaboratori) Gli utenti avranno bisogno di spostare spesso i computer nell'ambito dello spazio di lavoro? Gli utenti dovranno mettere in rete applicazioni particolarmente affamate di larghezza di banda, sono previste applicazioni multimediali? Qual è la velocità della connessione aziendale a Internet?
GLI HUB sono dispositivi di connessione che garantiscono a due computer di poter comunicare e "vedersi" reciprocamente in una tipologia di rete. Queste operazioni vengono compite usando una metodologia a medium condiviso: una sorta di conferenza telefonica dove tutti i partecipanti possono ascoltare gli altri sulla linea. Dal punto di vista della sicurezza, qualsiasi computer host sull'hub può vedere i dati che appartengono a un altro host sul medesimo hub. Se la sicurezza tra i singoli host sulla rete costituisce una preoccupazione primaria, si dovrebbe prendere in considerazione fin da subito questo problema. Il tipo più piccolo di hub supporta da due a otto connessioni, mentre quello più grande, che spesso è configurabile a stack, offre centinaia di porte, ognuna delle quali può gestire un singolo computer che trasferisce i dati a 10 Mbps. Attenzione però! L'intero hub può trasmettere i dati alla velocità massima di 10 Mbps in aggregato; in conseguenza, se due computer stanno cercando di trasferire 10 Mbps ciascuno, non sarà possibile ottenere questa velocità.
GLI SWITCH permettono di segmentare il traffico. Ciò significa che il computer A non può accedere ai dati che vengono trasferiti tra il Computer B e il Computer C. La cosa equivale a una normale chiamata telefonica: il mittente e il destinatario della chiamata sono gli unici partecipanti. Questa soluzione è quindi più sicura rispetto all'uso di un hub. Gli switch di fascia bassa offrono 24 porte, mentre i sistemi di fascia alta sono dotati di centinaia di porte. Ciascuna porta può gestire un singolo computer su una connessione da 10 o 100 Mbps.
LE LAN WIRELESS rispetto a switch e hub, costituiscono un elemento relativamente nuovo. Invece di collegare i computer con cavi fisici, le LAN wireless usano antenne per trasmettere i dati attraverso un insieme specifico di frequenze radio. Mentre i computer si possono spostare, il ricevitore e le antenne per la LAN devono spesso essere stazionarie e si devono trovare entro una certa distanza dai computer. Il fatto di non usare cavi e di essere liberi di spostarsi ha molte implicazioni. Dal momento che non ci sono cavi che collegano ciascun ufficio, non occorre creare un impianto di cablaggio e la scalabilità risulta molto più economica. Durante gli spostamenti, ci sono meno dispositivi da acquistare e da mantenere.

SCEGLIERE UNA TECNOLOGIA

Ciascuna tecnologia ha un proprio costo associato. Una parte dell'equazione dei costi è costituita dall'infrastruttura fisica indispensabile per usare una qualsiasi di queste tecnologie; si ricordi che in due soluzioni su tre bisogna creare una struttura di cavi nel quadro dell'implementazione. Il cablaggio di un ufficio con una ventina di postazioni può costare più di una decina di milioni. Il sistema "category" è uno standard per il tipo di cavi di rame che vengono utilizzati. In generale, il numero di category indica quanto strettamente il cavo è intrecciato e quindi anche la velocità dei dati che può trasportare. Il category 3 è lo standard di cablaggio minimo indispensabile per ottenre connessioni da 10 Mbps. I cavi category 5 possono raggiungere la velocità di 100 Mbps; prima di dedicarsi al ri-cablaggio dell'ufficio, è tuttavia opportuno tenere presente che i cavi category 5 possono costare il doppio di quelli category 3.
Quando arriva il momento decidere tra switch, hub e reti wireless, la soluzione più economica consiste in un hub. Quest'ultimo è caratterizzato da un modesto ingombro fisico e dalla presenza sul mercato di molti importanti produttori quali 3Com, Cabletron e

Lucent. Gli hub tuttavia possono causare una degradazione delle prestazioni di rete e problemi di sicurezza. Con il crescere dell'utilizzo, a causa del maggior numero di host oppure di programmi "a utilizzo elevato" come i visualizzatori multimediali, le prestazioni possono diminuire in modo notevole. Per esempio, un file da 10 Mbyte trasferito da una porta hub a 10 Mbps verso un'altr porta hub da 10 Mbps verrà in media trasferito alla velocità di circa 1 Mbps (portando a ottenere un tempo totale di trasferimento di 10 secondi). Se si desidera avere una rete più veloce, la scelta migliore potrebbe essere quella di usare switch in grado di gestire dei trasfrimenti a 100 Mbps. Su uno switch full-duplex da 100 Mbps, lo stesso file da 10 Mbyte citato nell'esempio dell'hub potrebbe essere trasferito a più di 10 Mbps; il trasferimento del file richiederebbe quindi meno di un secondo. Si tratta di un sostanziale incremento delle prestazioni, anche per un file relativamente piccolo. Si immagini come in questa situazione verrebbe trasferito più velocemente un filmato da 1 Gbyte, oppure un pacchetto software da 400 Mbyte.
Gli switche sono inoltre scalabili, dal momento che possono avere molte porte e permettono di inserire con facilità nuovo hardware nello stack. Se si decide di fare completamente a meno di una struttura di cavi, è possibile utilizzare i dispositivi wireless. In questo caso non è richiesta alcuna struttura di cavi ed è consentito il computing mobile in tutto l'ufficio. Naturalmente, questo schema risulta incredibilmente utile negli uffici che non hanno o non possono avere una struttura di cavi.

HALF E FULL DUPLEX

Una volta scelta la tecnologia di rete, la fase successiva nell'implementazione della rete aziendale consiste nel decidere a quale velocità la rete dovrà operare. Le impostazioni duplex sulla rete sono un'altra questione da prendere in considerazione. Il duplex indica se i dati che vengono trasmessi e ricevuti sono inviati attraverso gli stessi cavi oppure no. Analogamente a una strada senso unico, lo schema half-duplex è invece come una strada a due sensi, con una doppia linea bianca centrale. Il traffico scorre in entrambe le direzioni e non attraversa le corsie, portando ad avere un numero minore di collisioni. In termini di cavi, lo schema half-duplex invia tutto il traffico lungo una coppia di cavi. Entrambi questi cavi vengono usati per trasmettere o ricevere. Quando un pacchetto di dati da un host viene inviato su un cavo che contiene già un pacchetto in arrivo, si verifica una collisione ed entrambi i pacchetti vengono scartati. I nuovi pacchetti vengono inviati secondo intervalli ritardati a caso, in modo da minimizzare le probabilità che avvenga nuovamente una collisione. Le trasmissioni full-duplex mettono i dati su ciascun lato di coppie di cavi separate. Questo schema richiede che entrambe le estremità siano in grado di gestire la trasmissione full-duplex e il fatto di avere due coppie (quattro cavi) tra queste estremità. Lo schema full-dupex aumenta la possibilità che le velocità della linea (10 Mbps o 100 Mbps) si avvicini al massimo teorico.

GIGABIT ETHERNET

Esiste un'opzione che consente di superare la barriera dei 100 bps: lo schema Gigabit Ethernet. Se gli switch sono connessi da cavi category 5 e da interfacce di rete multiple, si può ottenere una velocità a livello di Gbps. Gli switch e le interfacce di rete devono in questo caso essere compatibili con la tecnologia Gigabit Ethernet. L'idea è quella di usare tutte le porte di scheda Ethernet a quattro porte e aggregare simultaneamente il traffico su di esse; in questo modo, un computer può teoricamente trasferire i dati con una velocità prossima a 1 Gbps.

DAGLI HUB AGLI SWITCH

Gli hub di rete possono esser collegati soltanto a cascata due a due: se si dispone di un hub a 24 porte, si può collegar un altro hub a una di queste porte. Ciò porta il totale

complessivo a 576 porte. Non è possibile aggiungere un ulteriore insieme di hub in modo da aumentare ancora di più il numero di porte, dal momento che il signaling fisico della rete non lo consente. In questo caso, la conseguenza è che gli hub hanno una inerente limitazione nella capacità di crescita. Ciò nel limita sostanzialmente la scalabilità.
Gli switch di rete, d'altra parte, possono essere concentrati. Inserendo nell'ambiente degli switch al alta densità e interconnessioni in fibra ottica, il numero di switch fisici che si vedono reciprocamente è limitato soltanto dalla quantità di fibra ottica disponibile. In breve, gli switch hanno un'elevata densità di porte (più porte per slot e per dimensioni di altezza) e possono essere collegati attraverso un anello di fibra ottica, che garantisce la possibilità di connettere reciprocamente centinaia di switch.
In una fase di transizione, è ragionevole prendere in considerazione una configurazione mista con switch e hub. Per implementare questa configurazione ed essere ancora "legali" dal punto di vista delle limitazione di signaling inerenti agli switch di rete (come specificato dalla IEEE), è necessario inserire uno switch multiporta (24 porte, 48 porte, o altro) e collegare a catena gli hub da qest'ultimo. Ciò garantisce la sicurezza di ogni hub, dal momento che tutto il traffico ad esso diretto passerà attraverso una porta sicura sullo switch. La segmentazione aiuta inoltre a ridurre le contese e la congestione della rete. Quello della congestione è uno dei fattori che più comunemente contribuiscono al raggiungimento di scarse prestazioni. I sistemi operativi NT e Unix sono in grado di sondare la congestione della rete vista da ciascun host. Se il livello di collisioni risulta maggiore del cinque per cento dei pacchetti totali in transito nell'interfaccia di quella macchina, esistono dei problemi di congestione.

MAC address e indirizzi IP:

Poiche' molte macchine possono condividere una singola connessione ethernet, ognuna di esse deve possedere un identificatore (ricordate che, in realta', e' la scheda di rete, l'hardware, a possedere un indirizzo, non la macchina in se'); questo non succede quando comunichiamo con una connessione dial-up utilizzando il nostro modem casalingo, perche' si presuppone che tutti i dati che inviamo siano destinati all'entita' che risiede all'altro capo della linea (in genere il nostro Internet Service Provider, che ci assegnera' un indirizzo IP dinamico). Tuttavia, se comunichiamo attraverso una rete ethernet dobbiamo specificare esattamente a quali macchina andranno consegnati i pacchetti inviati, anche se la rete fosse composta solamente da due computer: ricorderete che il protocollo ethernet fu sviluppato per permettere a migliaia di macchine di dialogare fra loro.

Cio' e' possibile 'inserendo' un numero esadecimale (cioe' con notazione a 16 cifre; il MAC address e' composto, invece, da 12 digit) in ogni destinazione ethernet ;
questo numero, in apparenza astruso e' l'indirizzo MAC.
Eccone un esempio: **00-40-05-A5-4F-9D**

Il MAC address e' composto da 48 bit (8bit = 1byte ; il bit e' l'unita' di misura fondamentale dell'informatica).
Questi 48 bit verranno divisi in due meta': 24 bit identificano il nome del produttore della ethernet card, i riamanenti 22 bit identificano il nemero di serie UNICO assegnato alla scheda dallo stesso produttore: in questo modo l'indirizzo MAC di due ethernet adapter non sara' mai uguale; questo serial number e' chiamato OUI (Organizationally Unique Identifier) - e gli ultimi 2 bit ? -

Il protocollo ethernet ci permette anche di comunicare con macchine che non risiedono sulla nostra stessa rete ma sono interallacciate alla nostra tramite il protocollo TCP/IP

(Transport Control Protocol over Internet Protocol, in realta' e' un'intera famiglia di protocolli): tuttavia non e' possibile inviare e ricevere i dati nella loro forma originale allo stesso modo in cui non e' possibile inviare per posta (snail mail) una lettera senza averla imbustata e dotata di francobollo e indirizzo del destinatario.

L'invio dei dati e la loro gestione in rete e' gestita dai diversi protocolli, a partire dall'ethernet, cosi' dovremo trattare i nostri dati in modo che i protocolli possano 'capire' cosa farne.

- cos'e' uno sniffer?

Uno sniffer e' un qualsiasi strumento, sia esso un software o un apparato hardware, che raccoglie le informazioni che viaggiano lungo una rete (network). Questa rete puo' utilizzare un protocollo di comunicazione qualunque: Ethernet, TCP/IP (Internet si basa principalmente su questo protocollo), IPX o altri.

Le funzioni tipiche degli sniffer non differiscono di molto e possono essere riassunte sinteticamente in:

* conversione e filtraggio dei dati e dei pacchetti in una forma leggibile dall'utente
* analisi dei difetti di rete, ad es. perche' il computer 'a' non riesce a dialogare con 'b'
* analisi di qualita' e portata della rete (performance analisys), ad es.per scoprire 'colli di bottiglia' lungo la rete
* setacciamento automatizzato di password e nomi di utenti (in chiaro o, piu' spesso cifrati) per successiva analisi
* creazione di 'log', lunghi elenchi che contengono la traccia, in questo caso, del traffico sulla rete
* scoperta di intrusioni in rete attraverso l'analisi dei log del traffico

I PROTOCOLLI

I protocolli sono gli standard che definiscono il modo in cui i computer comunicano l'un l'altro. La comunicazione tra i componenti è garantita dal protocollo e non dalla marca del computer o del sistema operativo che si sta usando. Il protocollo TCP/IP è lo standard di comunicazione che tutti i computer collegati a Internet devono usare.
La tecnica più largamente usata nelle reti di trasmissione dati come Internet è quella detta a **commutazione di pacchetto** (packet switching). In questo caso il messaggio viene diviso in pacchetti di dimensioni prefissate che costituiscono l'unità di trasmissione. La seconda tecnica in uso è la **commutazione di messaggio** (message switchin). Questa tecnica non prevede che il trasmittente sia connesso direttamente al ricevente, ma piuttosto che si limiti ad affidare il messaggio al più vicino centro di smistamento. Questa tecnica è oggi d'attualità soprattutto per la realizzazione dei sistemi di posta elettronica su scala internazione ed intercontinentale.
ARPANET fu il primo protocollo per reti, ma era lento e soggetto a frequenti crasher. Supportava un numero limitato di tipologie di reti.

MODELLO ISO/OSI

L'ISO, l'organismo internazionale (International Standards Organization) incaricato della standardizzazione in campo informatico, ha messo a punto un modello standard

largamente accettato che viene chiamato OSI (Open System Interconnection) e definisce sette strati di protocolli. Questo modello non definisce uno standard tecnologico, ma un riferimento comune ai concetti che riguardano le reti.

Application layer	Consente ai programmi di accedere ai servizi di rete. · Posta elettronica · Applicazioni per teleconferenze · World Wide Web
Presentation layer	Determina il modo in cui i dati sono formattati nello scambio tra due computer in rete. I dati ricevuti dallo strato dell'applicazione sono tradotti in un formato intermedio comunemente riconosciuto. Lo strato di presentazione è responsabile anche per le traduzioni e le codifica dei dati e conversioni dei set di caratteri e dei protocolli. Alcuni formati di presentazione gestiti dallo strato di presentazione sono: · ASCII · EBCDIC · XDR
Session layer	Svolge funzioni di sicurezza. Si occupa di identificare l'utente del programma che desidera accedere alla rete, per essere sicuri che ne abbia l'autorità. Assicura che i messaggi inviati dall'uno all'altro siano ricevuti con un alto grado di attendibilità. Organizza e sincronizza lo scambio di dati tra i processi di applicazione.
Transport layer	E' il cuore della gerarchia di protocolli, fornisce un trasporto affidabile ed efficiente tra l'host di origine e di destinazione. E' quello che divide il messaggio che proviene dallo strato superiore (il file, o il messaggio di posta elettronica) in segmenti da trasmettere separatamente e riassembla i dati in flusso di dati. Spedisce i segmenti al destinatario numerandoli sequenzialmente. Il destinatario, alla ricezione dei segmenti, invia un segnale di avvenuta trasmissione. Nel caso di non avvenuta ricezione di un segmento, il destinatario può richiederne la trasmissione. In questo modo sussiste il controllo degli errori nel trasporto dei dati. Provvede ad una connessione tra l'host mittente e l'host destinatario. A differenza di quanto avviene negli strati superiori, il sofrware dello strato di trasporto può gestire contemporaneamente più messaggi provenienti da sessioni diverse in corso sullo stesso computer.
Network layer (strato della rete)	Muove i pacchetti da sorgente a destinazione. Gestisce l'instradamento dei pacchetti creati da quello di trasporto e assicura la correttezza della comunicazione richiedendo la ritrasmissione dei pacchetti eventualmente danneggiati. Determina il modo migliore per spostare i dati da un host all'altro. Gestisce l'indirizzamento dei messaggi e la trduzione degli indirizzi logici (gli indirizzi IP) in indirizzi fisici (indirizzi MAC).
Data link layer (strato del collegamento dati)	Muove le informazioni da un capo all'altro di un singolo canale. Include i pacchetti in strutture più lunghe dette frame. I frame comprendono numerosi campi per le informazioni di controllo. Inoltre il messaggio viene completato con nuovi frame (frame acknowledgment) che contengono solo informazioni di servizio, ad esempio per la ricezione della avvenuta ricezione degli altri frame. Questo strato si occupa dell'invio dei frame dei dati dallo strato della rete a quello fisico.

	Quando riceve i bit dallo strato fisico, li traduce in frame di dati. Un frame comprende le seguenti componenti: · ID del destinatario. In genere è l'indirizzo dell'host di destinazione o del gatway predefinito · ID del mittente · Informazioni di controllo. Includono informazioni quali l'effettivo tipo di frame e notizie riguardo l'intradamento e la segmentazione · CRC. Effettua la correzione degli errori e verifica che il frame di dati sia arrivato intatto all'host destinatario Ha dunque il compito di offrire una comunicazione affidabile ed efficiente tra due macchine adiacenti, cioè connesse fisicamente da un canale di comunicazione (es. cavo coassiale, doppino, linea telefonica)
Phisical layer (strato fisico)	Definisce un insieme di regole relative all'hardware di comunicazione come ad esempio le tensioni e le correnti usate, cavi, fibre ottiche. Ha a che fare con la trasmissione di bit grezzi su un canale di comunicazione. Deve garantire che se parte 1, arrivi effettivamente un 1 e non uno 0. Riguarda dunque le caratteristiche meccaniche, elettriche e procedurali delle interfacce di rete (componenti che connettono l'elaboratore al mezzo fisico) e le caratteristiche del mezzo fisico.

MODELLO TCP/IP

TCP sta per Tranfer Control Protocol, IP sta per Internet Protocol. In realtà il protocollo TCP/IP è una famiglia di protocolli, ognuno con un sua funzione particolare, TCP ed IP sono due protocolli importanti di questa famiglia. Abilita la comunicazione tra computer eterogenei indipendentemente dalla rete fisica e dal sistema operativo.

Applicazione	Nello strato delle applicazioni si trovano le applicazioni che si basano sulla rete. Applicazioni di questo tipo sono le applicazioni Winsock dell'ambiente Windows quali **FTP e Telnet, SMPT, HTTP, NNTP, RLOGIN, NEWS, DNS** (Demain Name System – trasforma il nome della macchina in un numero IP). **PROTOCOLLI APPLICATIVI** **FTP – FILE TRASFER 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 del file. **HTTP – HYPERTEXT TRANFER PROTOCOL** E' il protocollo che interconnette quella vastissima collezione di siti internet generalmente nota con 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. E' la funzionalità di questo linguaggio, unita all'interfaccia grafica fornita dai browser, la vera ragione della praticità d'uso e quindi del successo del

	WWW. **SMPT – 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 a 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. **SNMP, Simple Network Management Protocol**, serve a gestire e monitorare lo stato della rete. Specifica la comunicazione tra il programma del server e il programma del client. **FILE ACCESS** Abilita il client ad accedere a file sul server. **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). Di solito le macchine UNIX permettono il login remoto, mentre i sistemi Windows non lo consentono. **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. SNPT e DNS sono protocolli aggiunti successivamente, per implementare gli altri servizi TCP/IP.
Trasporto	In questo strato si trovano i due protocolli **TCP** **UPD** (Connectionless: è un servizio non orientato alla connessione; ogni pacchetto viene trattato indipendentemente da tutti gli altri. Una sequenza di pacchetti spediti da un computer ad un altro potrebbero seguire cammini diversi per giungere a destinazione) Il compito è proprio quello di trasportare i dati da un host all'altro utilizzando le porte.

TCP fornisce un servizio byte-stream. Questo termine indica che i dati da e per i livelli superiori vengono presentati e ricevuti come un unico flusso di byte e non come pacchetti. Sarà compito del TCP suddividere i dati da spedire in tanti segmenti (un pacchetto TCP è detto **segmento** o **frame**) indipendenti e numerati.
In pratica ciascun frammento di dati viene numerato e spedito al destinatario. Il destinatario una volta ricevuti i frammenti provvede ad inviare al mittente un messaggio di avvenuta ricezione dei frammenti. A questo punto il mittente provvede ad inviare i frammenti successivi. In caso di mancata conferma dell'avvenuta ricezione da parte del destinatario il mittente provvede a spedire di nuovo i frammenti. Questo meccanismo ovviamente appesantisce la trasmissione, ma assicura un elevato grado di affidabilità.
Ad ogni segmento, TCP aggiunge il suo **header** in cui sono contenuti i seguenti dati:

- **source porte** e **destination port**. Ci sono diversi numeri standard per le comunicazioni più utilizzate detti well known service, ad esempio 21 per FTP, 23 per Telnet, 53 per DSN, 80 per Web Sever.
- **Sequence number** contiene il numero necessario per sapere quale sia l'ordine dei segmenti e per sapere se qualcuno è andato perduto
- **ed altri come** Acknowledgment number (usato per segnalare che sono arrivati tutti i dati. TCP corregge eventuali errori insorti durante la trasmissione ed in caso non siano arrivati tutti i frame vengono ritrasmessi. Ciò non succede nel protocollo UDT), window (indica in bit l'ampiezza della finestra che il computer è in grado di ricevere), data offset (indica dove iniziano i dati), reserved (per usi futuri), flags, checksum (serve per sapere se il datagramma corrente contiene errori nel campo dati), urgent pointer, options; padding
- **data** il campo riservato ai dati.

Quando due computer utilizzando TCP (comunicazione punto a punto) devono innanzitutto creare una **sessione**. La procedura attraverso la quale la sessione viene stabilita si chiama three way handshacking o handshacking a tre vie.
Nel corso di trasmissioni di questo tipo ci si serve di numeri sequenziali e di conferme per assicurare il trasferimento con successo dei dati. Normalmente, quando si stabilisce una comunicazione generica, TCP genera un numero di porta casuale. Se però si vuole iniziare una connessione con un protocollo di alto livello, come per esempio il protocollo SMPT, bisogna prima di tutto specificare che si vuole una connessione attraverso la porta n. 25 (o lo farà il lettore di posta). Solo dietro a questo numero di porta ci sarà SMPT in ascolto. Ci sono diversi numeri standard detti well known services, ad esempio 21 per FTP, 23 per Telnet, 53 per il servizio DNS, 80 per il Web Server. Quando si vuole terminare una sessione si usa una procedura di terminazione a quattro vie.
Per evitare congestioni indesiderate sulla rete, TCP dispone di alcuni algoritmi di controllo come slow stard, congestion avoidance, fast retrasmit, fast recovery.
Il protocollo TCP garantisce sicrezza e che i dati arrivino senza errori, senza omissioni e in sequenza. Esso passa poi i frame al protocollo IP che li indirizza (router) alla loro destinazione.

	La comunicazione tramite protocollo TCP viene implementata da programmi chiamati ROUTINES. Questi usano l'interfaccia di programmazione socket per settare la connessione TCP, inviare e ricevere dati e chiudere la connessione. TCP può ricevere e inviare dati nello stesso momento. Questa è chiamata connessione doppia. La connessione inoltre è sicura e i dati possono essere trasferiti solo quando si è stabilita una connessione. Utilizzando invece il protocollo **UDP** non vi è certezza dell'avvenuta ricezione da parte del destinatario dei dati spediti (i dati non vengono rispediti), ma in compenso la trasmissione risulta più semplice e veloce. Questo perché non è stabilita una connessione dedicata tra le due macchine. La connessione è virtuale. Non è dunque necessario stabilire una connessione prima di trasferire i dati, essi si possono inviare in ogni momento usando il metodo broadcast. Inoltre i dati trasmessi non sono sequenziali. UDP viene utilizzato nei casi in cui la velocità di trasmissione sia più importante della sicurezza della trasmissione (p.e. applicazione real-time). Oppure quando si deve inviare una richiesta che sta tutta in un solo datagramma. Per implementare la comunicazione tramite protocollo UDP sono usate delle semplici SUBROUTINES che creano, trasmettono e ricevono messaggi stand-alone.
Internet	***Attraverso questo livello vengono definiti gli indirizzi. I pacchetti che vengono utilizzati in questo livello si chiamano datagram e come tali contengono solo informazioni legate agli indirizzi IP e non a quelli fisici di competenza del livello inferiore. Quando un datagram è più grande della dimensione massima diunpacchetto trasmissibile in quel tipo di rete fisica utilizzata, il protocollo IP si deve prendere cura di scomporre il datagram in segmenti più piccoli e di ricombinarli correttamente alla destinazione.*** Lo strato internet svolge tre funzioni principali: · L'indirizzamento · La suddivisione in pacchetti · L'instadamento In questo strato risiede l'**IP** che offre la consegna di informazioni senza connessione e non garantita. Il protocollo IP non svolge alcun tipo di controllo per assicurarsi il buon esito del trasferimento di dati. Questo compito viene lasciato ai protocolli superiori come TCP. Di conseguenza i pacchetti possono andare perduti o non arrivare in sequenza. Il ruolo svolto da IP è quello di aggiungere a ciascun pacchetto una intestazione contenente una serie di informazioni per poter effettuare il corretto instradamento dei dati. L'intestazione contiene: · Indirizzo IP di origine: è l'indirizzo IP assegnato al mittente · Indirizzo IP del destinatario · Il protocollo di trasporto TCP o UDP. Serve ad indicare all'host destinatario il tipo di trasporto e di conseguenza il modo in cui manipolare i dati ricevuti · Checksum: è il CRC calcolato sui dati trasferiti/da trasferire che permette di verificare l'integrità dei dati · TTL: il tempo di durata in vita di un datagram; alla partenza viene assegnato un valore predefinito che diminuisce ad ogni attraversamento

di un router; quanto il TTL raggiunge il valore zero viene il datagram tolto dalla rete

L'IP router ha una tabella di destinazioni per trovare la path per inviare i datagrammi a destinazione. Nelle piccole reti IP usa delle tabelle di destinazione che sono mantenute manualmente da un amministratore di rete. Nelle grandi reti sono aggiornate automaticamente scambiando dati non altri router. IP può assicurare la connessione con molte interfacce hardware. Queste possono essere configurate come tecnologia Ethernet e Token Ring.
Se la destinazione del datagramma non è presente nella subnetwork dell'IP, esso invia il datagramma ad un altro router, se quest'ultimo non trova la destinazione nella sua tabella, invia il datagramma ad un altro router. IP invia i dati in unità chiamate datagrammi. Un datagramma ha un'intestazione IP che contiene le informazioni relative agli indirizzi per i livelli specifici, e provvede ad instradarli. Questo trasporto è chiamato connectionell (come per UDP) perché ogni datagramma è inviato indipendentemente. Non è garantita la sicurezza: i datagramma possono arrivare a destinazione danneggiati, duplicati, non in sequenza o non arrivare affatto.

SLIP (Serial Line Internet Protocol) implementa il protocollo IP ed è usato per trasmettere datagrammi IP. Slip indica anche la fine di un datagramma mediante numeri binari 11000000 o esadecimali. I dati vengono inviati byte byte, come una singola linea. SLIP connette diversi sistemi operativi. La comunicazione può avvenire host to host; host to router; router to router.
SLIP supporta solo il protocollo IP. Non supporta nessun tipo di autenticazione e non è uno standard: esistono molte versioni incompatibili.
CSLIP (Compressed SLIP) comprime l'intestazione di TCP/IP usando l'algoritmo Van Jacobson.

Altri protocolli situati nello strato Internet che servono per il controllo del funzionamento della subnet sono:

- **ARP** (Address Resolution Protocol)
- **ICMP** (Internet Control Message Protocol)
- **IGMP** (Internet Group Management Protocol)
- **RARP**

IL PROTOCOLLO ARP
Quando due computer su una stessa rete Ethernet vogliono comunicare, essi devono prima conoscere l'indirizzo fisico. Ogni volta che siamo TCP/IP su Ethernet e vogliamo comunicare con un sistema di cui conosciamo solo l'indirizzo IP, viene spedita una richiesta ARP di tipo di broadcast sulla rete. In essa si chiede ai computer in ascolto quale sia l'indirizzo fisico corrispondente a quell'indirizzo IP. Il computer interessato fornisce la risposta, noi la riceviamo, la mettiamo nella nostra ARP-Table, dopo diche possimao parlare con quel computer in modo diretto. Se in seguito abbiamo nuovamente bisogno di parlargli, guardando nella ARP-Table, ci accorgeremo che conosciamo già l'indirizzo fisico, così non dovremo

neppure inviare una richiesta ARP.
Quando tutto è pronto e si conosce grazie ad ARP l'indirizzo fisico del destinatario, non resta che spedire il tutto. Nel sistema ricevente, tutti gli header saranno analizzati ed utilizzati opportunamente e via via rimossi.

RARP (Reverse Address Resolution Protocol)
Quando, per vari motivi possibili, una macchina non conosce il proprio indirizzo IP, procede con il **Reverse Address Resolution Protocol** (RARP) emettendo un ***ARP-broadcast request*** ed indicando sè stesso come destinazione finale; sarà compito di alcuni server di rete autorizzati a fornire il servizio RARP, rispondere fornendo l'indirizzo richiesto.
Nella figura seguente è mostrato il protocollo RARP:

PROTOCOLLO ICMP (Internet Control Message Protocol)
Si trova sullo stesso livello di IP ma usa comunque IP per spedire i suoi dati. ICMP non aggiunge garanzie a IP, quindi è possibile che i datagrammi ICMP non arrivino a destinazione o che arrivino corrotti (esattamente come per IP). Il compito di ICMP è quello di inviare messaggi di servizio e messaggi di errore.

Si tratta di un meccanismo attraverso il quale i routers e gli utenti comunicano per sondare eventuali problemi o comportamenti anomali verificatisi in rete. Ricordiamo che il protocollo IP, di per sé, non contiene nessuno strumento per poter riscontrare, da parte della stazione sorgente né destinazione, la perdita di un pacchetto o il collasso di una rete.
L'**ICMP** consente una comunicazione straordinaria tra routers ed hosts permettendo lo scambio di segnali di errore o di controllo attraverso le interfacce software dell'internet, senza però arrivare su fino al livello degli applicativi; esso è una parte necessaria ed integrante dell'IP ed è contenuto nell'area dati di un datagramma IP.
L'ICMP include messaggi di ***source quench***, che ritardano il rate di trasmissione, messaggi di ***redirect***, che richiedono ad un host di cambiare la propria tabella di routing, e messaggi di ***echo request/reply***, che l'host può usare per determinare se la destinazione può essere raggiunta (**ping**).
Un ICMP ha tre campi di lunghezza fissa alla testa del messaggio: il ***type field*** (8 bits), che identifica il messaggio, il ***code field*** (8 bits), che contiene informazioni circa il tipo del messaggio, ed il ***checksum field*** (16 bits). I restanti campi del formato ICMP variano in base al tipo di messaggio.

X,25 Network E' una tecnologia che definisce l'interfaccia tra un computer e gli elementi della comunicazione di rete. Assicura la sicurezza nello scambio dati tra due macchine. I dati trasmessi devono arrivare in sequenza e senza errori. Quando i dati vengono trasmessi, sono salvati dal Network x,25 prima della fase di acknowledged. I messaggi vengono ritrasmessi dalla rete x,25 se non si riceve la conferma (ack). I dati vengono trasmessi attraverso simultanee connessioni.
X,25 Net è una delle molte tecnologie di rete per trasportare i datagrammi IP. IP utilizza il circuito x,25.

Rete	***Perché si possa avere una connessione con altri computer, è necessario inizialmente un supporto fisico, solitamente composto da un cavo e da interfacce di comunicazione. La connessione tipica in una rete locale è fatta utilizzando hardware Ethernet. Il cavo o i cavi e le schede Ethernet appartengono a questo livello.*** Lo strato rete immette sulla rete i frame in partenza e raccoglie quelli in arrivo. Prima di immettere sulla rete i frame, aggiunge ad essi una testata ed un controllo ciclico di ridondanza (CRC) per assicurare che i dati non siano corrotti durante il trasferimento. Un datagramma IP, quando viene passato al livello fisico, viene incapsulato in header Ethernet per formare un frame fisico. Il problema è che le dimensioni massime di questo frame sono limitate. Il valore di questo limite è chiamato MTU, maximum transfer unit. Se il datagramma IP è troppo grande per stare in una trama lunga al massimo MTU byte ? viene spezzettato in tanti frammenti abbastanza piccoli da entrare nel frame della rete. Ogni frammento possiede un proprio header molto simile all'header IP del datagramma originale, ma con i campi Identification, flags, Fragment Offset settati opportunamente. Quando i frammenti sono diventati nuovi datagrammi IP vengono inoltrati normalmente. Sul computer ricevente viene riassemblato il datagramma IP originale facendo uso di questi campi. La frammentazione è piuttosto fragile: la perdita di un solo frammento comporta la perdita dell'intero datagramma. In generale avere un frame molto grande permette di avereunamaggiore efficienza di trasmissione. Normalmente si cerca di evitare di dover ricorrere alla frammentazione. La lunghezza finale del datagramma dipende sia dollo spazzio occupato dagli header TCP e IP, che dalla lunghezza del segmento creato da TCP. Quando si usa una rete Ethernet bisogna aggiungere anche l'header di Ethernet, dove vengono aggiunti l'indirizzo Ethernet del mittente e del destinatario; bisogna fare attenzione: in Ethernet questo non è un indirizzo IP a 32 bit, ma quello della scheda di rete a 48 bit. Un indirizzo IP, 32 bit, viene indicato come 4 numeri decimali, ognuno esprime 8 bit es. 192,168,150,10. Un indirizzo IP a 32 bit può essere visto come una coppia di due numeri: il numero di rete e il numero di host o nodo. Il numero di bit usato per il numero di rete dipende dalla classe di indirizzo. Esistono cinque classi di indirizzi IP. Il numero di rete è assegnato da un ente centrale, l'InterNIC, il numero di host è invece deciso dal possessore di quel numero di rete. Quando il numero di host è fatto solo da 0, l'indirizzo esprime l'indirizzo di rete. Quando è fatto di soli 1, indica un broadcast a tutti i nodi della rete. Le reti possono essere LAN (locali – Local area Network), WAN (Wide area Network), MAN (Metropolitan area Network).

CONFRONTO TCP/IP – MODELLO OSI

<table>
<tr><th>Modello OSI</th><th>Modello TCP/IP</th></tr>
<tr><td>Applicazione</td><td rowspan="3">Applicazione</td></tr>
<tr><td>Presentazione</td></tr>
<tr><td>Sessione</td></tr>
<tr><td>Trasporto</td><td>Trasporto</td></tr>
<tr><td>Rete</td><td>Internet</td></tr>
<tr><td>Collegamento dati</td><td rowspan="2">Rete</td></tr>
<tr><td>Fisico</td></tr>
</table>

- nel modello TCP/IP gli strati ***fisico*** e ***collegamento dati*** sono fusi nello strato della ***rete***. In pratica non viene fatta alcuna distinzione tra la scheda di rete ed i loro driver, e questo consente di implementare il TCP/IP in qualsiasi topologia di rete.
- Lo strato ***Internet*** del TCP/IP, in cui viene implementato il protocollo IP, corrisponde allo strato di ***rete*** del modello OSI: entrambi si occupano dell'instradamento dei dati.
- lo strato di ***trasporto*** nei due modelli è analogo, ed entrambi permettono che tra i due host si stabilisca una sessione.
- lo strato dell'***applicazione*** TCP/IP, infine è il merge degli strati di ***applicazione***, ***presentazione*** e ***sessione*** del modello OSI

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 dimensioni adatte 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 identificare, 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 particolar per gestire i collegamenti transitori via modem, comprende meccanismi di auto-configurazione delle estremità del collegamento e di autenticazione.

Internet Protocol Addresses

Affinchè un sistema di comunicazione sia universale è necessario utilizzare un metodo di identificazione di ogni computer connesso ad esso (***host***). Il TCP/IP assegna ad ogni host, come identificatore universale, un **indirizzo binario** a 32 bits detto **Internet Address** o **IP Address**, usando una struttura analoga a quella degli indirizzi fisici di rete. L'indirizzo IP è formato:

- network number, il numero assegnato alla rete IP su cui si trova l'elaboratore
- host number, il numero assegnato all'elaboratore

Per rendere questi indirizzi più comprensibili, essi sono suddivisi in quattro gruppi di bits con i rispettivi valori scritti in decimale e separati da punti (***Dotted Decimal Notation***).
Concettualmente, ciascun indirizzo IP è una coppia **netid-hostid**, dove il ***netid*** identifica la rete dove è connesso l'host mentre l'***hostid*** identifica lo stesso host su quella rete, come mostrato in figura:

Gli indirizzi IP sono divisi in cinque classi, di cui tre primarie (**A**, **B**, **C**) distinguibili dai tre bit di ordine più alto.

- ***Classe A:*** usata per reti con più di 2 alla 16 (65536) hosts, dedica **7** bits per la ***netid*** e **24** per la ***hostid***.
  La classe A degli indirizzi IP utilizza gli 8 bit più a sinistra (il numero più a sinistra nella notazione puntata) per identificare la rete, lasciando gli altri 24 bit (o i restanti 3 decimali) per identificare gli host all'interno di essa.
  Negli indirizzi di classe A il bit più a sinistra del byte più a sinistra vale **sempre** zero - limitando l'intervallo dei valori del primo decimale della notazione puntata tra 0 e 127. Possono perciò esistere al più 128 reti di classe A, ciascuna delle quali in grado di ospitare 33544430 possibili interfacce.
  Gli indirizzi 0.0.0.0 (noto come "default route") e 127.0.0.1 (rete di "loop back") hanno un significato speciale e non sono utilizzabili per identificare una rete. In tal modo sono *disponibili* soltanto 126 indirizzi di classe A.

- ***Classe B:*** usata per reti con un numero di hosts compreso tra 2 alla 8 (256) e 2 alla 16 (65536) hosts, dedica **14** bits per la ***netid*** e **16** per la ***hostid***.
  La classe B degli indirizzi IP utilizza i 16 bit più a sinistra (i due byte più a sinistra) per identificare la rete, lasciando i restanti 16 bit (gli altri due byte) per identificare le interfacce. Negli indirizzi di classe B la coppia di bit più a sinistra vale 1 0. Questo lascia 14 bit per specificare l'indirizzo di rete con 32767 valori possibili. Le reti di classe B hanno quindi il primo decimale il cui valore varia tra 128 e 191 e le possibili interfacce sono 32766.

- ***Classe C:*** usata per reti con meno di 2 alla 8 (256) hosts, dedica **21** bits per la ***netid*** e **8** per la ***hostid***.
  La classe C degli indirizzi IP utilizza i 24 bit più a sinistra (i tre byte più a sinistra) per identificare la rete, lasciando i restanti 8 bit (il byte più a destra) a indirizzare le interfacce. I primi tre bit degli indirizzi di classe C sono sempre 110 permettendo di rappresentare i valori da 192 a 255. Sono disponibili quindi 4194303 indirizzi di rete, ciascuna delle quali in grado di

accogliere 254 interfacce (gli indirizzi di classe C con il primo byte maggiore di 223 sono comunque riservati e non utilizzabili).

- ***Classe D:*** è usata per la particolare distribuzione dei dati, detta ***multicasting***.

- ***Classe E:*** è destinata ad usi futuri.

Nella tabella seguente sono riportati i range della ***Dotted Decimal Notation*** corrispondenti a ciascuna classe degli indirizzi IP; alcuni valori sono riservati per scopi specifici (127.0.0.0 è riservato al local host):

Classe	**Lowest Address**	**Highest Address**
A	0.1.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Il numero di rete è assegnato da un ente centrale, l'InterNIC, il numero di host è invece deciso dal possessore di quel numero di rete. Quando il numero di host è fatto solo da "0", l'indirizzo esprime l'indirizzo di rete. Quando è fatto di soli "1", indica un broadcast a tutti i nodi della rete.
Dato che la suddivisione per classi è piuttosto grezza, è stato creato il concetto di subnet, o sottorete, che permette di sottrarre qualche bit dal numero dell'host in favore di una maggiore flessibilità di configurazione (ad esempio per separare il traffico in rete tramite un router), invisibile fuori dalla rete. In questo modo l'indirizzo è comorto da: un numero di rete, un numero di subnet, un numero di host.
Un indirizzo Ethernet, 48 bit, viene invece indicato con una notazione differente: 6 numeri esadecimali, ma ognuno di essi continua ad esprimere ancora 8 bit (8bitx6n=48bit), es. 20-53-52-b8-1f-00.
Ma cosa unisce l'indirizzo IP di una macchina con l'indirizzo fisico della scheda di rete di quella macchina? Nulla! E' per questo che hanno inventato un altro protocollo molto importante: **ARP**, Address Resolution Protocol.
Quando si assegna un indirizzo IP bisogna evitare i valori 0 e 255.
255 è il valore riservato nelle comunicazione broadcast, nelle reti LAN.
Il local host 127 è usato per testare il TCP/IP e per le comunicazioni tra client e server. Quando il programma usa il local host come destinazione il software protocollo nel computer rimanda i dati senza inviarli attraverso la rete.
Non possono essere usati numeri fatti tutti di zero o di uno.

Materialmente le reti sono interconnesse tramite computer molto veloci detti **router** che instradano i pacchetti leggendo l'indirizzo internet. Considerando che un router possa essere connesso a due o più reti fisiche, è necessario assegnare altrettanti indirizzi IP per identificare ciascuna rete; tali computers sono definiti ***multi-homed hosts***.
Poichè gli indirizzi IP codificano entrambi la rete e l'host ad essa connessa, essi non possono specificare un particolare computer, ma una "connessione" ad una rete. Perciò un router che connette ***n*** reti necessita di altrettanti indirizzi IP.
L'operazione di routing è molto efficace perché, in realtà, viene svolta leggendo solo la parte di indirizzo relativo alla rete.

Uno dei vantaggi della struttura di indirizzamento Internet è che la sua forma può specificare un indirizzo per un particolare host, una rete o tutti gli hosts su una rete (***Broadcast***). Lo svantaggio è che, se una macchina ha più indirizzi, la conoscenza di un indirizzo di rete potrebbe essere non sufficiente per raggiungerla, se tale rete non è disponibile.

Gli indirizzi IP appartengono alle Interfacce - NON agli host!
Per prima cosa, eliminiamo la causa di un errore fondamentale - gli indirizzi IP **non** sono assegnati agli host, ma bensì alle interfacce di rete presenti su un host.
Mentre molti (se non tutti) i computer di una rete IP avranno installata una singola interfaccia di rete (e avranno di conseguenza un singolo indirizzo IP), questo non accade sempre. Computer e altri dispositivi possono avere diverse (addirittura molte) interfacce di rete ciascuna delle quali con il proprio indirizzo IP.

Quindi un dispositivo con 6 interfacce attive (come un router) avrà 6 indirizzi IP - uno per ogni interfaccia connessa a una diversa rete. La ragione di ciò sarà chiara non appena daremo un'occhiata a una rete IP.

A dispetto di questo però, la gran parte della gente parla di ***indirizzo di questo host*** quando vuole riferirsi a un indirizzo IP. Ricordate soltanto che si tratta di un modo veloce per indicare ***l'indirizzo IP di questa interfaccia su questo host***. Molti (ma non la maggior parte) dei dispositivi in Internet hanno un'unica interfaccia e quindi un solo indirizzo IP.

Indirizzi IP come "Quartetti Puntati"
Nella loro implementazione corrente (IPv4), gli indirizzi IP consistono di 4 byte - e forniscono un totale di 32 bit di informazione disponibile. Sono numeri piuttosto grandi (anche se espressi in notazione decimale). Così per aumentare la leggibilità (ma anche per ragioni di organizzazione) gli indirizzi IP vengono normalmente scritti con la notazione puntata. L'indirizzo

```
192.168.1.24
```

ne è un esempio - 4 numeri (decimali) separati con un punto (.) l'uno dall'altro.

Dal momento che ciascuno dei quattro numeri è la rappresentazione decimale di un byte, ciascuno dei quattro numeri può rappresentare i valori compresi tra 0 e 255 (per un totale di 256 valori diversi - si ricordi cha anche lo zero è un valore).

Una parte dell'indirizzo indentifica la rete a cui un host appartiene, i restanti bit identificano l'host stesso (ehm - l'interfaccia di rete). L'esatta suddivisione tra bit usati per indirizzare la rete e quelli disponibili per identificare gli host (interfacce) in quella rete sono determinati dalla 'classe' della rete.

Indirizzi di rete, di interfaccia e di broadcast
Gli indirizzi IP possono avere tre differenti significati:

* rappresentare un rete IP (un gruppo di dispositivi IP che condividono l'accesso a un comune mezzo trasmissivo - come può accadere se sono tutti collegati dallo stesso segmento Ethernet). Un indirizzo di rete avrà sempre tutti i bit relativi allo spazio di indirizzamento delle sue interfacce impostati a 0 (a meno che la rete non sia in realtà una sottorete - come vedremo);

* l'indirizzo di broadcast di una rete IP (l'indirizzo usato per 'parlare' simultaneamente a tutti i dispositivi appartenenti alla rete). Gli indirizzi di broadcast presentano sempre tutti 1 nei bit dello spazio di indirizzamento destinato alle interfacce (a meno che la rete non sia in realtà una sottorete - come vedremo);
* l'indirizzo di una interfaccia (quale una scheda Ethernet o una interfaccia PPP su un host, su un router, su un server per la stampa ecc). Questi indirizzi possono avere qualunque valore nei bit per gli host, con **l'eccezione** di tutti 0 o tutti 1 - perché con tutti i bit per host a 0 l'indirizzo diventa un indirizzo di rete, mentre con tutti 1 diventa un indirizzo di broadcast.

Riassumendo per essere più chiari:

```
Per una rete di Classe A...
(un byte nello spazio di indirizzamento di rete seguito da tre
byte
per lo spazio destinato agli host)

        10.0.0.0 è un indirizzo di rete di classe A perché
                tutti i bit dello spazio destinato agli host sono
0
        10.0.1.0 è un host di quella rete
        10.255.255.255 è l'indirizzo di   broadcast di quella
rete
                perché tutti i bit dello spazio destinato agli
host
                sono 1

Per una rete di Classe B...
(due byte nello spazio di indirizzamento di rete seguito da due
byte
per lo spazio destinato agli host)

        172.17.0.0 indirizzo di classe B
        172.17.0.1 un host in questa rete
        172.17.255.255 indirizzo di broadcast

Per una rete di Classe C...
(tre byte nello spazio di indirizzamento di rete seguito da un
byte
per lo spazio destinato agli host)

        192.168.3.0 indirizzo di classe C
        192.168.3.42 un host in questa rete
        192.168.3.255 indirizzo di broacast
```

Tutti gli indiriizi di rete IP ancora disponibili per essere utilizzati oggi sono soltanto indirizzi di classe C.

Netmask e classi di rete

La funzione che codifica il ***network number*** e l'***host*** number nell'indirizzo ***IP*** è detta ***Network Mask*** (***netmask***); essa identifica quale porzione dell'indirizzo ***IP*** rappresenta il numero di rete e quale parte rappresenta l'indirizzo dell'***host***. Netmask è anch'esso un numero a 32 bit, i bit impostati a 1 indicano la porzione di rete dell'indirizzo ***IP***, quelli impostati a 0 sono relativi all'host dell'indirizzo. Per esempio, l'indirizzo 192.168.0.1 con una ***netmask*** di 255.255.0.0 ha come porzione relativa alla rete 192.168 e come indirizzo univoco dell'***host*** 0.1.
Ora, sfruttando le combinazioni della ***netmask*** si possono definire 3 classi di reti ***IP*** denominate "A", "B" e "C"; in realtà esistono altre due classi "D" ed "E", ma, siccome si tratta di classi riservate, non vengono prese in considerazione. La classe A è caratterizzata dal fatto che il primo bit è sempre impostato a 0, la classe B ha sempre indirizzi che cominciano con 10 (binario), la classe C con 110 (figura 3).

Una rete di classe A è rappresentata da una netmask 255.0.0.0 ovvero l'indirizzo di rete è rappresentato dai primo 8 bit (in realtà i primi 7 perché il primo è sempre 0), quindi possono esistere al mondo solo 126 reti di classe A. I rimanenti 24 bit servono per codificare gli ***host*** all'interno della rete, con 24 bit si possono codificare circa 2 milioni di macchine diverse quindi possono esistere pochissime reti di classe A (solo 126) ma di dimensioni enormi. La classe B ha un ***network*** number rappresentato dai primi 8+6 = 14 bit (due sono sempre fissi a 10) e quindi possono esistere circa 16000 reti, i rimanenti 16 bit permettono di avere circa 65000 host. Infine, le reti di classe C hanno l'***host*** number rappresentato dagli ultimi 8 bit e tutto il resto rappresenta la rete; quindi le reti di classe C possono contenere al massimo 254 macchine ciascuna però sono in numero molto elevato (circa 2 milioni).
Le ***netmask*** di default per le varie classi sono elencate nella figura 4; schematizzando, un indirizzo di classe A ha la forma N.H.H.H dove N sta per ***network*** ed H sta per host. Analogamente, un indirizzo IP di classe B ha la forma N.N.H.H, ed uno di classe C N.N.N.H.
Questo modo di classificare le reti IP provoca però la mancanza di una classe di rete appropriata per le organizzazioni di medie dimensioni. Infatti come detto, la rete di classe C, con un numero massimo di 254 indirizzi ***host***, risulta troppo piccola, mentre la rete di classe B che permette l'utilizzo di circa 65.000 indirizzo ***host*** è comunque troppo grande per risultare pratica.
Per risolvere tale problema, un approccio molto semplice consiste nel "prendere a prestito" un bit degli indirizzi per gli host e usarlo per gli indirizzi di rete; questo processo di prendere a prestito gli indirizzi per gli ***host*** e usarli per le reti è chiamato ***subnetting***. In altre parole il ***subnetting*** è l'atto di suddivisione di una rete IP in sottoreti più piccole e viene solitamente usato quando un'organizzazione ha un blocco di indirizzi che deve suddividere tra due o più siti fisicamente distinti tra loro.
Analogamente, per ottenere l'effetto opposto cioè raddoppiare le dimensioni di una rete, è sufficiente togliere un ***bit*** alla ***netmask*** in modo da avere più ***host*** a disposizione: questo meccanismo, che "espande" la rete, è detto ***supernetting*****.**
Ogni rete IP logica è identificata da una serie di indirizzi standard riservati, tra questi abbiamo l'indirizzo di base di rete (***network address***) e l'indirizzo di ***broadcast***. Il primo viene utilizzato per identificare la rete stessa ed è associato al numero più basso (con tutti i ***bit*** impostati a 0 nella porzione dell'***host***) nella rispettiva rete IP. Il secondo è invece uno speciale indirizzo sul quale tutti i dispositivi della rete IP si mettono in ascolto, ed è associato al numero più alto (con tutti i bit impostati a 1 nella porzione dell'***host***) nella

rispettiva rete IP. Ciò significa che gli indirizzi effettivamente utilizzabili sono sempre 2 in meno rispetto a quelli assegnabili.
Per fare un esempio, con una ***netmask*** pari a 255.255.255.0 ed un indirizzo di rete 192.168.1.x, allora l'indirizzo di base di rete è 192.168.1.0 e l'indirizzo di broadcast è 192.168.1.255, quindi rimangono 254 indirizzi assegnabili (da 1 a 254) anche se l'intervallo di indirizzi generabili è 0-255.
Oltre all'indirizzo di base di rete e all'indirizzo di ***broadcast***, è stato definito un blocco di indirizzi che non potranno mai essere direttamente connessi a nessuna delle reti pubbliche; uno di questi indirizzi di rete privati identifica la cosiddetta rete di ***loopback***, si tratta di una rete virtuale che punta allo stesso ***host*** dal quale il pacchetto è stato inviato. L'indirizzo più comunemente usato per la rete di ***loopback*** è 127.0.0.1.

Sottoreti
Una sottorete rappresenta un modo per prendere un singolo indirizzo di rete IP e suddividerlo **localmente** in maniera tale che questo stesso indirizzo possa essere utilizzato su diverse reti locali interconnesse. Si ricordi che un singolo indirizzo di rete IP può essere usato soltanto per una rete.

La parola chiave è **locale**: per tutto quanto riguarda il mondo che sta all'esterno rispetto alla macchine e alle reti fisiche coinvolte nell'operazione di realizzazione delle sottoreti a partire da un'unica rete IP, nulla è cambiato - il tutto viene visto ancora come un'unica rete IP. Questo concetto è importante - il "sub-networking" è una configurazione **locale** ed è invisibile al resto del mondo.

Una subnet viene utilizzata in tutti i casi in cui si ha un certo numero di hosts (cioè di computer) facenti tutti parte di uno stesso segmento di rete. Esempio tipico, la rete casalinga che molti di noi hanno, composta da uno o più PC “belli” (quelli più nuovi su cui si lavora di solito) ed uno, un po' più anzianotto, destinato alla gestione degli RTX e che svolge funzioni di router/server, collegati fra loro via ethernet. Utilizzando una subnet si semplifica notevolmente la realizzazione delle tabelle di routing, essendo immediato distinguere fra un indirizzo locale (cioè facente parte della subnet) ed uno esterno (per collegare il quale è quindi necessario passare attraverso il router).

Perché usare le sottoreti?

La ragione che sta dietro a questa soluzione risale alla prime caratteristiche di IP - quando una manciata di siti utilizzavano indirizzi di classe A permettendo a milioni di host di connettersi ad essi.

È evidente che si presenterebbero enormi problemi di traffico e di amministrazione se tutti i computer di un grande sito dovessero essere connessi alla stessa rete: provare a gestire un tale mostro sarebbe un incubo e la rete potrebbe (quasi certamente) collassare sotto il carico del suo stesso traffico (saturazione).

Adottando il "sub-networking": la rete di Classe A può essere suddivisa in diverse (anche molte) reti separate, l'amministrazione delle quali può facilmente a sua volta essere ripartita.

Questo consente di realizzare piccole reti, facilmente gestibili - in grado anche, in una certa misura, di utilizzare tecnologie differenti. Si ricordi che non si possono mescolare

Ethernet, Token Ring, FDDI, ATM ecc sulla stessa rete fisica - ma possono sempre essere interconnesse.

Altre ragioni per usare le sottoreti sono:

* La conformazione fisica di un sito può aggiungere delle restrizioni (lunghezza dei cavi) in termini di possibilità di collegamento delle infrastrutture, richiedendo reti multiple. Realizzando delle sottoreti l'eventuale suddivisione può essere fatta avendo a disposizione un solo indirizzo di rete IP.
Questa soluzione viene normalmente adottata da quegli ISP che desiderano fornire ai cliente un indirizzo IP statico per garantire una connessione permanente.
* Il traffico di rete è sufficientemente alto da causare significativi rallentamenti. Suddividendo la rete in sottoreti, il traffico locale a un segmento può essere mantenuto locale - riducendo il traffico generale e aumentando la velocità senza necessariamente aumentare la banda effettiva.
* Ragioni di sicurezza possono imporre che a classi diverse di utenti non sia consentito condividere la stessa rete - dal momento che il traffico su una rete può sempre essere intercettato da un utente riconoscibile sulla rete stessa. Il meccanismo delle sottoreti consente di impedire al dipartimento commerciale di ficcare il naso nel traffico del dipartimento Ricerca e Sviluppo (oppure consente di impedire agli studenti di fare lo stesso con la rete d'amministrazione dell'ateneo)!
* Possedete dispositivi che usano tecnologie di rete incompatibili tra loro, ma avete necessità di conneterle insieme (come già detto).

MESSAGE DIGEST 5 (MD5)
Permette di inviare un messaggio usando una chiave segreta. E’ usato con il TCP/IP per implementare un’autenticazione sicura. L’utente manda una userid all’host che può essere il server. Il server manda un messaggio all’utente. Viene così generata una chiava segreta. Per le trasnsazione client/server si utilizza MD5. I dati vengono criptati prima di essere inviati. I metodi sono criptazione simmetrica (unica chiave per criptare e decodificare) e criptazione asimmetrica (due chiavi o detto a chiave pubblica).