

Capitolo 8: Reti e Comunicazione

Dispense del corso di Tecnologia dei Sistemi Informatici: Basi di Dati e Reti

Queste brevi note non hanno la pretesa di essere un nuovo libro di testo sulle tecnologie informatiche. Vogliono invece costituire *un quaderno di appunti* agile del corso di TSI per gli allievi Ingegneri Gestionali dell'Università di Napoli Federico II.

Per questa sua natura e specificità, questa dispensa non è definitiva ed è soggetta a ulteriori revisioni individuate dalla data di compilazione del documento.

Draft del: 14 dicembre 2005

Contents

1	Introduzione	2
2	Caratteristiche Hardware delle reti	5
2.1	Reti Locali	5
2.2	Reti Geografiche	10
2.3	Interconnessione di Reti	14
3	Aspetti Software delle Reti	15
3.1	Il modello internet	19
3.2	Applicazioni di Rete	22
3.3	Le reti internet private	24

1 Introduzione

La storia dell'umanità ha registrato negli ultimi trecento anni l'introduzione di un nuove tecnologie che hanno modificato profondamente la vita dell'uomo. D'altra parte, come dice il filosofo Hannah Arendt, l'essenza di tutte le rivoluzioni è legata all'apparire di una "novità" nell'esperienza umana. Ciò è vero anche e soprattutto per le innovazioni tecnologiche, quali la rivoluzione industriale, favorita dalla nascita dei primi sistemi meccanici e dall'invenzione dei motori a vapore; senza dubbio gli ultimi cinquant'anni del secolo scorso sono stati invece caratterizzati dalle tecnologie dell'informazione e delle comunicazione. Nel secolo appena passato si sono via via diffusi a livello mondiale il sistema telefonico, la radio e la televisione, i computer ed i satelliti per telecomunicazioni. Queste tecnologie stanno rapidamente convergendo: la combinazione di elaboratori e sistemi di telecomunicazione, in particolare, ha avuto una profonda influenza sull'*organizzazione* dei sistemi di calcolo, passando, infatti, dal vecchio modello *mainframe - terminali* – in cui la potenza di calcolo è concentrata in un unico grande elaboratore a cui si accede per mezzo di un certo numero di terminali – a quello attuale in cui vi è un grande numero di elaboratori *autonomi ed interconnessi* fra loro. Sottolineiamo che autonomia significa, in prima battuta, che ogni sistema per poter portare a termine il suo compito non deve necessariamente rivolgersi ad un erogatore di servizi (server), mentre interconnessione significa che gli elaboratori devono essere capaci di scambiare informazioni, sfruttando un opportuno mezzo fisico. Possiamo allora dare una definizione *moderna* di rete.

DEFINIZIONE 1.1 RETE DI CALCOLATORI. *Una rete di calcolatori è un insieme interconnesso di calcolatori autonomi.*

Moltissimi sono gli usi delle reti di elaboratori, sia per le organizzazioni che per i singoli individui e ne elencheremo nel seguito i più importanti.

- condivisione risorse*: si possono rendere disponibili a chiunque programmi e informazioni anche distanti migliaia di km;
- affidabilità* si ottiene mettendo in rete sorgenti alternative delle risorse (ad es. duplicando le applicazioni e i dati su più computer). E' importante in sistemi che devono funzionare a tutti i costi (traffico aereo, centrali nucleari, sistemi militari, ecc.)
- diminuzione dei costi*: una rete di personal computer costa molto meno di un mainframe. A volte alcuni elaboratori sono più potenti ed offrono agli altri dei servizi (modello client-server, vedi figura).
- scalabilità* si possono aumentare le prestazioni del sistema aumentando il numero di elaboratori (entro certi limiti)
- comunicazione fra persone*: è possibile inviare messaggi, scambiarsi file, ecc.

Prima di introdurre le principali caratteristiche hardware e software delle reti, è necessario premettere una serie di concetti che in buona parte provengono dalla teoria più generale delle reti di comunicazione. Iniziamo anzitutto a distinguere tra le comunicazioni di tipo "broadcast" e quelle "punto a punto".

Le **reti broadcast** sono dotate di un unico "canale" di comunicazione che è condiviso da tutti gli elaboratori (vedi figura 1). In particolare, dei messaggi di breve lunghezza (spesso chiamati *pacchetti*) vengono inviati da un elaboratore e sono quindi ricevuti da tutti gli altri elaboratori. Per specificare chi è l'effettivo destinatario del messaggio, il trasmettitore specifica nel messaggio un "indirizzo" del destinatario, inteso, per ora, come un riferimento unico nel sistema del computer destinatario. Quando un elaboratore riceve un pacchetto, esamina l'indirizzo di destinazione: se questo coincide col proprio indirizzo, allora il pacchetto viene elaborato altrimenti viene ignorato. Le reti broadcast, in genere, 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.

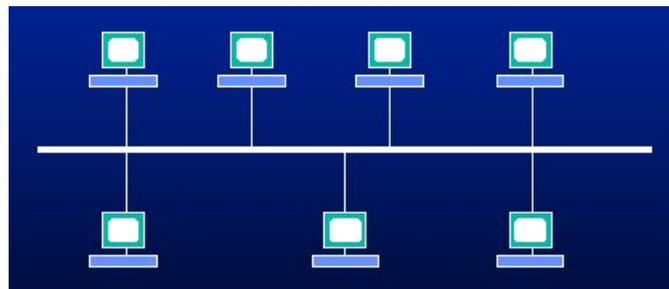


Fig. 1. Rete broadcast (a bus)

Le **reti punto a punto** consistono invece di un insieme di connessioni fra coppie di elaboratori (vedi figura 2). Per arrivare dalla sorgente alla destinazione, un pacchetto può dunque dover passare per uno o più elaboratori intermedi, e spesso esistono più cammini alternativi per arrivare da un sorgente ad un destinatario: si comprende, allora, intuitivamente il ruolo importante degli algoritmi di "instradamento" o "routing" in questo contesto. In generale, anche se non sempre è vero, le reti localizzate geograficamente tendono ad essere di tipo broadcast, mentre le reti molto estese tendono ad essere punto a punto.

Ulteriore differenza è spesso fatta sulla base del modello di elaborazione effettuata, ovvero il modello client-server e quello peer to peer. Una rete **client-server** è costituita da entità che richiedono dati, o client, e da entità che forniscono dati, o server.

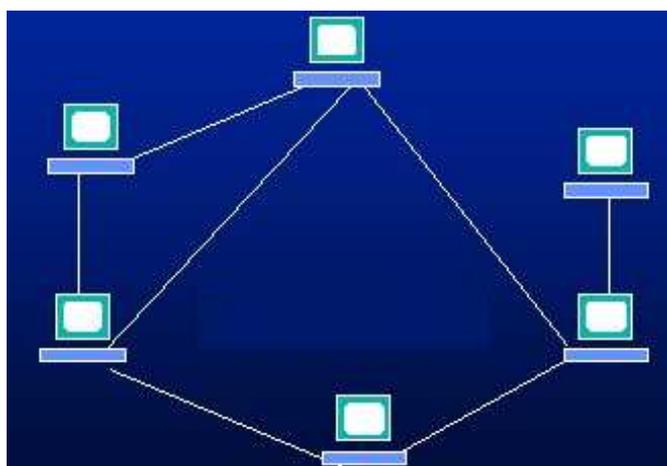


Fig. 2. Rete punto a punto

Distanza	Ambito	Tipo di rete
10 m	Stanza	Rete locale
100 m	Edificio	Rete locale
1 Km	Campus	Rete locale
10 Km	Città	Rete metropolitana
100 Km	Nazione	Rete geografica
1000 km	Continente	Rete geografica
10.000 km	Pianeta	Internet (Interconnessione di reti)

Table I. Tipi di Rete

Il server di solito è un calcolatore più potente che gestisce risorse condivise, come ad esempio stampanti, data base, file, programmi. Un client è di solito un elaboratore "leggero", poco potente (al limite - ma ciò accadeva soprattutto in passato - un terminale con tastiera e schermo). Nelle reti **peer to peer** la filosofia è completamente differente: tutti gli elementi della rete sono allo stesso livello ed i calcolatori della rete comunicano direttamente gli uni con gli altri senza far riferimento ad un server. In altri termini un computer può fungere in un'architettura P2P sia da client che da server a seconda delle necessità.

Una classificazione delle reti su base dimensionale è fornita in tabella 1, dove si può evidenziare una distinzione tra reti locali, reti metropolitane e reti geografiche come dettaglieremo nei prossimi paragrafi.

2 Caratteristiche Hardware delle reti

2.1 Reti Locali

Le reti locali, o *Local Area Network*, **LAN**, sono reti in genere possedute da una singola organizzazione (*reti private*) ed hanno un'estensione che arriva fino a qualche km, all'interno di un singolo edificio o di un campus (si ricordi che allo stato non si può, di norma, posare cavi sul suolo pubblico).

Le LAN sono molto usate per connettere tra di loro Personal Computer e/o workstation. Esse si distinguono dagli altri tipi di rete per tre caratteristiche: (i) hanno una dimensione ridotta; (ii) usano una tecnologia trasmissiva a broadcast; (iii) hanno una "topologia" classicamente a *stella*, *bus* o ad anello (*ring*). Si ricorda che con il termine topologia si fa riferimento alle strutture architettoniche che rappresentano la disposizione dei cavi della rete e il conseguente interfacciamento delle postazioni.

Nella **topologia a stella**, il ruolo centrale della trasmissione è svolto da un dispositivo o insieme di dispositivi chiamati *centri stella* (vedi figura 3) o *hub*, ripetitori che semplicemente inviano le informazioni che ricevono a tutte le porte collegate. L'hub permette la comunicazione tra i vari computer fornendo un sistema di connessione comune e localizzato ("concentrato"). Gli hub possono essere disposti a cascata in modo da espandere la rete in modo progressivo. Nelle reti con topologia a stella i pacchetti che vengono inviati da un elaboratore ad un altro sono ripetuti su tutte le porte del centro stella: questo permette a tutti i PC di vedere qualsiasi pacchetto inviato sulla rete. La topologia a stella consente un controllo centralizzato (grazie agli hub) delle comunicazioni con prestazioni elevate per le connessioni; come rovescio della medaglia, si possono verificare dei punti critici nella linea, proprio in corrispondenza degli hub.

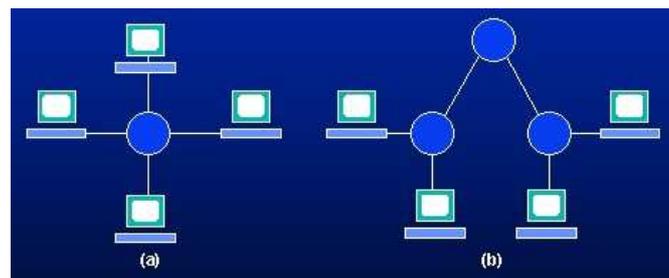


Fig. 3. Topologia a stella

Nella **topologia a bus** (vedi figura 1), in ogni istante un elaboratore solo può

trasmettere, mentre gli altri devono astenersi: è dunque necessario un *meccanismo di arbitraggio*, centralizzato o distribuito, per risolvere i conflitti quando due o più elaboratori vogliono trasmettere contemporaneamente. In un arbitraggio centralizzato, una apposita apparecchiatura accetta richieste di trasmissione e decide chi abilitare, mentre nell' arbitraggio distribuito, ognuno decide per conto proprio.

Lo standard IEEE 802.3 (chiamato impropriamente **Ethernet**) è lo standard di riferimento per la trasmissione su reti broadcast, basate su un bus, con arbitraggio distribuito, operante a 10 oppure 100 Mbps (oggi anche a 1 Gbit/s e a 10 Gbit/s).

Più nel dettaglio, per risolvere una contesa si utilizza uno schema di accesso a canale condiviso detto **CSMA/CD**: *Carrier Sense Multiple Access Collision Detection*. Il principio di funzionamento di tale tecnica è estremamente semplice: quando una stazione presente sul canale deve trasmettere lo fa senza attendere alcuna autorizzazione. Se la trasmissione ha successo, cioè i dati trasmessi non "collidono" con quelli trasmessi da altre stazioni, bene; altrimenti la stazione è in grado di rilevare la collisione e provvede, in un secondo momento, a ritentare la trasmissione dei dati, fino a quando questa non ha successo (vedi figura 4).

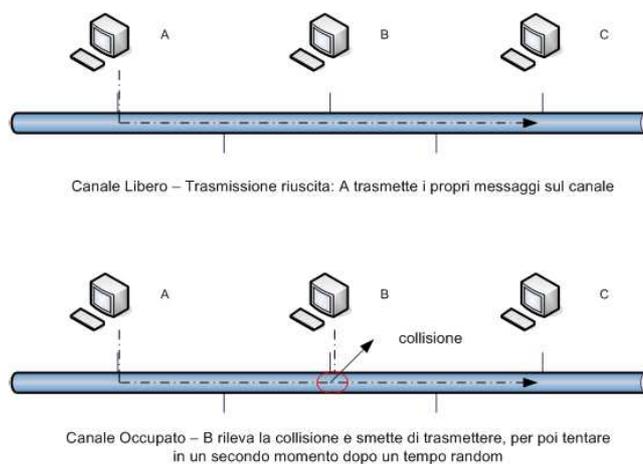


Fig. 4. CSMA/CD

In altri termini, ogni stazione della rete è *in ascolto* sul canale, e, non appena il canale è libero (lo si scopre individuando la presenza o meno di un segnale, onde il nome "carrier sense"), essa, qualora abbia informazioni da inviare, può iniziare a trasmettere. In generale, più stazioni sono in attesa di trasmettere (onde il nome

”*multiple access*”), e le diverse informazioni si possono propagare da diverse zone fino a collidere. Non appena le trasmissioni rilevano queste collisioni, si arresta il tentativo di trasmissione, si aspetta un tempo casuale e poi si riprova a trasmettere (nella figura presedente è il caso della stazione B), nel caso di mancata collisione, invece, la trasmittente può completare l’invio del messaggio (nella figura presedente è il caso della stazione A).

La topologia a bus è una topologia passiva nel senso che, le stazioni non concorrono in alcun modo alla trasmissione dei messaggi lungo la linea: esse rimangono solo in ascolto, nell’attesa o di inviare un messaggio o di ricevere un messaggio a loro destinato. Ciò conduce a diverse implicazioni, di cui due piuttosto importanti: se una stazione va in errore (o viene a mancare) il funzionamento del resto della rete non verrà alterato; se, però, il cavo venisse interrotto in un punto qualsiasi, la trasmissione e quindi la comunicazione, risulterebbe bloccata per l’intera rete. A suo vantaggio va inoltre citato anche il costo estremamente basso sia dei cavi che della connessione.

Nella **topologia a ring**, le macchine sono disposte lungo un anello (vedi figura 5) ed ogni bit-informazione ”circumnaviga” l’anello in un tempo tipicamente inferiore a quello di trasmissione di un messaggio. Anche qui è necessario un meccanismo di arbitraggio spesso basato sul possesso di un gettone (*token*) che abilita alla trasmissione. Più nel dettaglio, il diritto di trasmettere si basa sul continuo passaggio del token circolante fra le stazioni della rete: la stazione che ha il token può trasmettere (le altre si trovano in modalità di ascolto) fino al completamento dell’invio del messaggio; il gettone viene quindi passato alla stazione successiva che passa allo stato di trasmissione se ha qualcosa da trasmettere, altrimenti passa, a sua volta, il token alla stazione che la segue nell’anello. Si noti che il token altro non è che un insieme di bit con particolare configurazione che circola continuamente sull’anello.

In figura 6 sono mostrate le due diverse modalità operative in cui può trovarsi una stazione nella topologia ad anello. Nel primo caso la stazione è in modalità di ascolto e quindi riceve i messaggi e li ritrasmette, senza alterarli, sull’anello; nel secondo caso la stazione è in modalità di trasmissione, quindi una volta ricevuto il token, genera i messaggi da trasmettere e li invia sull’anello.

Questo è un tipo di rete in cui le stazioni hanno un ruolo attivo poichè ognuna di loro agisce anche come trasportatore di segnale poichè riceve dati dalla stazione che la precede e trasmette dati a quella seguente. Tecnicamente, la topologia ad anello è un continuo punto-punto circolare tra tutte le stazioni della rete. Di conseguenza, l’anello può diventare inutilizzabile in caso di malfunzionamento delle schede d’interfaccia delle singole stazioni o nel caso di un’eventuale interruzione della continuità elettrica sul cavo di collegamento.

Lo standard IEEE 802.5 (derivante dalla rete IBM Token Ring) è lo standard di riferimento per reti broadcast basate su ring, con arbitraggio distribuito, operante a 4

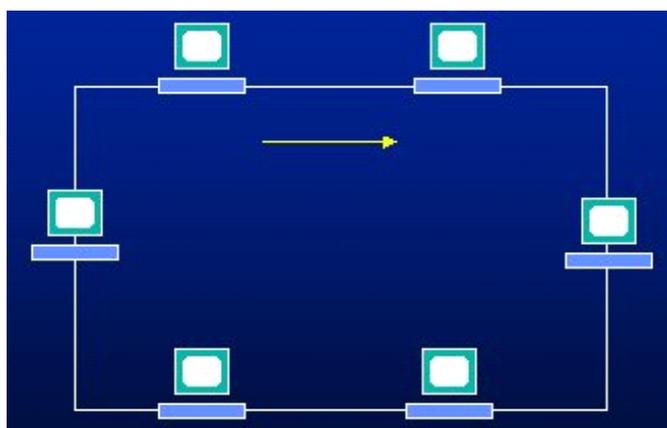


Fig. 5. Topologia ad anello

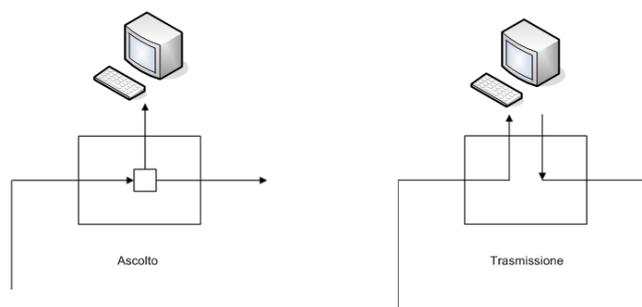


Fig. 6. Modalità di ascolto e trasmissione in una rete ad anello

o 16 Mbps.

A titolo di esempio, mostriamo infine di seguito le classiche componenti di una rete locale, come anche mostrato dalla figura 7:

—*sistema di cablaggio*: è il sistema fisico di interconnessione costituito dai cavi (UTP o STP, coassiali, fibre ottiche) o connessioni wireless (onde radio) che permetta il collegamento fisico tra i vari computer che compongono la rete. Il cablaggio segue norme ben precise – cablaggio strutturato – (ad esempio, TIA/EIA 568B, ISO/IEC 11801 ed EN 50173), a cui si fa in genere riferimento per quanto riguarda l'installazione dei cavi, la topologia della rete, i mezzi trasmissivi, le tecniche di identificazione dei cavi, la documentazione e le caratteristiche tecniche dei prodotti

impiegati.

Il sistema di cablaggio comprende di solito un cosiddetto *cablaggio di dorsale*, che collega diversi edifici (dorsale di campus) e piani di differenti edifici (dorsale di edificio), di solito in fibra ottica, e *cablaggio di piano* che partendo da un armadio tecnologico contenente concentratori raggiunge tutti i vari posti di lavoro, realizzando una *topologia a stella*. Il sistema di cablaggio condiziona, in modo a volte determinante, la velocità e le prestazioni di una rete.

- Server e Workstation*: i servizi utente di una rete sono offerti da macchine che ricoprono ruoli specifici e che sono denominati, come già accennato, server. In particolare, i servizi relativi a programmi, dati e file in genere, sono offerti dai file server. Su queste macchine risiedono, di norma, le risorse che devono essere condivise da tutti gli utenti. Altri servizi comunemente disponibili sono i servizi di stampa (print server) e quelli di comunicazione (fax server, communication server, etc.). Una singola macchina può offrire più di un servizio per cui, ad esempio, una macchina può essere contemporaneamente file-server e print-server. L'alta specializzazione dei server, ossia uno per ogni servizio, è giustificabile solo in quelle installazioni in cui, il particolare servizio presenta un volume di operazioni talmente elevato, nell'unità di tempo, da portare rapidamente alla saturazione un'unica macchina nel caso in cui coesistessero anche altri servizi. Gli utenti accedono ai servizi offerti dai server dalle proprie stazioni di lavoro (denominati anche: workstation, stazioni client o semplicemente client). In linea di principio, non c'è nessun motivo per cui le stazioni di lavoro siano concettualmente diverse dai server di una rete: entrambi sono computer che possono essere in tutto e per tutto uguali, salvo che per il loro utilizzo: la differenza tra server e stazioni di lavoro, in linea di principio, è nel software di base delle macchine (il sistema operativo). Nella realtà si preferisce - per motivi di efficienza, prestazioni e sicurezza - che i server siano macchine mediamente più potenti delle relative stazioni di lavoro il cui carico di elaborazione sia inferiore, nelle normali applicazioni, a quello dei server.
- schede di rete*: per creare una rete, occorre installare su ogni elaboratore una scheda di rete che permetta al computer di inviare e ricevere messaggi, via cavo o via onde radio.
- dispositivi condivisi*: stampanti, scanner, dispositivi di memorizzazione di massa e altre periferiche a seconda delle esigenze degli utenti.

2.2 Reti Geografiche

Le reti geografiche o *Wide Area Network*, **WAN**, si estendono a livello di una nazione, di un continente o dell'intero pianeta.

Per introdurci alle principali aspetti tecnologici legati alle reti, prendiamo consideriamo una rete di comunicazione *planetaria* di uso comune, la rete telefonica. La rete

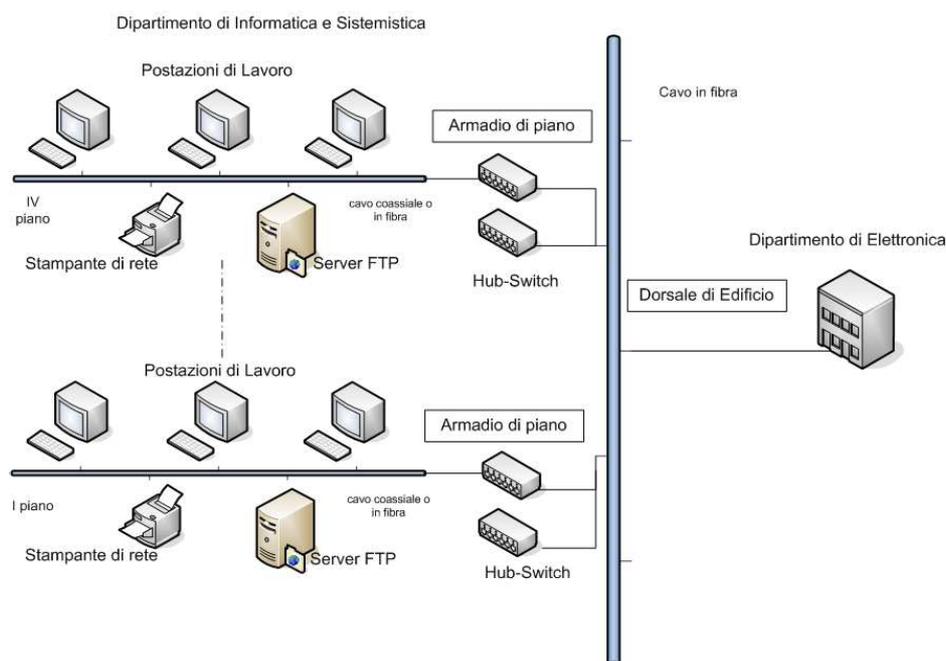


Fig. 7. Componenti di una rete locale

è disegnata in questo modo: esiste un distretto telefonico che contiene una centrale di smistamento, che comunica con le centrali degli altri distretti. Quando facciamo una telefonata, la chiamata viene fatta passare attraverso una o più centrali, fino a raggiungere il numero chiamato: le centrali *costruiscono* una connessione diretta fra i due telefoni, che dura per tutto il tempo della telefonata. In altre parole, viene creato un circuito virtuale che unisce i due telefoni all'atto della chiamata: per questo, tale tipologia di comunicazione viene anche detta a "commutazione di circuito", in quanto il canale viene "costruito" per ogni nuova sessione di comunicazione, collegando singoli tratti di linee dedicate come evidenziato in figura .

E' chiaro che la soluzione adottata per le reti telefoniche non si adatta bene alle comunicazioni tra elaboratori: si utilizza in questo caso, infatti, un diverso tipo di commutazione detta "a pacchetto".

Nella "commutazione a pacchetto" (*packet switching*), ogni messaggio è diviso in tanti elementi di dimensione fissa detti *pacchetti* e opportunamente numerati. Ogni pacchetto contiene altresì l'informazione relativa all'indirizzo del computer desti-

natario e a quello del mittente e viene trasmesso separatamente, facendo virtualmente una strada diversa dagli altri pacchetti del messaggio per arrivare al destinatario. Si noti, allora, che i pacchetti non arrivano necessariamente nello stesso ordine con cui sono stati inviati: per questo il destinatario deve aspettare la ricezione di tutti i pacchetti per poterli poi ricomporre e ricostruire il messaggio (vedi figura 8). Una rete di comunicazione che è basata su questo principio viene anche detta *punto a punto*, o *store and forward*.

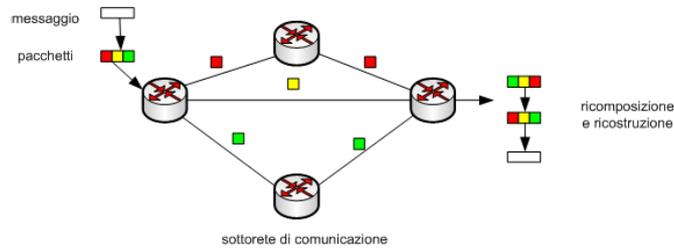


Fig. 8. Commutazione di pacchetto

Una WAN, dunque, è costituita di due componenti distinte: un insieme di elaboratori detti *host* oppure *end system* ed una *communication subnet* (o subnet). A sua volta, la subnet consiste di due componenti: *linee di trasmissione* (dette anche circuiti, canali, trunk) ed elementi di commutazione (*switching element*), detti anche "sistemi intermedi", oppure "nodi di commutazione" o anche "**router**".

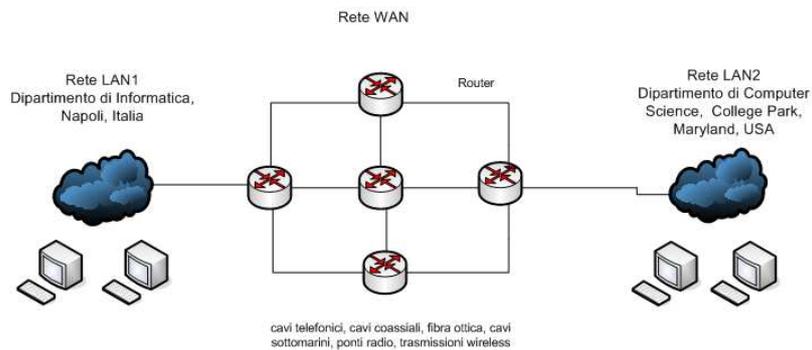


Fig. 9. LAN collegate da una WAN

Come mostrato in figura 9, una WAN è usata per connettere più LAN tra di loro.

In generale una WAN contiene numerose linee (spesso telefoniche) che congiungono coppie di router. Ogni router allora deve:

- (1) ricevere un pacchetto da una linea in ingresso;
- (2) memorizzarlo in un buffer interno;
- (3) instradare il pacchetto appena la necessaria linea in uscita è libera: ogni nodo, infatti, mantiene una tabella che indica a quali vicini ritrasmettere un pacchetto non destinato a lui, in base all'indirizzo di destinazione del pacchetto;

Si noti che la scelta del nodo a cui inoltrare il pacchetto dipende anche da situazioni temporanee di carico della rete, da guasti eventuali e così via. In altri termini ogni router monitora la rete calcolando la distanza che lo separa dai router vicini, e, di conseguenza la sua tabella di instradamento risulta dinamica e viene costruita in maniera tale da fare seguire ad ogni pacchetto la strada più veloce per raggiungere la rispettiva destinazione mediante l'ausilio di appositi e sofisticati algoritmi di instradamento.

L'instradamento dei pacchetti può seguire due approcci diversi:

- approccio a datagrammi*: in questo caso i pacchetti sono trattati in modo indipendente l'uno dall'altro: se per qualche motivo il destinatario al momento della ricostruzione del messaggio si accorge che un pacchetto è alterato o mancante, allora chiede la ritrasmissione di questo pacchetto;
- approccio a circuito virtuale*: in questo caso, prima della spedizione dei pacchetti si stabilisce un cammino "virtuale" tra sorgente e destinatario per semplificare l'instradamento dei pacchetti, scomparendo col pacchetto finale della comunicazione.

Tra i router si adoperano molte topologie di interconnessione, con differente ridondanza di connessione (in figura 10 ne sono mostrate alcune):

- (1) *a stella* (ridondanza zero);
- (2) *ad anello* (ridondanza zero);
- (3) *ad albero* (ridondanza zero);
- (4) *maglia completa* (ridondanza massima);
- (5) *anelli intersecati* (ridondanza minima);
- (6) *maglia incompleta* (ridondanza media).

Per concludere, citiamo le reti metropolitane (*Metropolitan Area Network, MAN*), che hanno un'estensione tipicamente urbana. Per le reti metropolitane è stato introdotto uno standard apposito, IEEE 802.6 o DQDB, che prevede l'esistenza di un mezzo trasmissivo di tipo broadcast (due bus 802.6) a cui tutti i computer sono attaccati.

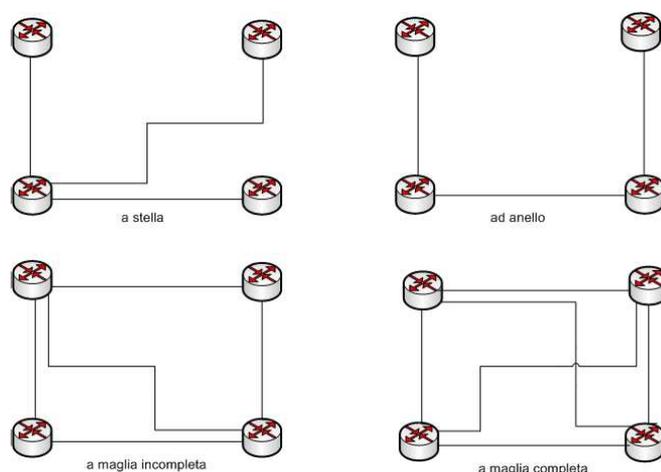


Fig. 10. Topologie di interconnessione

2.3 Interconnessione di Reti

Con il termine *internetworking* ci si riferisce all'insieme di norme tecniche, protocolli e dispositivi che consentono la connessione di due o più reti "eterogenee". Una *internetwork* è quindi formata quando reti diverse (sia LAN che MAN o WAN) vengono collegate fra loro.

Alcuni problemi però sorgono inevitabilmente quando si vogliono connettere fra di loro reti progettualmente diverse (spesso incompatibili fra loro). In questo caso si deve ricorrere a speciali attrezzature, dette *gateway* (o *router multiprotocollo*), che oltre ad instradare i pacchetti da una rete all'altra, effettuano le operazioni necessarie per rendere possibili tali trasferimenti.

Oltre al *router*, per l'interconnessione delle reti si utilizzano altri dispositivi che citeremo brevemente:

- repeater*: è un dispositivo che collega reti LAN identiche e fornisce la possibilità di "rigenerare" i segnali in transito tra una rete e l'altra, amplificandoli (in tal modo è possibile estendere l'area della rete);
- bridge*: è un dispositivo che collega reti diverse aventi però uno stesso schema di indirizzamento; di solito il bridge rimane in ascolto sulle due reti che connette e, quando riconosce un pacchetto proveniente da una rete e destinato a una stazione appartenente all'altra rete, lo preleva, lo memorizza e lo ritrasmette con il metodo

di accesso proprio della rete di destinazione (viene di solito usato per connettere reti LAN con tecnologia diversa, e.g. reti token-ring con reti ethernet);

—*gateway*: è un dispositivo che crea collegamenti tra reti con ambienti applicativi differenti.

In figura 11 è mostrato un esempio di internetworking.

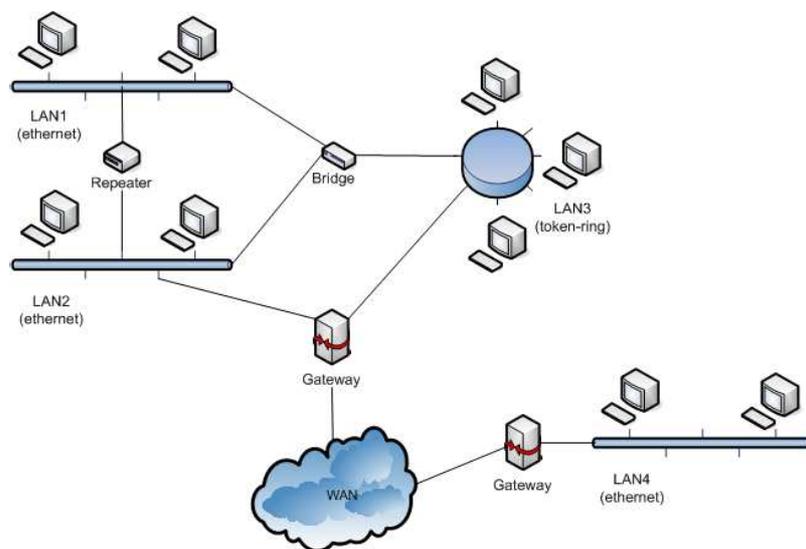


Fig. 11. Internetworking

3 Aspetti Software delle Reti

Dopo aver mostrato quelle che sono le connessioni fisiche tra calcolatori, dobbiamo cercare di capire come farli comunicare dal punto di vista del "software". Gli elaboratori, infatti, devono seguire alcune regole dette **protocolli di comunicazione**. Un protocollo stabilisce le regole di comunicazione che debbono essere seguite da due interlocutori.

Consideriamo il classico esempio del colloquio tra due persone che si parlano al telefono: le prime frasi scambiate (pronto? chi parla? Sono Carlo, con chi parlo?) costituiscono un esempio di regola in cui gli interlocutori stabiliscono la loro identità prima di iniziare un colloquio vero e proprio.

Per protocollo di comunicazione tra due elaboratori si intende, più precisamente, un insieme di regole che permette la corretta instaurazione, mantenimento e terminazione di una comunicazione di qualsiasi tipo tra due o più entità. Per questo motivo, il protocollo deve poter definire la sintassi da seguire (il formato del messaggio), e l'ordine dello scambio di messaggi.

Data la complessità del problema derivante dal problema della comunicazione tra gli host di una rete, più che un protocollo, in realtà, si definiscono famiglie di protocolli, in cui ogni protocollo *gestisce univocamente* una componente ben definita della comunicazione *condividendo* con gli altri protocolli *i dati* di cui essi necessitano.

L'architettura dei protocolli è organizzata a livelli. Lo scopo di ogni livello – come consuetudine di ogni sistema fatto a strati – è di *fornire servizi alle entità del livello immediatamente superiore*, mascherando il modo in cui questi sono implementati e *sfruttando opportunamente i servizi* che gli vengono a sua volta forniti *dal livello immediatamente inferiore*, come mostrato in figura 12.

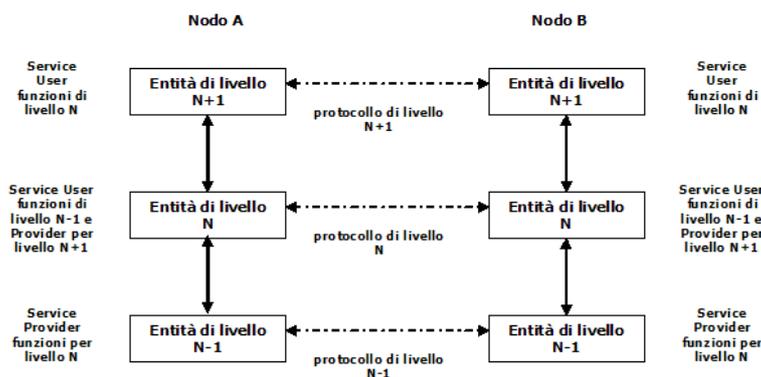


Fig. 12. Architettura a livelli

Per quanto attiene la comunicazioni tra computer, cerchiamo anzitutto di comprendere quali sono gli "strati" fondamentali da considerare, in quanto una visione a livelli permette di semplificare notevolmente il problema della comunicazione.

A tal fine, pensiamo alla seguente analogia umana (vedi figura 13), nella quale un *filosofo indiano* vuole conversare con uno *stregone africano*, sapendo che il filosofo indiano parla solo l'hindi, mentre lo stregone africano solo lo swahili. C'è allora bisogno di due traduttori, che hanno parlato una lingua in comune tra di loro, ad

esempio l'inglese: un traduttore traduce da hindi in inglese ed un traduttore da swahili in inglese. Dopo aver fatto la traduzione, si inviano quanto tradotto su un mezzo fisico, ad esempio via fax. Dal punto di vista logico, il filosofo dialoga con lo stregone, il traduttore indiano con il traduttore africano, e il fax indiano con il fax africano.

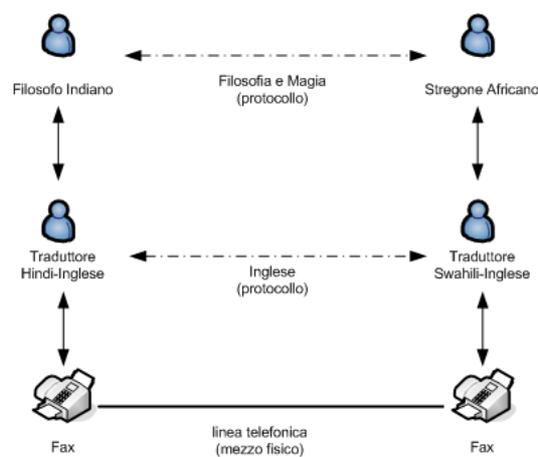


Fig. 13. Problema della comunicazione

Dall'esempio fatto notiamo anzitutto che per comunicare è necessaria l'esistenza di un *canale fisico* di comunicazione, ovvero di una infrastruttura che permetta di scambiare segnali tra le due entità della comunicazione. A ciò occorre aggiungere la conoscenza da parte del trasmittente e del ricevente dei *protocolli di trasmissione*, ovvero di regole che permettono di interpretare i segnali scambiati. Infine, è necessario concordare delle regole che permettono di dare una interpretazione ai segnali scambiati (*protocollo applicativo*). Si noti che dal punto di vista dell'utente finale, le soluzioni adottate per i diversi "livelli" della comunicazione devono essere completamente trasparenti. Le entità (processi) che effettuano tale conversazione si chiamano *peer entity* (entità di pari livello). Il dialogo fra due peer entity di livello n viene materialmente realizzato tramite i servizi offerti dal livello precedente e virtualmente mediante il protocollo applicativo definito allo stesso livello, mentre il dialogo tra peer entity dello stesso host avviene sfruttando apposite interfacce di comunicazione (vedi figura 14).

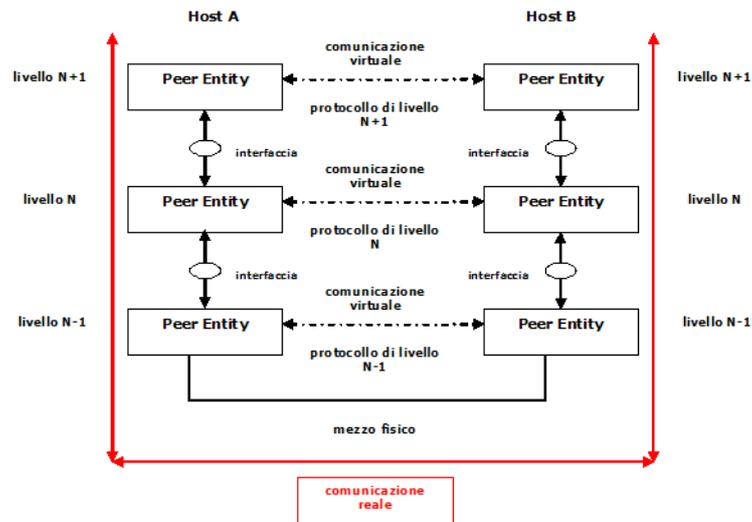


Fig. 14. Comunicazione tra host

Nell'esempio mostrato in figura i protocolli applicativi potrebbero essere quelli di livello N e livello $N + 1$, mentre il protocollo di trasmissione coincide con quello di livello $N - 1$.

Dato che i protocolli devono essere usati da tutti gli elaboratori, essi sono definiti da organismi internazionali di standardizzazione. Il più famoso è l'ISO (International Standard Organization) che ha proposto lo standard OSI (Open System Interconnection) per la schematizzazione a livelli di un'architettura di rete con l'obiettivo di garantire l'*interoperabilità* tra vari sistemi.

I livelli del protocollo ISO-OSI, mostrati in figura , sono i seguenti:

- (1) *Livello Fisico (Physical Interface Layer)*: è preposto alla gestione degli aspetti fisici della comunicazione, dei meccanismi di collegamento ed offre ai livelli superiori funzionalità indipendenti dal mezzo trasmissivo utilizzato.
- (2) *Livello dei collegamenti dei dati (Data Link Control)*: si occupa della correttezza del trasferimento dei dati (suddivisione dei pacchetti in frame, rilevazione e correzione di errori, controllo del flusso dei pacchetti).
- (3) *Livello di rete (Network Layer)*: si occupa del controllo della congestione della rete e gestisce e controlla il routing.
- (4) *Livello di trasporto (Transport Layer)*: ha lo scopo di segmentare una unità di trasmissione in messaggi fisici di uguale grandezza (pacchetti) e di garantire l'affidabilità della comunicazione (controllo flusso dei messaggi).
- (5) *Livello sessione (Session Layer)*: si occupa di aprire e chiudere il dialogo tra gli elaboratori.
- (6) *Livello di presentazione (Presentation Layer)*: si occupa di convertire codici e formati tra il mittente ed il destinatario del messaggio.
- (7) *Livello applicazione (Application Layer)*: è responsabile di offrire servizi telematici generalizzati tra cui, ad esempio, la posta elettronica ed il trasferimento dei file.

A partire dal livello 4 le comunicazioni tra vari peer entity diventano di tipo "host to host (end to end)", in altri termini a questo livello è completamente nascosta l'infrastruttura di comunicazione fisica sottostante.

3.1 Il modello internet

Differentemente dal modello teorico OSI, il modello "Internet" è impostato su un'architettura a 5 livelli (vedi figura 16):

- (1) *Livello fisico (Physical Interface Layer)*: funge da interfaccia fisica tra le stazioni e il mezzo fisico di comunicazione per la trasmissione dei dati.
- (2) *Livello di accesso alla rete (Medium Access Control Layer)*: regola lo scambio dati fra un sistema finale e la rete a cui è collegato, specificando come organizzare i dati in frame e come trasmetterli sulla rete.
- (3) *Livello internet (Internet Layer)*: si occupa dello scambio di dati tra sistemi che non appartengono alla stessa rete. In particolare, a tale livello si trova l'Internet Protocol (IP) che definisce le procedure per l'attraversamento di reti multiple

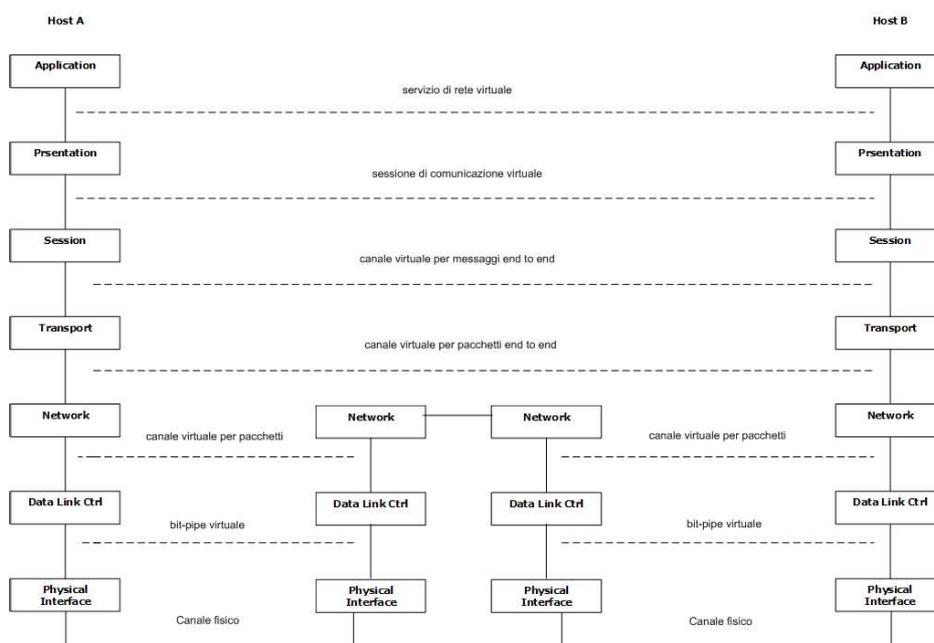


Fig. 15. Modello ISO/OSI

interconnesse. Più nel dettaglio, esso specifica il formato dei pacchetti inviati attraverso la rete e i meccanismi utilizzati per farli transitare dal calcolatore sorgente attraverso uno o più router e verso il destinatario (instradamento o routing).

- (4) *Livello di trasporto (Transport Layer)* (host to host): a tale livello i messaggi provenienti dai livelli superiori sono segmentati (e riassemblati quando giungono dai livelli inferiori) in pacchetti. Il protocollo base di tale livello, il Transmission Control Protocol (TCP), garantisce inoltre che i pacchetti siano trasmessi in modo affidabile, con la garanzia che tutti giungano a destinazione nello stesso ordine di partenza (controllo del flusso).
- (5) *Livello di applicazione (Application Layer)*: (host to host) specifica come un'applicazione può utilizzare l'insieme dei protocolli TCP/IP comunicando cooperativamente con calcolatori differenti.

Il successo di questa architettura si deve al fatto che è stata ed è un'eccellente piattaforma per la realizzazione di applicazioni di rete affidabili ed efficienti ed ha permesso da subito di condividere informazioni tra organizzazioni diverse. Il TCP/IP, in-

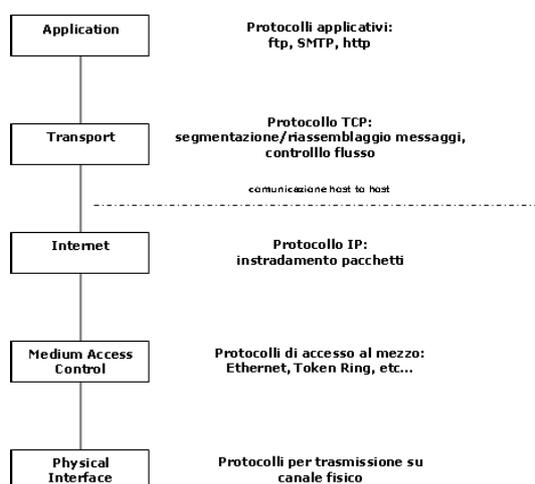


Fig. 16. Modello Internet

oltre, è stato implementato in quasi tutti i sistemi operativi di rete ed è stato supportato dalle grandi case costruttrici di apparati attivi di rete.

In TCP/IP l'indirizzamento è su due livelli, *l'indirizzo IP e la porta TCP*. L'indirizzo IP è un indirizzo globale unico associato a ogni calcolatore collegato ad una *sub-net* e viene utilizzato da IP per l'instradamento e la consegna dei pacchetti; *la porta TCP* è invece un indirizzo unico all'interno dell'host e viene usato da TCP per consegnare i dati, magari aggiungendovi altre informazioni di controllo, alla particolare applicazione interessata.

Gli indirizzi IP sono orientati alla macchina e sono difficili da utilizzare dagli esseri umani. Per questo motivo è stato definito un sistema per passare da *indirizzi IP numerici a nomi* facilmente memorizzabili: il **Domain Name System** associa a ogni indirizzo IP uno o più indirizzi simbolici, gestendone la conversione.

Per questo gli indirizzi IP sono organizzati in maniera gerarchica (domini, sotto-domini, sotto-sotto-domini). Il nome simbolico di un elaboratore è costituito da una successione di stringhe alfanumeriche separate da punti (per esempio, `picariello.labadam.unina.it`) dove ogni stringa identifica un "dominio": la stringa più a destra rappresenta il dominio di primo livello (detto anche dominio generale) e identifica *la nazione di appartenenza* (**it** per Italia, **uk** per Gran Bretagna, **de** per Germania, ad esempio) o identifica la categoria cui appartiene la società proprietaria del calcolatore (**com** per commerciale, **edu** per università o istituzioni che si occupano di formazione, **org** per organizzazioni non-profit di vario genere); la seconda

stringa, indica il dominio di secondo livello, ovvero un sottodominio del dominio di primo livello che di solito individua una singola organizzazione (università, azienda, ad esempio). Le stringhe successive indicano i domini di terzo livello (sottodomini dei domini di secondo livello), quelli di quarto il quarto livello, e così via finché non si arriva a individuare un dominio che comprende il singolo calcolatore.

A ogni dominio è associato a un calcolatore responsabile del dominio: per esempio, l'indirizzo `picariello.labadam.unina.it` prevede un computer responsabile per il dominio `it`, un computer per il dominio `unina.it`, un terzo computer per il dominio `labadam.unina.it` ed un ulteriore computer per `picariello.labadam.unina.it`. Il calcolatore responsabile di un dominio mantiene un elenco dei calcolatori responsabili dei suoi sottodomini (e ne conosce i relativi indirizzi IP): il calcolatore responsabile del dominio `it` deve sapere chi sono i calcolatori responsabili di tutti i suoi sottodomini (tra cui c'è `unisa.it`, ma anche `miur.it`); il calcolatore responsabile del dominio `unina.it` deve a sua volta sapere chi sono i calcolatori responsabili di tutti i suoi sottodomini (tra cui c'è `labadam.unina.it`, ma anche `mobilab.unina.it`) e così via. Per tradurre, allora, l'indirizzo DNS di un calcolatore nel suo indirizzo IP si deve interrogare il responsabile di ciascuno dei domini cui quel calcolatore appartiene.

3.2 Applicazioni di Rete

In questo paragrafo andremo ad illustrare i servizi applicativi più comuni offerti dai più diffusi modelli di rete. Molti dei servizi utente, e soprattutto il modo con cui sono presentati all'utente, dipendono non solo dall'insieme di protocolli usati per implementare la rete ma anche dal sistema operativo usato.

Le applicazioni che richiedono i servizi di rete, e che li rendono visibili ed utilizzabili all'utente, sono costituiti da processi che girano nel contesto del sistema operativo della macchina sulla quale si utilizzano. In generale i sistemi operativi "server" implementano questi servizi in maniera indipendente dal modello di client: l'utilizzo più o meno efficiente di questi servizi dipende quasi in maniera esclusiva dai sistemi operativi client. Nondimeno esiste un insieme minimo di servizi che devono essere assicurati e che, salvo deprecabili eccezioni, sono disponibili su quasi tutti i sistemi operativi utilizzati sui client di rete: è a questo insieme minimo che faremo riferimento nell'esposizione che segue.

—**HTTP** - il servizio HTTP, acronimo di HyperText Transfer Protocol, è un protocollo che regola lo scambio di ipertesti (pagine web) tra gli host presenti in Internet. E' il protocollo alla base del cosiddetto World Wide Web (WWW) che è un sistema di rappresentazione di informazioni basate sulle tecnologie ipertestuali. WWW ha portato il concetto di ipertesto, generalizzandolo sotto vari aspetti, su Internet dan-

do origine all'idea del villaggio globale dell'informazione su rete. WWW presenta le informazioni sotto forma di "pagine", dove una pagina può contenere del testo ordinario, immagini, filmati, suoni ed una serie di link ad altre pagine. Il software che permette di usufruire del servizio WWW e di visualizzare le pagine web viene, di norma, chiamato browser WWW o semplicemente browser. In sintesi, attraverso l'http, è possibile esplorare l'insieme delle pagine web (residenti su apposite macchine, denominate "HTTP Server"), da cui è costituito il WWW.

- FTP** - il servizio FTP, acronimo di File Transfer Protocol, è un protocollo che si utilizza per trasferire file tra computer collegati ad internet. Con l' FTP ci si può connettere a distanza ad un sistema remoto (" FTP server"), visualizzare i suoi archivi di file e trasferire file dal computer personale a quello remoto e viceversa. È il sistema più usato al mondo per pubblicare siti. Per trasferire files con FTP c'è bisogno di installare sul computer un programma ad hoc che viene quasi sempre fornito dai sistemi operativi che supportano il protocollo TCP/IP. Windows, ad esempio, include un client FTP nella sua installazione, ciononostante, anche in rete sono disponibili molti client FTP, molti dei quali openware o shareware.
- Telnet** - Il servizio di "terminale remoto virtuale" è forse il più tecnico tra i tools storici di Internet e pertanto successivamente superato dalle evoluzioni delle tecnologie informatiche che hanno portato allo sviluppo di tools di controllo remoto con un'interfaccia sempre più amichevole (servizi di desktop remoto). Telnet è un protocollo di comunicazione che consentiva all' utente generico di un computer, nodo della rete, di utilizzare la propria postazione di lavoro come terminale di un altro qualsiasi nodo (con un servizio di telnet abilitato) e permetteva così di controllare un computer a distanza. Fino alla diffusione dei personal computer, i "computer" utilizzati erano grosse stazioni di lavoro che, tramite il sistema operativo Unix, permettevano a più utenti di lavorare contemporaneamente utilizzando terminali differenti. In pratica, tramite Telnet si "entra" in un computer remoto (mediante un proprio login e una propria password), e nel caso si dispone di un'area personale (una parte del suo hard disk a propria disposizione), si potevano svolgere a distanza tutte le normali operazioni (eseguire programmi, leggere e spedire posta elettronica, copiare, cancellare, rinominare file...). Telnet è, quindi, differente da protocolli come HTTP o FTP, che permettono semplicemente il trasferimento di file sulla rete. Per poter accedere ad un computer remoto
- E-mail** - : La posta elettronica o e-mail realizza la versione elettronica del tradizionale sistema postale. Come sempre, per poter utilizzare un servizio di Internet, occorre disporre di due cose: un calcolatore connesso alla rete e che parli in Tcp/Ip e un prodotto software che fornisce l'interfaccia utente per utilizzare lo specifico servizio TCP/IP. Nella fattispecie della posta elettronica il prodotto software di e-mail (client di posta elettronica o mailer) deve consentire, dal punto di vista del mittente, di: (i)

scrivere una lettera in formato elettronico (dunque un banale word processor), (ii) specificare un mittente ed un destinatario su una sorta di busta elettronica, (iii) consegnare il messaggio alla rete per la trasmissione, e, naturalmente, dal punto di vista del destinatario di: (i) ricevere dalla rete il messaggio, (ii) leggere la lettera. Il tutto, come nel tradizionale servizio postale, deve avvenire in maniera asincrona tra i due attori della comunicazione (ovvero, il mittente deve poter scrivere e spedire la lettera senza preoccuparsi di cosa sta facendo il destinatario in quel momento e viceversa). In altri termini, la posta elettronica (e-mail) è un servizio di messaggistica personale, di norma protetto, che permette di facilitare le comunicazioni tra gli utenti. Per implementare un servizio simile è necessario che una macchina, detta mail server, agisca da gestore dell'ufficio postale, cui pervengono tutti i messaggi e dal quale sono inoltrati ai rispettivi destinatari. In questo tipo di servizio il sistema operativo si limita a fornire il supporto per un mail server e, nelle stazioni, per i mail client assicurando, quando possibile, la massima segretezza per i messaggi. La comunicazione tra client e i server di posta elettronica avviene attraverso due appositi protocolli applicativi denominato SMTP (Simple Mail Transfer Protocol) e POP (Post Office Protocol) che governano, rispettivamente, l'inoltro e la ricezione dei messaggi di posta.

3.3 Le reti internet private

L'introduzione di internet ha dato grande impulso ai sistemi informativi aziendali, proponendo soluzioni a basso costo ed efficaci simili al paradigma di internet. Una rete **intranet** è una rete privata interna ad una azienda che utilizza come l'infrastruttura classica di internet e del Web. Attraverso l'intranet, l'azienda consente ai propri dipendenti di accedere con rapidità alle informazioni interne aziendali e di condividere risorse utili per il proprio lavoro. A ciò si aggiunge che viste di quelle informazioni possono essere messe anche a disposizione dei clienti o di altri soggetti interessati. Sviluppando la tecnologia intranet, si può creare una rete **extranet** che offre un accesso esterno (ad esempio a fornitori o collaboratori aziendali) sicuro e controllato. Le reti extranet si sono molto diffuse per particolari applicazioni del business to business (b2b), come gli acquisti e le vendite.

Sia per le reti internet che per quelle intranet, la *sicurezza* è un requisito fondamentale. Una delle tecniche oggi più usate per prevenire accessi non autorizzati nelle reti è quella che si basa su firewall. Un **firewall** è un sistema hardware e software che blocca gli utenti non autorizzati impedendogli l'accesso alla intranet: ciò si ottiene costringendo tutti i pacchetti a passare attraverso una *porta* che regola i flussi di ingresso tra le reti, identificando gli utenti, filtrando eventuali virus e mettendo in essere altre sofisticate misure di controllo e sicurezza.