Dipartimento del Tesoro

Internet/Intranet

INDICE

1. Architettura e Protocolli

Una delle ragioni principali del successo di Internet va senza dubbio individuata nella efficienza e semplicità delle tecnologie che ne consentono il funzionamento. Come è noto nel mondo dell'informatica un ruolo importante è svolto dai programmi e dai protocolli : il software. Prima di procedere nel nostro viaggio attraverso Internet, dunque, è opportuno dare, anche da questo punto di vista, un'occhiata 'dentro la scatola'.
Non intendiamo certo trasformare questa documentazione in un manuale tecnico sui sistemi di internetworking: cercheremo solamente di introdurre i principi fondamentali delle tecnologie che garantiscono a Internet di funzionare in modo efficiente e sicuro.
Questa introduzione, se per un verso risponde alle esigenze di completezza a cui un manuale deve ottemperare, fornisce nondimeno al lettore alcune nozioni che debbono far parte del bagaglio di conoscenze di un utente 'esperto' della rete Internet. Un bagaglio indispensabile per sfruttarne al meglio le potenzialità; sapere come funzionano le cose, infatti, permette di individuare le cause di eventuali problemi o malfunzionamenti, e, se non sempre di risolverli, almeno di dare informazioni precise a chi dovrà intervenire.
Inevitabilmente, saremo costretti ad usare un certo numero di strane sigle, con le quali vengono di norma designati i sistemi su cui si basa la rete. Ma a questo è bene fare l'abitudine: il lessico di Internet è popolato di sigle (nella maggior parte acronimi, spesso molto creativi).

1.1 UN LINGUAGGIO COMUNE: IL PROTOCOLLO TCP-IP

Internet è uno strumento di comunicazione. Uno strumento di comunicazione tra i computer, e tra gli uomini che usano i computer interconnessi attraverso la rete. Naturalmente i due soggetti in campo, computer e uomini, hanno esigenze diverse, spesso contrastanti, che occorre tenere presenti per fare in modo che la comunicazione vada a buon fine. Le tecnologie su cui si basa Internet si sono evolute nel corso degli anni proprio per rispondere con la massima efficienza a queste esigenze.
Il primo problema in ogni processo di comunicazione è naturalmente la definizione di un linguaggio che sia condiviso tra i diversi attori che comunicano; attori che, nel caso di Internet, sono in primo luogo i computer. E i computer, come ben si sa, pur usando tutti lo stesso alfabeto — il codice binario — 'parlano' spesso linguaggi differenti e incompatibili. Fuori di metafora, computer diversi usano sistemi operativi, codici di caratteri, strutture di dati, che possono essere anche molto diversi. Per permettere la comunicazione tra l'uno e l'altro è necessario definire delle regole condivise da tutti. Questa funzione, nell'ambito della telematica, viene svolta dai protocolli.
Nel mondo diplomatico per 'protocollo' si intende una serie di regole di comportamento e di etichetta rigidamente codificate, che permettono a persone provenienti da diversi universi culturali di interagire senza creare pericolose incomprensioni. Protocolli sono detti anche gli accordi o i trattati internazionali. Queste accezioni del termine possono essere accolte per metafora anche nell'ambito della telematica: un protocollo di comunicazione definisce le regole comuni per manipolare e inviare i bit tra computer che usano ambienti operativi ed architetture hardware (culture?) diversi. Naturalmente nel caso di Internet, che interconnette milioni di computer e di sottoreti, il problema di individuare protocolli comuni è fondamentale.
Il protocollo che permette attualmente il funzionamento di questa complessa società multietnica viene indicato con la sigla TCP/IP, che è un acronimo per Transfer Control Protocol/Internet Protocol. Possiamo dire che una delle ragioni del successo di Internet risiede proprio nelle caratteristiche del suo protocollo di comunicazione.
In primo luogo TCP/IP è un open standard, ovvero le sue specifiche sono liberamente utilizzabili da chiunque. Questo ha permesso il rapido diffondersi di implementazioni per ogni sistema operativo e piattaforma esistente, implementazioni spesso distribuite gratuitamente o integrate in modo nativo nel sistema stesso.
Inoltre il TCP/IP è indipendente dal modo in cui la rete è fisicamente realizzata: una rete TCP/IP può appoggiarsi indifferentemente su una rete locale Ethernet, su una linea telefonica, su un cavo in fibra ottica ATM, su una rete di trasmissione satellitare... e così via. Anzi consente di integrare

facilmente diverse tecnologie hardware in una unica struttura logica di comunicazione, come appunto è avvenuto per Internet.
Infine TCP/IP è un protocollo di comunicazione che risolve in modo molto efficiente i tipici problemi di ogni sistema telematico:

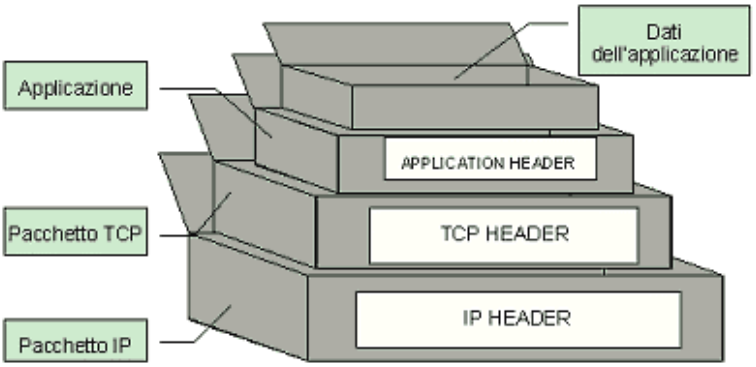
- sfruttare al meglio le risorse di comunicazione disponibili
- permettere un indirizzamento efficiente e sicuro dei computer collegati, anche se questi sono diversi milioni
- garantire con la massima sicurezza il buon fine della comunicazione
- permettere lo sviluppo di risorse e servizi di rete evoluti e facilmente utilizzabili dall'utente.

1.1.1 Un protocollo a strati

Il TCP/IP in realtà è costituito da un vero e proprio insieme di protocolli di comunicazione, ognuno con un compito specifico, organizzati in maniera gerarchica. In termini tecnici si dice che è un 'protocollo a strati di servizi' (layers of services). Per la precisione TCP/IP si basa su un modello a quattro strati:

- lo strato della rete fisica
- lo strato di indirizzamento dei computer e dell'invio dei dati
- lo strato di controllo e di organizzazione dei dati per la trasmissione
- lo strato delle applicazioni e dei servizi di rete per l'utente

In questa struttura ad ogni livello corrispondono alcune operazioni necessarie per la trasmissione dei dati: il primo livello ovviamente è quello della gestione delle connessioni fisiche, dei cavi; il secondo si occupa di inviare i dati ai vari computer collegati, sfruttando al meglio il livello hardware; il terzo livello invece ha il compito di controllare che la comunicazione di un certo blocco di dati sia andata a buon fine, e di ritrasmettere quello che eventualmente è andato perso; il quarto livello infine produce i dati veri e propri da inviare. Ogni strato è gestito da uno o più protocolli.
In fase di invio i dati partono dal livello delle applicazioni, e passano in sequenza attraverso la pila di strati; ogni protocollo riceve i dati dal livello superiore, aggiunge le informazioni di gestione che gli competono in una intestazione (header), e poi passa il tutto al livello inferiore. In fase di ricezione avviene naturalmente il processo inverso. I dati arrivano al protocollo del primo strato che legge la intestazione a lui destinata, compie le conseguenti operazioni, e poi passa il tutto al livello successivo, e così via. Naturalmente nella realtà le cose sono molto più complicate, ma questa descrizione rende l'idea. TCP/IP, insomma, può essere visto come una sorta di servizio di recapito basato su un meccanismo a scatole cinesi: al momento della spedizione i dati sono 'avvolti' in una scatola (che riporterà all'esterno alcune indicazioni sul contenuto), questa scatola viene inserita in un'altra scatola (con all'esterno un altro tipo di indicazioni), e così via. Al momento della ricezione le scatole vengono 'aperte' una dopo l'altra, ricavando da ognuna le informazioni su di essa riportate. Ogni interazione tra due computer della rete è costituita dalla confezione e dall'invio di una serie di scatole.



Rappresentazione schematica dei dati inviati tramite TCP/IP

In realtà, il gruppo di protocolli TCP/IP in senso stretto non si occupa della gestione diretta della infrastruttura hardware della rete. Come abbiamo detto, esso è indipendente da tale infrastruttura, e

questa sua caratteristica ne ha facilitato la diffusione. Esistono dunque una serie di specifiche che descrivono in che modo ogni singola architettura fisica di rete possa interfacciarsi con il TCP/IP: ad esempio per la rete Ethernet, il tipo di rete locale più diffusa al mondo, ci sono l'Address Resolution Protocol (ARP) e lo Standard for the Transmission of IP Datagrams over Ethernet Networks. Le implementazioni software dei protocolli TCP/IP normalmente integrano queste tecnologie, e dunque permettono di creare reti Internet/Intranet su qualsiasi tipo di cavo.

1.1.2 L'Internet Protocol e gli indirizzi della rete

La trasmissione dei dati e la gestione del traffico tra i vari computer in una rete TCP/IP sono governati dallo Internet Protocol (IP). Il protocollo IP ha il compito di impacchettare i dati in uscita e di inviarli, trovando la strada migliore per arrivare ad un particolare computer tra tutti quelli connessi alla rete. Le informazioni necessarie a questo fine sono inserite in una intestazione (header) IP che viene aggiunta ad ogni pacchetto di dati.
La tecnica di inviare i dati suddivisi in pacchetti (detti anche datagrammi) recanti tutte le informazione sulla loro destinazione è una caratteristica delle reti di tipo TCP/IP, che sono dette reti a commutazione di pacchetto. In questo modo è possibile usare lo stesso tratto di cavo fisico per far passare molte comunicazioni diverse, sia che provengano da più persone che operano sullo stesso computer, sia che provengano da più computer collegati a quel tratto di rete. Mai nessuno occuperà un certo tratto di rete fisica per intero, come invece avviene nella comunicazione telefonica. Questa tecnica di trasmissione dei dati permette una grande efficienza nella gestione dei servizi di rete: infatti se per una qualche ragione una singola sessione di invio si interrompe, il computer emittente può iniziare un'altra transazione, per riprendere in seguito quella iniziale. E occorre ricordare che, per un computer, interruzione vuol dire pochi millesimi di secondo di inattività!
Il secondo compito del protocollo IP è l'invio dei dati per la 'retta via'. Per fare in modo che la comunicazione tra gli host vada a buon fine è necessario che ogni singolo computer abbia un indirizzo univoco, che lo identifichi senza alcuna ambiguità, e che indichi la via per raggiungerlo tra i milioni di altri host della rete. A questo fine viene impiegato uno schema di indirizzamento dei computer collegati in rete, che si basa su un sistema di indirizzi numerici.
Ogni computer su Internet, infatti, è dotato di un indirizzo numerico costituito da quattro byte, ovvero da quattro sequenze di 8 cifre binarie. Normalmente esso viene rappresentato in notazione decimale come una sequenza di quattro numeri da 0 a 255 (tutti valori decimali rappresentabili con 8 bit), separati da un punto; ad esempio:
151.100.20.17
Questi indirizzi numerici hanno una struttura ben definita. Come abbiamo detto Internet è una rete che collega diverse sottoreti. Lo schema di indirizzamento rispecchia questa caratteristica: in generale la parte sinistra dell'indirizzo indica una certa sottorete nell'ambito di Internet, e la parte destra indica il singolo host di quella sottorete. La esatta distribuzione dei quattro byte tra indirizzo di rete e indirizzo di host dipende dalla 'classe' della rete. Esistono cinque classi di rete designate con lettere latine A, B, C, D, E; di queste solo le prime tre classi sono utilizzate effettivamente su Internet. Una rete di classe A, ad esempio, usa il primo byte per indicare la rete, e i restanti tre byte per indicare i singoli nodi. Una rete di classe C invece usa i prime tre byte per indicare la rete e l'ultimo per l'host. Inoltre, poiché il riconoscimento del tipo di indirizzo viene effettuato sul primo byte, esistono dei vincoli sul valore che esso può assumere per ogni classe. Per le reti classe A i valori potranno andare da 1 a 127, per quelle di classe B da 128 a 191, per quelle di classe C da 192 a 223.
Ne consegue che possono esistere solo 127 reti di classe A, a ciascuna delle quali però possono essere collegati ben 16.777.214 diversi computer. Invece le reti di classe B (due byte per l'indirizzo) possono essere 16.384, ognuna delle quali può ospitare fino a 65.534 host. Infine le reti di classe C potranno essere 2.097.152, composte da un massimo di 254 host.
Per capire meglio lo schema di indirizzamento di Internet basta pensare alla struttura di un normale indirizzo postale. Lo scriviamo come nei paesi anglosassoni, con il numero civico prima: 2, Vicolo Stretto, Roma, Italia. Anche qui abbiamo quattro byte: "Roma, Italia, Vicolo Stretto" svolge la funzione di un indirizzo di rete, "2" corrisponde all'indirizzo del computer. Un indirizzo di classe C!

Per trovare una analogia con un indirizzo di classe A potremmo pensare a "Italia, Presidenza della Repubblica".
L'analogia con il sistema postale è in realtà molto più profonda di quanto non potrebbe sembrare. Infatti il sistema di recapito dei pacchetti di dati attraverso la rete è funzionalmente simile al modo in cui un servizio postale tradizionale organizza il recapito delle lettere (anche queste pacchetti di dati). Quando infatti il protocollo IP di un computer riceve dei dati da inviare ad un certo indirizzo, per prima cosa guarda alla parte dell'indirizzo che specifica la rete. Se l'indirizzo di rete è quello della rete locale, i dati sono inviati direttamente al computer che corrisponde all'indirizzo. Se invece l'indirizzo di rete è esterno, i dati vengono inviati ad un computer speciale denominato gateway o router che a sua volta li invierà al gateway, da lui conosciuto, competente per un certo indirizzo di rete: ogni sottorete di Internet ha dunque almeno un gateway.
Pensiamo al sistema postale: quando imbuchiamo una lettera questa arriva all'ufficio postale locale (il gateway); se la lettera ha un indirizzo di competenza di un altro ufficio postale, sarà inviata a quell'ufficio postale, che si preoccuperà di recapitarla al destinatario. Naturalmente l'ufficio postale locale non conosce gli indirizzi di tutti gli altri uffici postali locali del mondo. Se una lettera è indirizzata ad esempio in Francia, l'ufficio locale la spedirà prima all'ufficio nazionale delle poste, che a sua volta manderà tutta la corrispondenza indirizzata alla Francia al suo omologo francese, il quale farà procedere la nostra lettera verso l'ufficio postale locale, che infine la recapiterà al destinatario.
Anche Internet funziona così. Il gateway locale infatti ha un elenco di altri gateway per ogni indirizzo di rete che conosce, più un gateway per tutti gli altri indirizzi. Normalmente i gateway conosciuti direttamente sono su parti contigue nella topologia di rete (che non necessariamente corrisponde alla contiguità geografica).
L'assegnazione effettiva degli indirizzi di rete viene curata da un organismo internazionale, il Network Information Service (NIS), il quale a sua volta delega ad enti nazionali la gestione degli indirizzi di rete nei vari paesi. In Italia tale gestione è curata dal GARR-NIS. Naturalmente la cura degli indirizzi di ogni singolo host è affidata ai gestori (o meglio system manager) delle varie reti. Ed è ovviamente importante che gli indirizzi assegnati ai vari host siano diversi l'uno dall'altro.
Una conseguenza del complicato (ma efficiente) schema di indirizzamento di Internet è che gli indirizzi sono limitati. Tanto per farsi una idea: gli indirizzi di classe A sono stati esauriti da molto tempo, quelli di classe B quasi, e non vengono più assegnati, quelli di classe C sono assegnati al 50 per cento. Con gli attuali ritmi di crescita di Internet si corre seriamente il rischio di esaurire entro pochi anni tutti gli indirizzi disponibili. Per questa ragione è stato sviluppata recentemente una versione evoluta del protocollo IP, denominato 'IP Next Generation', o 'IP 6', basata su un sistema di indirizzamento a 64 bit. Le possibili combinazioni sono decisamente aldilà del numero di abitanti del pianeta. Il prossimo collo di bottiglia, se mai ci sarà, verrà causato da amici alieni! Il nuovo protocollo IPNG è alla base delle sperimentazioni di Internet 2.

1.1.3 Il Transfer Control Protocol

Internet, si è detto, è una rete a commutazione di pacchetto. Questo significa che i dati sulla rete viaggiano in blocchi di dimensione definita: un datagramma IP è per default grande 1500 byte. Ma è chiaro che assai raramente i dati scambiati dagli utenti di Internet avranno dimensioni pari o inferiori a quelli dei piccoli pacchetti IP.
Ad ovviare a questi limiti interviene il protocollo che gestisce l'organizzazione dei dati e il controllo della trasmissione, il Transfer Control Protocol (TCP). Se la dimensione del blocco di dati da inviare eccede la dimensione di un singolo pacchetto (come avviene di norma) il TCP è in grado di suddividerlo, in fase di invio, in una catena di pacchetti, e di ricomporlo in fase di ricezione.
Quando il modulo TCP riceve dei dati da trasmettere da parte di una certa applicazione del livello superiore, suddivide il flusso di dati in segmenti; ad ogni segmento viene aggiunta una intestazione (TCP header) che specifica che tipo di applicazione ha prodotto il flusso di dati e a che punto del flusso appartiene il blocco in questione. In questo modo il TCP ricevente sarà in grado di ricomporre i dati nella loro sequenza e di passarli alla applicazione giusta.
Ma il TCP svolge anche un'altra importante funzione, come il nome stesso suggerisce: assicura che la trasmissione dei dati vada a buon fine, esercitando un controllo sulla comunicazione.
Per fare questo il modulo TCP del computer A che invia stabilisce un contatto diretto con il suo pari (peer in termini tecnici) nell'host B che riceve. La comunicazione inizia con una richiesta rivolta da A a B di prepararsi a ricevere dati. In caso di risposta positiva A inizia il trasferimento del primo segmento di dati, e poi attende che B invii un segnale di conferma di aver ricevuto tutti i dati inviati. Se questo non avviene o se B dichiara di avere ricevuto solo una parte dei dati inviati, A ritrasmette il segmento perduto.
Naturalmente questo schema semplifica il vero funzionamento delle transazioni TCP, e offre un'idea solo teorica delle comunicazioni in rete. L'essenziale è tuttavia che un meccanismo di questo tipo permette alla maggior parte delle comunicazioni su Internet di andare a buon fine; se pensate che ogni giorno avvengono in rete miliardi di transazioni, vi potrete rendere conto della efficienza e dell'importanza di questo sistema.

2. Le applicazioni e i servizi di rete

Lo strato dei servizi applicativi è l'ultimo livello nell'architettura del TCP/IP. A questo livello si pongono tutte le applicazioni che producono i dati e che fanno uso dei protocolli TCP ed IP per inviarli attraverso la rete. Si tratta per la maggior parte delle applicazioni e dei servizi di rete con i quali gli utenti interagiscono direttamente.
Infatti Internet offre all'utente una molteplicità di servizi e di applicazioni che facilitano l'uso della rete e lo scambio o il reperimento di informazioni. Si va dalla posta elettronica allo scambio di file, fino alla diffusione di informazione multimediale. Ogni singolo servizio di rete Internet si basa su un dato protocollo, specifico di quel particolare servizio. Ma come funzionano le varie applicazioni che complessivamente sono presenti su Internet?
I servizi telematici di Internet si basano su una particolare modalità di interazione, denominata tecnicamente architettura client-server. Con tale formula si indica in generale una applicazione informatica, un software, che è costituito da due moduli interagenti ma distinti, che collaborano tra loro per eseguire un certo compito richiesto dall'utente, e che possono trovarsi su piattaforme hardware diverse.
Il client è il programma che costituisce l'interfaccia con l'utente e che si occupa di richiedere e presentare i dati. Il server invece si occupa solo del mantenimento, del reperimento e dell'invio dei dati al client che li ha richiesti. Normalmente client e server sono installati su macchine diverse: il primo si trova sul computer locale utilizzato dall'utente finale (che ha quindi bisogno di sapere solo come funziona il suo programma client). Il secondo si trova sul sistema remoto, e l'utente non ha alcun bisogno di conoscerne il funzionamento. Tuttavia nulla impedisce che entrambi i moduli si trovino sulla stessa macchina (questo avviene normalmente in tutte le macchine che ospitano server).

Affinché l'interazione tra client e server possa stabilirsi, è necessario che entrambi utilizzino un linguaggio comune, ovvero un protocollo di comunicazione. Tra i vari protocolli specifici delle applicazioni abbiamo ad esempio il Simple Mail Transfer Protocol (SMTP) per la posta elettronica, il File Transfer Protocol (FTP) per il trasferimento di file tra host, e il protocollo su cui si basa World Wide Web, denominato Hyper-Text Transfer Protocol (HTTP).
Quando l'utente richiede un certo documento o file situato in un dato host della rete, il client invia una richiesta al server attraverso il TCP/IP. Il server, ricevuta la richiesta, ricerca i dati desiderati, e li invia al computer su cui è installato il client. Sarà quest'ultimo che si occuperà di presentare opportunamente i dati sul video per facilitare l'interazione con l'utente.
Una conseguenza di questa architettura è che possono esistere programmi client diversi per accedere agli stessi servizi, anche a seconda dell'ambiente operativo utilizzato, e che ci possono essere più versioni di un certo client.

3. I nomi della rete

Il metodo di indirizzamento numerico dell'Internet Protocol, sebbene sia molto efficiente dal punto di vista dei computer, che macinano numeri, è assai complicato da maneggiare per un utente. Ricordare le varie sequenze numeriche corrispondenti agli indirizzi dei computer a cui ci si intende connettere può essere molto noioso, come lo sarebbe dover ricordare a memoria tutti i numeri telefonici dei nostri amici e conoscenti. Per questo sono nate le agende: se voglio telefonare a Gino, cerco sulla mia agenda, magari elettronica, il suo nome (facile da rammentare) e leggo il suo numero di telefono. Pensate, poi, quanto sarebbe comodo dire al telefono "voglio telefonare a Gino" e sentire il telefono comporre da solo il numero.
Per ovviare a questi problemi e facilitare l'impiego della rete da parte degli utenti è stato sviluppato un sistema di indirizzamento simbolico, che funziona in modo simile: si chiama Domain Name Service (DNS).
Attraverso il DNS ogni host di Internet può essere dotato di un nome (domain name), composto da stringhe di caratteri. Tali stringhe, a differenza dell'indirizzo numerico, possono essere di lunghezza illimitata. È evidente che per un utente utilizzare dei nomi simbolici è molto più semplice e intuitivo che maneggiare delle inespressive sequenze di numeri. Ad esempio, all'host 151.100.20.17 corrisponde il seguente nome: rmcisadu.let.uniroma1.it.
Come si può vedere anche i nomi sono sequenze di simboli separati da punti. Questa articolazione rispecchia la struttura gerarchica del Domain Name Service. Esso suddivide la intera rete in settori, denominati domini, a loro volta divisi in sottodomini, e così via per vari livelli; ogni sottodominio fa parte del dominio gerarchicamente superiore: alla base della piramide ci sono i singoli host.
L'identificativo di un host riassume le varie gerarchie di domini a cui appartiene: ogni sottostringa rappresenta o un dominio, o un sottodominio, o il nome del computer. Ma l'ordine di scrittura è inverso all'ordine gerarchico! Suona complicato, ma non lo è. Vediamo più da vicino il nostro esempio.
La parte di indirizzo più a destra nella stringa indica il dominio più alto della gerarchia, nel nostro caso 'it'. In genere, il livello più alto identifica il paese o, per gli Stati Uniti, il tipo di ente che possiede il computer in questione. Gli altri livelli della gerarchia, muovendosi da destra a sinistra, scendono verso il sistema specifico presso il quale è ospitato l'utente identificato dall'indirizzo. Così, nel caso sopra considerato 'uniroma1' si riferisce all'Università di Roma "La Sapienza", 'let' si riferisce alla facoltà di Lettere di questa università, e infine 'rmcisadu' è il nome dell'host, che nel caso specifico prende il nome dal Centro Interdipartimentale Servizi di Automazione nelle Discipline Umanistiche della facoltà. Dunque un nome simbolico fornisce all'utente dotato di un minimo di esperienza una serie di informazioni che possono essere molto utili.
I domini di primo livello sono essenzialmente di due tipi: domini di organizzazione e domini nazionali. Quando il DNS è stato creato, Internet era diffusa, salvo rare eccezioni, solo negli Stati Uniti. Per questa ragione i domini statunitensi (ed alcuni domini 'non geografici') sono stati divisi per tipo di organizzazione:

- EDU: università ed enti di ricerca
- COM: organizzazioni commerciali

- GOV: enti governativi
- MIL: enti militari
- NET: organizzazioni di supporto e di gestione della rete
- ORG: organizzazioni ed enti di diritto privato non rientranti nelle categorie precedenti, come enti privati no-profit, associazioni, organizzazioni non governative.

In seguito la rete ha cominciato a diffondersi a livello internazionale. Per questo sono stati creati altri domini di primo livello, suddivisi per nazioni: questi domini usano delle sigle che spesso (ma non sempre) corrispondono alle sigle delle targhe internazionali. L'Italia, come si può evincere dal nostro esempio, è identificata dalla sigla 'IT', l'Inghilterra dalla sigla 'UK', la Francia da 'FR', e così via. Recentemente sono stati annunciati altri domini di primo livello internazionali, che, seguendo l'evoluzione della rete, estendono la originale partizione:

- FIRM: aziende e società
- STORE: siti commerciali e servizi di commercio online
- WEB: enti e organizzazioni dedicate allo sviluppo di World Wide Web
- ARTS: siti culturali e artistici
- REC: siti dedicati all'intrattenimento
- INFO: siti dedicati all'informazione
- NOM: siti che contengono pagine Web personali.

Nell'ambito di ogni dominio possono essere creati un numero qualsiasi di sottodomini.
Dal punto di vista tecnico il Domain Name Service è costituito da un sistema di database distribuiti nella rete chiamati name server, che sono collegati tra loro. Ogni dominio e ogni sottodominio ha almeno un name server di riferimento. Quest'ultimo svolge la funzione di tradurre i nomi in indirizzi numerici per conto degli host o di altri name server. Infatti la comunicazione effettiva tra gli host avviene sempre attraverso gli indirizzi numerici. La traduzione viene chiamata tecnicamente risoluzione.
Quando un host (sollecitato da un utente o da una applicazione) deve collegarsi ad un altro host che ha un determinato nome simbolico, ad esempio sunsite.dsi.unimi.it, chiede al proprio name server locale di tradurre il nome simbolico nel corrispondente indirizzo numerico. Il name server locale va a vedere nella sua tabella se ha l'informazione richiesta. In caso positivo risponde all'host che lo ha interpellato, fornendo il corrispondente indirizzo numerico, altrimenti chiede ad un altro name server (detto name server di primo livello). La scelta di questo 'super-aiutante' è determinata dal dominio di primo livello dell'indirizzo da risolvere ('it', nel nostro caso). I name server di primo livello vengono detti authoritative name server. Essi possono sia rispondere direttamente, sia dirottare la richiesta a degli altri name server (questa volta di secondo livello). Il processo può continuare per vari sottolivelli, finché non viene risolto per intero l'indirizzo dell'host cercato. Intelligentemente, nel fare questo lavoro di interrogazione il nostro name server locale si annota gli indirizzi che ha conosciuto, in modo che le future richieste possano essere risolte immediatamente.
Grazie a questo meccanismo il DNS è sempre aggiornato: infatti la responsabilità di aggiornare i singoli name server è decentralizzata e non richiede una autorità centrale che tenga traccia di tutti i milioni di host computer collegati a Internet.
Come avviene per gli indirizzi, la gestione del sistema DNS in un dominio di primo livello viene affidata a degli enti specifici. Questi enti hanno il compito di assegnare i nomi di sottodominio e di host, curando attentamente che non esistano omonimie; essi inoltre debbono occuparsi di gestire il database principale del dominio di cui sono responsabili, e dunque di garantire il funzionamento del DNS a livello globale. In Italia l'ente che effettua la gestione del DNS è il medesimo che assegna gli indirizzi di rete numerici, il GARR-NIS.

4. La tipologia delle connessioni a Internet

Sappiamo che Internet collega milioni di computer. Il collegamento di un computer ad Internet può avvenire tecnicamente in diversi modi.
Possiamo distinguere al loro interno due categorie principali:

- collegamenti diretti con linee dedicate

- collegamenti dialup con linee telefoniche normali o ISDN

La connessione diretta ad Internet implica dei costi di investimento iniziali e di gestione piuttosto alti, in genere non alla portata del singolo utente, e interessa normalmente enti ed aziende che vogliono entrare in rete.
Quanto alla connessione dialup, fino a pochi anni fa l'utente finale che non aveva accesso diretto ai centri di calcolo di enti ed università dotate di collegamento a Internet poteva solo collegarsi via modem ad un host con un software di emulazione terminale, ed usare i servizi di rete presenti sull'host.
Questa limitazione è stata superata con la diffusione di due protocolli che permettono di effettuare una connessione diretta alla rete attraverso un semplice collegamento su linea seriale, e dunque di stabilire un collegamento Internet completo attraverso il modem e la linea telefonica. I due protocolli che permettono il collegamento dialup, come viene denominato, sono il Serial Line Internet Protocol (SLIP) e il Point-to-Point Protocol (PPP).

5. Indirizzamento

5.1 GLI INDIRIZZI IP

L'indirizzo, o IP address, è un campo composto da 32 bit. I primi bit permettono di distinguere 5 forme standard identificate da una lettera del alfabeto, e dette classi.
Come si può vedere in figura, le prime tre classi dell'IP address contengono sia l'indirizzo di una rete (netid), sia quello di una macchina nella stessa (hostid). In realtà l'indirizzo non identifica necessariamente una macchina, ma una connessione alla rete. Per esempio, un router ha almeno due indirizzi, avendo connessioni ad almeno due reti. Questo in quanto un router appartiene a entrambe le reti, e quindi sono necessari due indirizzi dato che un IP address ha posto per un solo indirizzo di rete. Se l'indirizzo dell'host è 0, allora l'IP address si riferisce alla rete stessa. Se viceversa tutti i bit riservati all'indirizzo dell'host sono 1, allora l'indirizzo viene utilizzato per identificare tutti gli host della rete (broadcasting). Uno speciale indirizzo formato da 32 bit posti a uno è chiamato local network broadcast address e serve solo in casi molto particolari. Il concetto di broadcasting è quello della diffusione a tutto raggio, un po' come fa un'emittente radiofonica. In generale internet interpreta i campi formati da tutti uno come all, cioè «tutti», mentre quelli formati da tutti zero come this, cioè «questo», «qui». Questo per quanto riguarda le classi A, B e C. La classe D è usata per un particolare tipo di distribuzione dei dati detto multicasting. La classe E è riservata a usi futuri. Dato che specificare ogni singolo bit di un indirizzo IP sarebbe alquanto poco pratico e di scarsa leggibilità, la convenzione è quella di leggere ogni ottetto, cioè ogni gruppo di 8 bit, come un intero, e di separare i quattro ottetti con un punto (Figura 3). Oltre a i casi speciali già descritti, l'indirizzo di classe A 127.0.0.0 è riservato per un particolare processo di test che rimanda indietro i dati al mittente senza propagarli nella rete.
Uno dei vantaggi di questo schema è la possibilità da parte dell'organismo centrale che assegna gli indirizzi (Network Information Center) di delegare ai responsabili delle singole reti l'assegnazione di una parte dell'indirizzo all'interno della rete stessa. La cosa avviene un poco come con i numeri di telefono. A livello internazionale ogni stato ha il suo prefisso internazionale. Per esempio, per l'Italia, è 39. All'interno ogni stato divide il paese in aree geografiche a cui assegna un ulteriore codice. Per esempio, Roma è identificata dal 6, Milano dal 2, Firenze da 55, e così via. All'interno poi della provincia o della città possono essere definite ulteriormente sottoaree a cui si assegnano due, tre o quattro cifre. Per esempio 529 oppure 7054. Infine ogni telefono in tali aree avrà il suo numero. Così, se Mr. Smith deve chiamare dagli Stati Uniti il signor Mario Rossi abitante all'EUR, a Roma, comporrà per esempio il numero 011.39.6.529.4467. In questo caso lo 011 serve per uscire dagli USA, un po' come il nostro 00.
Analogamente in internet i numeri di classe C sono assegnati alla piccole reti, quelle cioè con meno di 256 host, quelli di classe B alle reti con al massimo 65536 host, e quelli di classe A alle reti con oltre 16 milioni di host. Ogni rete decide poi come suddividere gli indirizzi che gli sono stati riservati al suo interno come meglio crede. Ovviamente, una internet privata non ha la necessità di seguire

queste regole, né a utilizzare indirizzi assegnati dal NIC, ma il non farlo potrebbe impedire in futuro la connessione alla TCP/IP Internet.
Dato che l'indirizzo può essere a volte abbastanza ostico da ricordare, è possibili associare a ogni host anche un nome, che può essere utilizzato come mnemonico per un IP address, e la cui risoluzione è responsabilità di particolari macchine chiamate name server. In realtà il name server è un programma software che può girare in qualunque macchina connessa alla rete, e che mantiene l'associazione tra nomi e indirizzi IP, fornendo tali corrispondenze quando richiesto da un altro programma chiamato name resolver. Di fatto, si preferisce far girare il name server su una macchina dedicata, che prende anch'essa, a questo punto, il nome di name server. Potete pensare al name server come a una agenda telefonica elettronica, che contiene una lista parziale di nomi e numeri telefonici. In internet infatti, non esiste un singolo elenco telefonico, ma tanti name server che cooperano per fornire quello che è un vero e proprio elenco distribuito. In realtà il sistema funziona in modo gerarchico, un po' come se una certa agenda contenesse solo i prefissi internazionali e il puntatore alle agende di ogni singolo stato, le quali a loro volta contengono i prefissi regionali e i puntatori agli elenchi regionali, e così via, fino ad arrivare all'agenda che contiene solo le estensioni telefoniche di un singolo edificio.

6. Servizi applicativi

6.1 FTP

6.1.1 Introduzione

È stato calcolato che attualmente, sparpagliati nelle memorie degli host computer connessi a Internet, ci siano diversi milioni di file. Si tratta di uno sconfinato serbatoio di programmi, immagini digitali, suoni, ecc. molti dei quali di 'pubblico dominio'. Il sistema che ci consente di trasferire questi file sul nostro computer, si chiama File Transfer Protocol (FTP).
Prima di affrontare il discorso legato all'FTP, riteniamo valga la pena soffermarci brevemente sulla definizione di software di pubblico dominio (PD per brevità), e cercare di illustrarne i principi base; a beneficio in particolar modo di coloro che ancora non ne hanno compresa l'utilità e non ne rispettano le regole.
Anni fa, chiunque avesse realizzato un programma di un qualche valore senza lavorare per una software house, avrebbe avuto scarse possibilità di vederlo usato da molti, e quasi nessuna di guadagnarci qualcosa. C'erano le riviste tecniche che pubblicavano i cosiddetti 'listati', o che allegavano un dischetto; ma in ogni caso, a parte la difficoltà di venire pubblicati, i programmi originali disponibili al di fuori dal circuito strettamente commerciale erano poche decine. C'era anche chi, per eccesso di modestia o per mancanza di intraprendenza, pur avendo realizzato qualcosa di valido, non lo proponeva alle ditte distributrici. Strada ancora più impervia toccava al software che potremmo definire 'di nicchia', quello che comunque non interessa il grande pubblico: le applicazioni scientifiche, i progetti di ricerca universitaria e via discorrendo.
Oggi tutti questi ostacoli sono superati. Infatti praticamente tutte le università, i centri di ricerca, e numerose altre organizzazioni, anche commerciali, riservano parte delle proprie risorse di sistema per ospitare i programmi di pubblico dominio. Negli enormi hard disk di questi enti sono memorizzati un gran quantitativo di file, prelevabili gratuitamente e da qualsiasi località (più avanti vedremo come).
Con la telematica è finalmente possibile scovare il software più specialistico: dal database testuale per gli studiosi di linguistica, a una riedizione del gioco Pong per Windows.
Affinché però questa incredibile macchina non si fermi, è necessario rispettarne le poche regole. Chi preleva da un sito Internet o da una BBS un programma shareware, e poi lo utilizza, deve — secondo le clausole di distribuzione — versare i pochi dollari di registrazione: non perché qualcuno altrimenti lo denuncerà per pirateria — probabilmente non succederebbe — ma perché alle spalle del programma prelevato gratuitamente c'è chi ci ha lavorato molto e ha scelto un canale di

distribuzione che è assai vicino alle esigenze dell'utente. Chi preleva un programma con questo sistema può infatti fare qualcosa che nessun'altra fabbrica o ditta del mondo gli consentirebbe: verificare la qualità di ciò che vuole comprare con delle prove, anche prolungate, prima di pagare.
È un modo di vendere che va incoraggiato, perché è il più equo, è quello che consente davvero di scegliere il meglio (visto che il prelievo e l'uso a titolo di prova sono gratuiti, l'acquirente ha la facoltà di prelevare anche cinque o sei tipi di programma simili, per poi versare la quota solo del migliore) e infine perché allarga enormemente le possibilità di scelta: sono poche le software house in grado di raggiungere ogni angolo del pianeta con le proprie reti distributive, mentre tutti, o quasi, possono arrivare a Internet.
Oltre allo shareware ci sono anche altre categorie di software. C'è quello completamente gratuito (di solito identificato con il termine freeware), quello che richiede come pagamento un versamento volontario anche non necessariamente in denaro (giftware) e quello che si accontenta di una cartolina (cardware).
Chi non versa la quota di registrazione forse si sente furbo, perché ha un programma senza averlo pagato, e senza aver violato apparentemente nessuna legge; in realtà nuoce a sé stesso, perché se un giorno la politica shareware dovesse fallire, la scelta di software di cui possiamo beneficiare attualmente verrebbe enormemente ridotta, e sul mercato sopravviverebbero solo le grandi software house con la loro politica dei prezzi.

6.1.2 Usare FTP: concetti di base

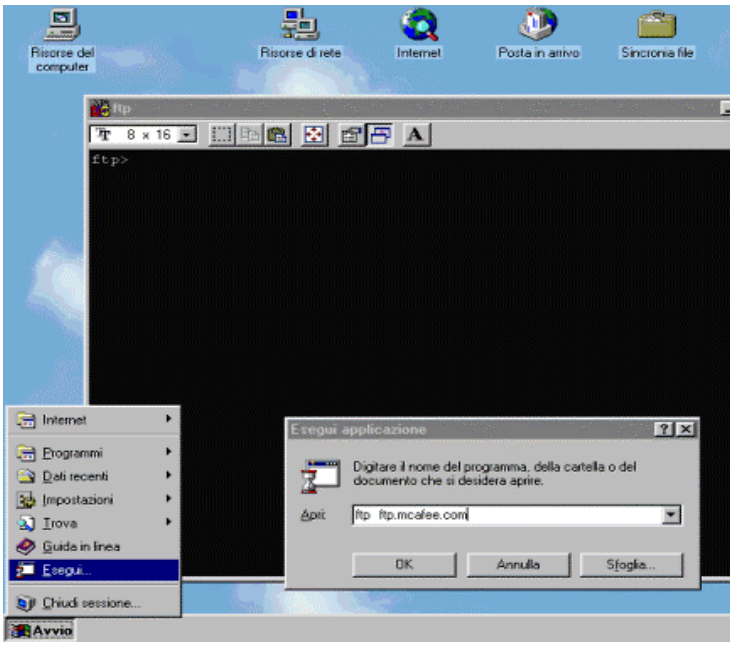
Nei capitoli successivi, quando parleremo di Archie e di siti come http://www.shareware.com, affronteremo il tema della ricerca di un programma su Internet; ora diamo invece un'occhiata a come funziona il protocollo che ci consentirà di trasferirlo sul nostro computer, dando per scontato che già ne conosciamo la localizzazione.
Indipendentemente dal tipo di applicazione utilizzata per attivare una sessione FTP, ci sono due modalità di collegamento ad una macchina remota: FTP anonimo, e FTP con account.
Il trasferimento di file tramite FTP anonimo è quello tradizionalmente utilizzato per il prelievo di file presso università, enti, società. Consiste in un login, ovvero nell'ingresso in un computer remoto, effettuato senza disporre presso di esso di un proprio codice utente e di una propria password, quindi anonimamente. In questa modalità non avremo, per ovvi motivi di sicurezza, pieno accesso al computer remoto; potremo quindi entrare solo in determinate directory — tipicamente nella directory chiamata 'pub' (ovvero public) e nelle sue sottodirectory — e potremo solo leggere alcuni file, ma non cancellarli, spostarli o modificarli.
L'utilizzazione di FTP con account, invece, dà pieno accesso ad una determinata directory del sistema remoto, nella quale potremo inserire, modificare e cancellare file, proprio come se fosse una directory del vostro hard disk. Di norma è riservata ai dipendenti dell'università, dell'ente o della società che ospita il server FTP, oppure ai loro collaboratori, oppure ancora ai loro clienti. Se, ad esempio, decidete di pubblicare su Internet una vostra pagina Web, acquistando lo spazio presso un Internet provider, quest'ultimo con ogni probabilità vi concederà un account FTP e una password personale.

6.1.3 Alcuni programmi per l'uso di FTP

Come di consueto, i programmi (client) per fare FTP si dividono in due categorie: quelli che dispongono di una interfaccia a caratteri, e quelli con una interfaccia grafica.

6.1.4 Programmi con interfaccia a caratteri

I client FTP con interfaccia a caratteri possono sembrare un po' ostici, ma sono molto efficienti e versatili. Nella figura che segue è visibile, a titolo di esempio, il client FTP fornito di serie con Windows 95.



Il client FTP a caratteri di Windows 95

Per vedere quali sono i comandi di cui si dispone in una sessione FTP, effettuiamo un collegamento di prova con la McAfee Associates, negli Stati Uniti, la nota software house specializzata in programmi antivirus.
La prima cosa da fare, ovviamente, è attivare il client FTP. La procedura cambia a seconda del programma utilizzato, del sistema operativo adottato, ecc., ma è quasi sempre una operazione molto semplice. Vediamo ad esempio come si procede con Windows 95: stabilito che l'host computer della McAfee Associates ha per 'indirizzo' ftp.mcafee.com, è sufficiente scrivere dalla shell di comando (fare clic su 'Avvio' e poi su 'Esegui...'):
• ftp ftp.mcafee.com
A questo punto il computer della McAfee chiede il nominativo per l'accesso. Poiché non disponiamo di account, e desideriamo semplicemente avere accesso alla directory 'pub' (e alle sue sottodirectory), forniamo come risposta 'anonymous' (senza virgolette). A video compare quanto segue:
Name (ftp.mcafee.com:(none)): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password: nome.cognome@mio.fornitore
Siamo entrati. Da notare che, come ci ha suggerito lo stesso server, abbiamo fornito il nostro indirizzo di posta elettronica in luogo della password. Da questo momento in poi abbiamo a disposizione alcuni comandi, come 'dir' o 'cd', del tutto simili a quelli del nostro personal; la differenza è che in questo caso operano sugli hard disk del computer remoto. Attenzione: non è il nostro personal computer a eseguirli, non variano perciò da sistema operativo a sistema operativo, ma vengono eseguiti dal computer al quale ci siamo collegati (nel nostro esempio, il server FTP della McAfee Associates) e del quale ora il nostro PC è diventato a tutti gli effetti un terminale.
Conosciamo già la struttura del sito della McAfee e perciò decidiamo subito di entrare nella directory chiamata 'antivirus', che si trova nella directory 'pub'. Per farlo utilizziamo il comando 'cd':
ftp> cd pub/antivirus
Notare che il carattere usato per dividere 'antivirus' da 'pub' è la barra inclinata a destra (/), secondo la sintassi Unix, piuttosto che la barra inclinata a sinistra, propria dell'MS-DOS. Infatti la quasi totalità dei server FTP gira su Unix, o comunque ne rispetta la sintassi.
La struttura dei siti FTP 'pubblici' è quasi sempre la stessa, basta conoscerne una per potersi muovere con facilità in moltissime altre. Per visualizzare il contenuto di una directory sul computer remoto, occorre utilizzare il comando 'dir'; nel nostro caso ('pub/antivirus'), ecco il risultato:
total 2522
-r--r--r-- 1 root wheel 1760 Mar 21 19:13 00-Index

-r--r--r-- 1 root 50 193841 Dec 13 21:31 3nsh156.zip
-r--r--r-- 1 root 50 193381 Dec 13 21:31 4nsh156.zip
-r--r--r-- 1 root wheel 274380 Mar 19 20:48 clean113.zip
-r--r--r-- 1 root wheel 15743 Nov 24 20:08 killmnk3.zip
-r--r--r-- 1 root wheel 186497 Sep 1 1993 langv106.zip
-r--r--r-- 1 root wheel 288851 Mar 19 20:48 ocln113.zip
-r--r--r-- 1 root wheel 259290 Mar 19 20:48 oscn113.zip
-r--r--r-- 1 root wheel 255246 Mar 19 20:48 scanv113.zip
-r--r--r-- 1 root 50 25220 Sep 20 1993 sentry02.zip
-r--r--r-- 1 root wheel 160330 Feb 24 00:45 strtl2.exe
-r--r--r-- 1 root wheel 77586 Nov 17 01:24 strtli.exe
-r--r--r-- 1 root wheel 76159 Mar 21 19:12 virdt113.zip
-r--r--r-- 1 root wheel 146331 Mar 19 20:48 vsh113.zip
-r--r--r-- 1 root wheel 310274 Mar 19 20:48 wscan113.zip
226 Transfer complete.

Nella parte sinistra dell'elenco vediamo alcune informazioni di sistema, su cui in questo momento sorvoliamo. Sulla destra invece individuiamo piuttosto facilmente i dati relativi alla lunghezza del file, alla data e all'ora di rilascio. Gli ultimi caratteri sono per il nome del programma. Certo, il semplice nome può non dirci molto sul tipo di programma. In questi casi, può essere opportuno per prima cosa prelevare un indice più dettagliato. Lo troviamo quasi sempre in file con un nome simile a '00-Index' (lo 00 iniziale serve a farlo comparire per primo nell'elenco, come nell'esempio appena visto).

Supponiamo, dopo aver consultato il file di indice, di voler prelevare la versione 1.13 del programma Vshield (file vsh113.zip). Prima di tutto dovremo comunicare al computer remoto che si tratta di un file binario e non di testo, cosa che viene fatta usando il comando 'bin' (questa operazione non è sempre necessaria, dato che molti host capiscono da soli quando impostare il trasferimento in modalità binaria; tuttavia non è male usarlo comunque). Ora possiamo prelevare il file. Per farlo si deve usare il comando 'get <nome_del_file>':

ftp> get vsh113.zip
200 PORT command successful.
213 146331
150 Opening BINARY mode data connection for vsh113.zip (146331 bytes).
226 Transfer complete.
146331 bytes received in 1.2e+02 seconds (1.2 Kbytes/s)

Fatto! Il 'get' ha copiato il file 'vsh113.zip' dal server FTP della McAfee Associates al nostro hard disk. A questo punto, possiamo chiudere la connessione con il computer remoto.

Il comando 'get' offre anche altre piccole potenzialità. Ad esempio ci consente di prelevare un programma e di riceverlo con un nome diverso dall'originale. 'Get' utilizzato in questo modo preleva il file chiamato 'pippo.zip' e ce lo fa arrivare con nome 'paperino.zip'. È una comodità soprattutto per chi usa MS-DOS e si imbatte in file con nomi lunghi o non gestibili (perché magari contengono più di un punto al loro interno).

Una piccola variante rispetto a 'get' è 'mget'. Con 'mget' si possono prelevare più programmi contemporaneamente. Ad esempio 'mget term*.zip' preleva tutti i file che iniziano con 'term' e finiscono con '.zip' (terminus.zip, terminal.zip, ecc.). Il comando 'mget *.*' spedisce (teoricamente) tutti i file presenti nella directory dell'host system cui si è collegati. La maggior parte dei computer, tuttavia, disabilita questa funzione perché può scatenare un traffico di dati enorme; si pensi che ci sono hard disk con molti gigabyte liberamente duplicabili (e anche con modem veloci ci vorrebbero giorni prima di smaltire tanto traffico).

FTP in modalità carattere mette a disposizione una serie di altri comandi. Il seguente elenco ne spiega la funzionalità:

Comando	Descrizione
Ascii	è il comando inverso rispetto a 'bin'. Imposta la trasmissione in modalità testo

Bin	imposta la trasmissione in modalità binaria, ovvero la modalità adatta a programmi, immagini digitali, ecc. Alcuni server FTP commutano automaticamente in 'binary mode' quando si preleva uno di questi file
cd nome_directory	cambia directory. Da notare che quando si vogliono indicare anche le sottodirectory, vanno separate con la barra inclinata a destra, secondo la consuetudine Unix. Ad esempio: 'cd pub/antivirus' (e non 'cd pub\antivirus')
Cdup (oppure cd . oppure ancora cd ..)	sale di una directory. Ad esempio porta alla directory 'pub' se ci si trova in 'pub/antivirus'. Se il server risponde che il comando non esiste, provare con 'cd .' (cd, spazio, punto), oppure con 'cd ..' (cd, spazio, punto, punto)
delete nome_file	cancella un file (il comando funziona solo durante sessioni con account; per evidenti motivi di sicurezza)
dir	visualizza il contenuto di una directory
dir abbreviazione*	se si vogliono visualizzare, ad esempio, solo i file il cui nome inizia con 'f', si può scrivere 'dir f*'
get nome_file	preleva un file. Se il file non è un semplice testo, è buona norma far precedere questo comando dal comando 'bin'
get nome_file -	simile al comando 'type' di MS-DOS: stampa a video un file di testo (notare il trattino dopo il nome del file)
hash	durante un download, fa sì che venga visualizzato un carattere '#' ogni Kbyte arrivato (oppure ogni due, o più, dipende da come è configurato il server). Utile per meglio monitorare i trasferimenti
help	fornisce l'elenco dei comandi disponibili
help nome_comando	fornisce una breve spiegazione sul comando indicato
lcd nome_directory	cambia la directory locale (quella del proprio PC), ovvero la directory nella quale il client memorizzerà il file che si sta prelevando. Dato da solo, indica qual è la directory selezionata
put nome_file	questo comando consente di trasferire un file dal proprio computer al server FTP cui si è connessi. Solitamente è utilizzabile solo in sessioni FTP con account e password, in quanto via FTP anonimo non si è abilitati in scrittura. A tale ultimo proposito, tuttavia, vale la pena aggiungere che alcuni server FTP, anche quando ci si collega in modalità anonima, mettono a disposizione una directory aperta in scrittura, quasi sempre chiamata 'incoming'. Anche il 'put', se il file da spedire non è un semplice testo, è buona norma farlo precedere dal comando 'bin'
pwd	visualizza il nome (e il path) della directory nella quale ci si trova quit chiude una sessione FTP. Se non funziona provare con 'bye', 'close', 'logout', ecc.

Può succedere che il server al quale ci si collega non metta a disposizione alcuni di questi comandi, o ne metta a disposizione altri. I fondamentali, comunque, come 'dir', 'get', 'bin' e 'cd' sono sempre disponibili.

6.1.5 Altre informazioni utili legate all'FTP con interfaccia a caratteri

Prima di lasciarvi avventurare tra gli sterminati archivi di programmi di pubblico dominio, vale la pena aggiungere due consigli.
Se, avete provato a prelevare un file, e il computer remoto vi ha risposto con un laconico 'No such file or directory', con ogni probabilità avete trascurato di rispettare le maiuscole e le minuscole contenute nel nome del file. Infatti, secondo il sistema operativo Unix, e quindi secondo la maggior parte dei server FTP, il file 'pippo.zip' è diverso da 'Pippo.zip' e da 'PIPPO.ZIP'. Se perciò si scrive 'get pippo.zip', e il nome del file è 'Pippo.zip' (con la 'P' maiuscola), il server non lo trova.
In un successivo capitolo affronteremo la questione della ricerca dei file; può essere comunque utile disporre della cosiddetta FTP-list, una sorta di pagine gialle dei server FTP. Il file 'ftp-list.zip' si può prelevare via anonymous FTP al seguente indirizzo: ftp://garbo.uwasa.fi, nella directory:

/pc/doc-net/ (la URL è quindi ftp://garbo.uwasa.fi/pc/doc-net/ftp-list.zip), oppure presso oak.oakland.edu, directory: /SimTel/msdos/info/ (la URL in questo caso è perciò: ftp://oak.oakland.edu/SimTel/msdos/info/ftp-list.zip).
Può essere utile, infine, ricordare che nella quasi totalità dei casi i file che possiamo trovare sui siti FTP sono sottoposti a compressione. Questo processo serve a risparmiare spazio e a raccogliere in un unico archivio più file. Esistono diversi programmi di compressione, spesso legati ai diversi sistemi operativi. Ognuno di essi produce dei file caratterizzati da particolari estensioni. Nel seguente elenco sono indicate quelle con cui avrete occasione di imbattervi più spesso, con i relativi programmi.

Estensione	Tipo file
.gz	file compresso con GNU Gzip
.hqx	file compresso Macintosh (BinHex)
.lzh	file compresso (in genere per MS-DOS, ma il formato è molto diffuso anche tra i computer Amiga)
.sit	file compresso Macintosh (StuffitExpander)
.tar	file compattato con il programma Unix tar
.tar.gz	file compattato e poi compresso con tar e gzip
.Z	file compresso con il programma Unix compress
.zip	file compresso con PkZip o Info-Zip

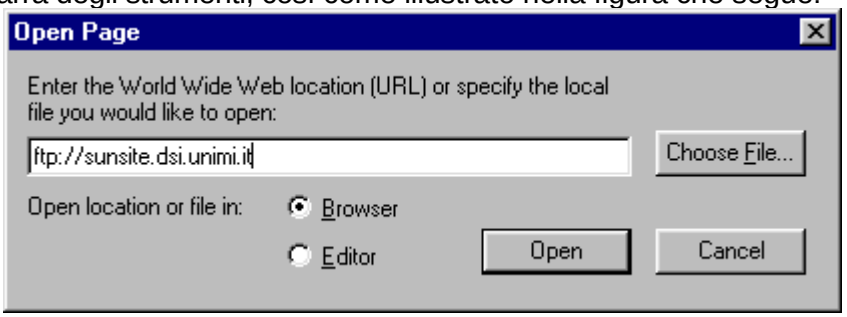
Si noti che i file compressi, di qualsiasi tipo (zip, lzh, gzip.), dopo essere stati trasferiti sul proprio hard disk, debbono essere espansi al loro formato originale, utilizzando i relativi programmi di decompressione. Il programma di compressione più diffuso in assoluto, nato in ambiente MS-DOS e Windows, è PkZIP.

6.2 PROGRAMMI CON INTERFACCIA GRAFICA

Le interfacce grafiche hanno definitivamente avuto la meglio nel mondo delle telecomunicazioni, così anche per il prelievo di file sono ormai disponibili programmi a base di icone e mouse. Ce ne sono diversi, per tutti i sistemi operativi; qui di seguito illustriamo il client FTP inserito in Netscape (il suo funzionamento è identico sia che si possieda un PC con Windows, sia che si utilizzi un Macintosh, o un sistema Unix con ambiente X-Window) e l'ottimo programma specifico CuteFTP, per Windows (molto buono è anche WS_FTP, il cui funzionamento comunque è molto simile). L'integrazione fra il programma di gestione risorse e la navigazione in rete fa anche di Internet Explorer 5 un potente strumento di FTP grafico; la versione beta disponibile al momento in cui scriviamo non consente ancora un pieno 'drag and drop' FTP fra risorse locali e remote, ma è probabile che questo limite verrà superato nella versione definitiva del programma.

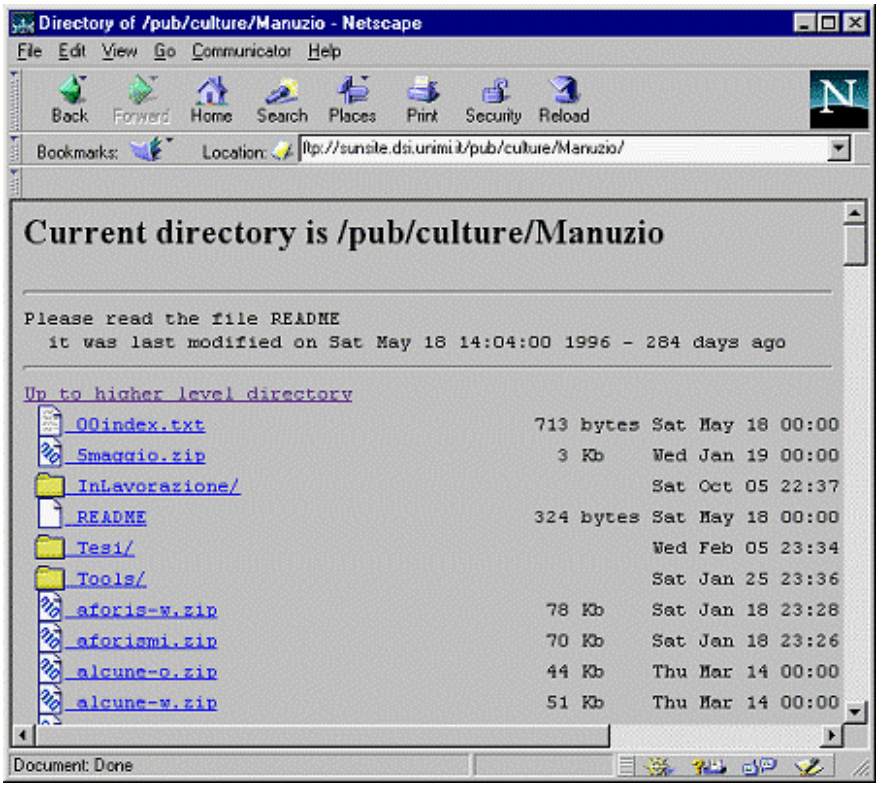
6.2.1 Netscape e l'FTP anonimo

Il client FTP di Netscape è fortemente integrato con le altre funzionalità del programma. Per collegarsi con un sito FTP tramite Netscape è sufficiente inserire la URL del sito che vogliamo raggiungere (se il sito è ad esempio 'sunsite.dsi.unimi.it', la relativa URL sarà 'ftp://sunsite.dsi.unimi.it') dopo aver fatto clic con il mouse sul bottone 'Open Page' presente all'interno della barra degli strumenti, così come illustrato nella figura che segue:



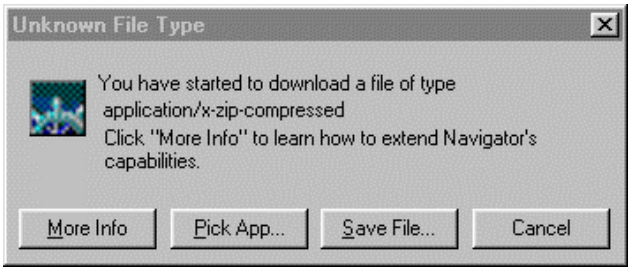
L'apertura di una sessione FTP con Netscape

Notare che è possibile inserire la URL completa di path (ftp://sunsite.dsi.unimi.it/pub/culture/Manunzio/), così da saltare direttamente alla subdirectory che ci interessa. Con Netscape la procedura iniziale di login, durante la quale solitamente si inserisce 'anonymous' alla voce utente, e il proprio recapito e-mail in luogo della password, si salta: provvede il programma a spedire automaticamente queste informazioni. Nella figura seguente, riportiamo una schermata tipo di una sessione FTP di Netscape.



Il client FTP di Netscape

La sua interpretazione è molto semplice. I 'foglietti bianchi' e quelli con '010' sono file generici, i 'foglietti con le righe' sono file di testo (per leggerli è sufficiente farci clic sopra con il mouse, il che equivale al 'get nome_file -' dell'FTP con interfaccia a caratteri), le 'cartelle', infine, sono le directory. Per entrare in una directory, o per prelevare un file, basta un clic del mouse. In quest'ultimo caso, dopo qualche secondo, compare un box simile a quello della figura che segue:



Il box di Netscape che compare dopo aver cliccato su un file in una sessione FTP

Per trasferire il file sul proprio hard disk, a questo punto, non si deve fare altro che un clic su 'Save File...' e attendere che il trasferimento sia completo (possono essere necessari alcuni secondi o molti minuti: dipende dalla dimensione del file, e dalla velocità del proprio collegamento).

6.2.2 Netscape e FTP con account

Il funzionamento di Netscape in una sessione FTP con account è identico a quello di una sessione anonima. Aggiungiamo solo un paio di note su come si forniscono al sistema remoto il proprio codice e la propria password e su come si invia un file (ovvero su come si effettua l'equivalente di un PUT). Non si tratta, al momento, di un metodo propriamente amichevole — è probabile che le versioni future di Netscape finiscano per adottare un modulo FTP più vicino a quello disponibile in client specifici come Cute FTP (v. oltre).
A partire dalla versione 2.0 di Netscape, l'inserimento del codice e della password avviene a livello di indirizzo; quando si indica a Netscape l'indirizzo del computer al quale ci vogliamo collegare, dobbiamo aggiungere il codice e la password secondo questa sintassi:

- ftp://codice:password@sito

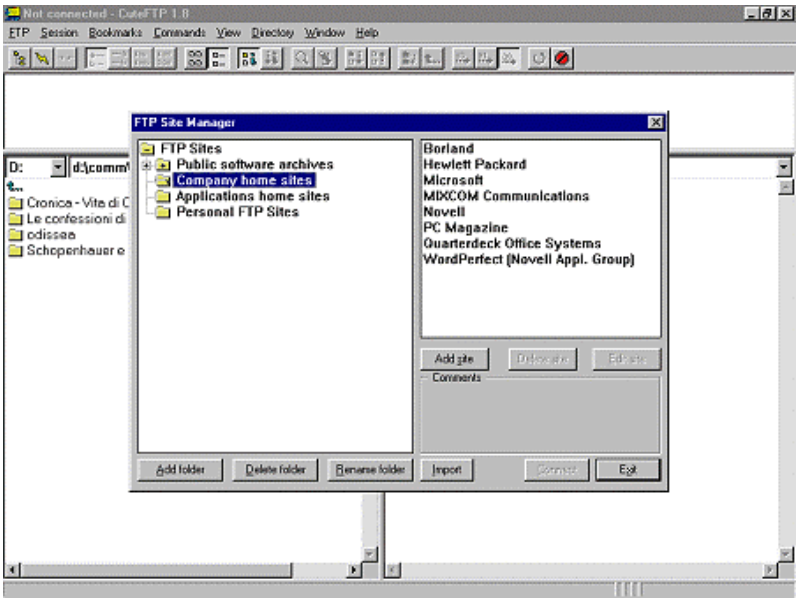
Ovvero: 'ftp://' + il proprio codice + ':' + la propria password + '@' + l'indirizzo del server FTP vero e proprio. Ad esempio, se vogliamo collegarci a MC-link (indirizzo del server FTP: 'ftp.mclink.it'), con codice 'MC0000' e password 'abcd.1', dobbiamo scrivere:

- ftp://MC0000:abcd.1@ftp.mclink.it

Da notare che la password non deve contenere né il carattere ':' (due punti) né il carattere '@'. Nel caso ci fosse uno di questi due caratteri, le uniche alternative sono quelle di modificare la password, o di adottare un altro client FTP.
Un altro limite di questo sistema è che nel digitare la password, questa rimane in chiaro sul video, aumentando il rischio che qualcuno la veda. Perciò: prudenza!
L'invio di un file (put) con il client FTP di Netscape (possibile solo a partire dalla versione 2.0 del programma) si effettua semplicemente con un clic sul comando 'Upload file...' che troviamo sotto il menu 'File' una volta posizionatici nella directory di destinazione.

6.2.3 CuteFTP

Il client FTP di Netscape è comodo quando dobbiamo prelevare un file medio-piccolo tramite una sessione anonima; in altre circostanze è preferibile utilizzare un client FTP specifico, che oltre a fornire un maggior numero di comandi, solitamente garantisce anche prestazioni migliori in termini di velocità di trasferimento.
Non potendo esaminare ogni singola applicazione esistente per i diversi sistemi operativi, forniamo sinteticamente delle indicazioni sul client CuteFTP per Windows 95 di Alex Kunadze (e-mail: alex@sbk.trigem.co.kr). Si consideri tuttavia che esistono prodotti più o meno simili per qualità e funzionalità per quasi tutti i sistemi operativi (nello specifico, CuteFTP è disponibile anche per Windows3.x). Alcune comode caratteristiche, inoltre, come la rubrica interna di indirizzi FTP, sono quasi universali. Potete reperire una copia del programma CuteFTP sul sito http://www.cuteftp.com/.
Nella figura che segue potete vedere la schermata iniziale, con attiva la rubrica di indirizzi FTP. Il programma viene distribuito con alcuni indirizzi FTP già impostati, selezionati tra i più famosi (es.: il sito FTP della Microsoft, ftp://ftp.microsoft.com) o i più utili, come gli archivi — veramente vasti e aggiornati — di programmi di pubblico dominio CICA (ftp://ftp.cica.indiana.edu), GARBO (ftp://garbo.uwasa.fi) e SimTel (ftp://ftp.coast.net).



Il client CuteFTP di Alex Kunadze

La filosofia che è alla base del funzionamento dei client grafici è, fortunatamente, molto razionale: il programma, o meglio, questo tipo di programmi, suddivide generalmente lo schermo in quattro sezioni. La prima, in alto, costituisce una fila di bottoni, che vengono associati ai comandi più frequentemente utilizzati. In CuteFTP, ad esempio, il primo bottone in alto a sinistra richiama la rubrica di indirizzi, il gruppo di bottoni dal quarto al settimo determina il criterio di ordinamento dei file (alfabetico, alfabetico inverso, in base alla data, in base alla dimensione) e così via.
La seconda sezione, larga quanto tutto lo schermo, ma di norma piuttosto sottile (è comunque possibile ridimensionarla), è la finestra destinata ai messaggi inviatici dal sistema remoto; tipicamente, in questa finestra controlleremo se il login è avvenuto correttamente, e se il trasferimento di un file è andato a buon fine oppure no.
La terza e la quarta sezione (nella figura parzialmente coperte dalla rubrica) occupano la maggior parte dello schermo e presentano, quella di sinistra, il contenuto dell'hard disk dell'utente, e quella di destra il contenuto dell'hard disk remoto. Per trasferire un file dal sito FTP fino al proprio computer, non si deve fare altro che 'prendere' con il mouse l'icona relativa e trascinarla nella sezione a sinistra dello schermo. Il processo inverso permette di effettuare una operazione di upload (dal nostro computer al sistema remoto). Il prelievo e l'invio di più file sono possibili semplicemente selezionando più icone.
Anche per i programmi con interfaccia grafica valgono le considerazioni fatte a proposito del prelievo di file binari anziché di testo. In CuteFTP il tipo di trasferimento si determina con il comando 'Transfer type' che troviamo sotto il menu 'FTP'. Ci sono 3 opzioni: 'binary', 'ASCII' e 'auto'. Si può lasciare tranquillamente attivo il riconoscimento automatico di trasferimento, non abbiamo mai notato problemi; e nella remota eventualità che un trasferimento non parta in modalità binaria automaticamente, c'è sempre il comodo bottone 'Stop', che consente di interrompere qualsiasi operazione in corso. In CuteFTP tale bottone si trova nella porzione in alto a destra del video.
L'uso di programmi come CuteFTP è molto semplice, e non vale la pena soffermarvisi oltre. Come nota conclusiva, per gli utenti che facessero un uso evoluto di FTP, segnaliamo che la versione più recente di CuteFTP ha integrato una funzione estremamente utile: i 'Custom Commands' (sotto il menu 'Commands'), che permettono di attivare anche con l'interfaccia grafica particolari procedure, personalizzabili. Ad esempio, il 'Change Files Access Mask' consente di modificare gli attributi di protezione dei file con sintassi Unix (utile a chi gestisce da casa un sito FTP pubblico ospitato — come accade quasi sempre — su un sistema Unix, oppure a chi ha pubblicato pagine Web su siti che richiedono particolari procedure di attivazione). La versione registrata di CuteFTP consente anche il 'resume' automatico di download interrotti.

7. COLLEGAMENTO REMOTO ALLA RETE

7.1 SLIP E PPP

I protocolli SLIP e PPP permettono di stabilire una connessione TCP/IP su un collegamento seriale, quale è il collegamento via modem e cavo telefonico, consentendo così all'utente di collegarsi ad Internet anche da casa.
Lo SLIP è stato il primo ad essere sviluppato, ed è tecnologicamente più arretrato: infatti non prevede alcun controllo sulla stabilità del collegamento e nella sua versione originale richiede l'assegnazione di indirizzi fissi ad ogni computer che si collega. Il suo vantaggio era la facilità di implementazione che ne ha permesso una rapida diffusione presso i cosiddetti access provider. Ma ormai SLIP è stato quasi ovunque rimpiazzato dal Point-to-Point Protocol. Il PPP è un protocollo molto efficiente. Esso prevede sistemi di controllo della trasmissione e permette con semplicità l'assegnazione dinamica degli indirizzi IP: quando un utente effettua la connessione via modem, riceve un indirizzo che rimane assegnato al suo computer solo per il tempo della connessione, e che rimane poi libero per altri utenti. Per funzionare sia SLIP sia PPP richiedono l'installazione dei rispettivi moduli software tanto sul computer che chiede il collegamento quanto su quello che lo fornisce. Quest'ultimo naturalmente deve essere dotato di una connessione diretta ad Internet e deve avere a disposizione un certo 'pacchetto' di indirizzi ufficiali. Quando arriva una richiesta di connessione, il modulo PPP assegna al computer chiamante un indirizzo Internet che gli permette di essere individuato dagli altri host di Internet, e dunque di ricevere o inviare direttamente informazioni attraverso la rete. La connessione tramite SLIP, e ora tramite PPP, ha rappresentato sicuramente un notevole progresso nella connettività di rete per quel che riguarda Internet, ed ha permesso la diffusione di un 'vero' collegamento in rete anche presso l'utenza finale non professionale. Tuttavia tale tipo di connessione presenta anche alcuni limiti. In primo luogo, quello rappresentato dalla scarsa velocità e portata della rete telefonica, soprattutto se non si dispone di un collegamento ISDN. Infatti, la trasmissione di informazioni multimediali richiede lo spostamento di decine o centinaia di kilobyte, che, anche alle velocità massime attualmente supportate dalle connessioni via modem, richiedono attese spesso lunghe. Questo comporta naturalmente alti costi per l'utente finale. Tuttavia la diffusione di modem che supportano il protocollo V/34, in grado di offrire transfer-rate effettivi intorno ai tremila byte al secondo, ha costituito un notevole passo in avanti. Una alternativa più efficiente alla comunicazione su linee telefoniche analogiche è rappresentata dalla già citata tecnologia ISDN (Integrated Service Data Network). Si tratta di un sistema di trasmissione digitale che usa il normale cavo telefonico, e che consente una velocità minima di 64 Kbit al secondo — corrispondenti a circa ottomila byte al secondo. I costi di questa connessione sono mediamente più elevati di quelli della normale linea telefonica ma, in attesa di una futura estensione delle linee in fibra ottica fino alle abitazioni private, ISDN offre all'utente della rete un indubitabile salto di prestazioni.
Il secondo problema delle connessioni PPP è che il software può essere di difficile configurazione per un utente inesperto, poiché sono richieste alcune conoscenze tecniche sul funzionamento dei protocolli TCP/IP. Ma anche questo problema è ormai almeno in parte risolto. Infatti i sistemi operativi delle ultime generazioni integrano i moduli PPP in modo nativo, e offrono delle interfacce notevolmente semplificate per configurare i parametri necessari alla connessione. I protocolli base per la connettività a Internet sono già disponibili direttamente nei sistemi operativi Unix, Windows 95 e NT, Macintosh 7.5, OS/2 Warp. Ce ne occuperemo in dettaglio nel prossimo capitolo.

8. LA POSTA ELETTRONICA

8.1 CONCETTI DI BASE

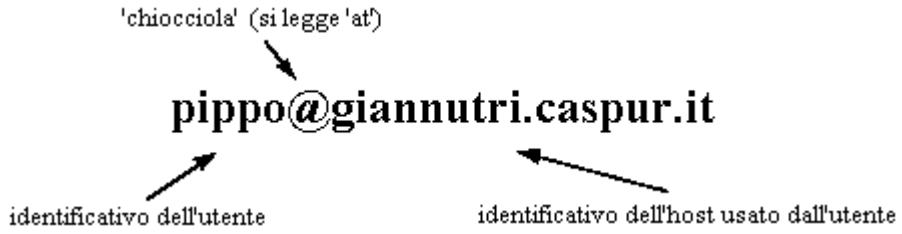
Iniziamo adesso l'esame sistematico delle varie funzionalità messe a disposizione da Internet, partendo dalla prima e forse più nota: la posta elettronica, o e-mail. Tramite la posta elettronica è possibile scambiarsi in tempi estremamente ridotti sia messaggi (file di puro testo) sia, utilizzando gli opportuni strumenti, ogni altro tipo di file.

8.1.1 Indirizzo e casella postale

Condizione indispensabile per lo scambio di un messaggio attraverso la posta elettronica è che mittente e destinatario siano 'su Internet', dispongano cioè di un proprio 'indirizzo' (e-mail address). L'indirizzo ci è assegnato dal nostro fornitore di connettività, e corrisponde a una sorta di casella postale ospitata dal computer al quale 'telefoniamo' al momento di collegarci ad Internet: in sostanza, uno spazio sul suo disco rigido, nel quale i messaggi che ci sono indirizzati vengono depositati automaticamente. Questo significa, fra l'altro, che non c'è bisogno che il nostro computer sia perennemente collegato ad Internet, in attesa dei messaggi che ci potrebbero arrivare: è il computer del fornitore di connettività che si assume questo incarico per noi. Dal canto nostro, quando decideremo di collegarci controlleremo nella nostra casella postale se ci sono messaggi in attesa: in sostanza, il computer di chi ci fornisce l'accesso a Internet funziona un po' da segreteria telefonica, ricevendo per noi i messaggi che arrivano mentre non ci siamo (cioè mentre non siamo collegati), e informandocene alla prima occasione. Vediamo innanzitutto come è fatto un indirizzo di posta elettronica. La sua forma generale è la seguente:

- nomeutente@nome.host.computer

La parte di indirizzo alla sinistra del simbolo @ (detto 'chiocciola' o, con riferimento al suo significato all'interno di un indirizzo Internet, 'at') identifica l'utente in maniera univoca all'interno del sistema informatico che lo ospita (host system); spesso si tratterà del nostro cognome, o di un codice, o di un nomignolo che ci siamo scelti. L'importante è che non ci siano due utilizzatori di quel sistema con lo stesso identificativo. La parte di indirizzo a destra del simbolo @ identifica invece in maniera univoca, all'interno dell'intera rete Internet, il particolare sistema informatico presso il quale l'utente è ospitato, e corrisponde all'indirizzo simbolico dell'host. L'indirizzo di un utente denominato 'Pippo' collegato all'host denominato giannutri.caspur.it sarà dunque



Un indirizzo Internet: l'identificativo dell'host è sempre in forma gerarchica.

Come è facile comprendere, la procedura appena descritta di 'costruzione' di un indirizzo di posta elettronica garantisce che esso identifichi univocamente l'utente all'interno dell'intera rete Internet.
Di norma il nostro indirizzo di posta elettronica ci viene indicato dal fornitore di connettività al momento di stipulare il contratto di abbonamento (o, nel caso di un fornitore istituzionale come un centro di calcolo universitario, al momento dell'attivazione amministrativa del nostro accesso). Sarà proprio questo l'indirizzo che dovremo comunicare ai nostri corrispondenti, e magari (è diventato di moda) far stampare sul nostro biglietto da visita.

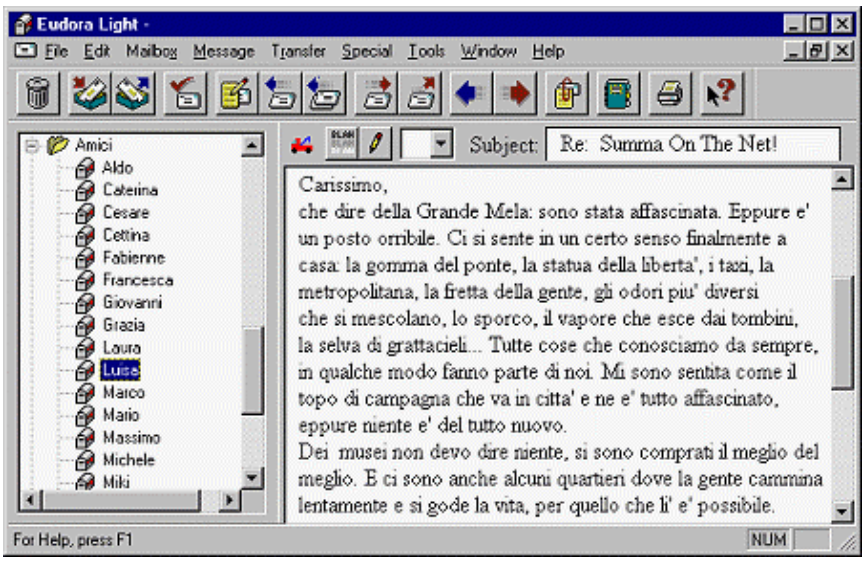
8.1.2 Messaggi personali

L'utilizzazione più elementare della funzione di posta elettronica è lo scambio di messaggi di testo fra due persone, una che spedisce e una che riceve. Si tratta di una operazione assai intuitiva, e simile alla normale spedizione di una lettera. Vediamo come è fatta una di queste lettere elettroniche nella sua forma più completa, ma come vedremo per certi versi anche più 'primitiva'. Va infatti tenuto presente – e lo verificheremo direttamente tra breve — che i programmi avanzati di gestione della posta elettronica, come Eudora, di solito 'filtrano' automaticamente il messaggio, evitando (a meno che non la si richieda esplicitamente) la visualizzazione delle informazioni che in genere interessano meno, come i dettagli sull'itinerario seguito dalla lettera, e impaginandolo in maniera graficamente più piacevole.
I numeri di riga sulla sinistra del messaggio sono stati aggiunti per facilitare la spiegazione, il nome originale del mittente è stato sostituito con 'NOME'.

```
01 ========================================
02 MAILBOX
03 Msg# 78465, 03/10/94 01:24 [1049]
04 Da: NOME@hkucc.hku.hk
05 A : MC3430 Gino Roncaglia
06 ----------------------------------------
07 Oggetto: Mesino
08
09 From ammi.mclink.it!hkucc.hku.hk!nome Mon Oct 3
10 1:24:16 1994 remote from ax433
11 Received: from hkucc.hku.hk by ammi.mclink.it id
12 aa24617; 3 Oct 94 1:24 CET
13 <01HHU06GJ7ME0020RP@hkucc.hku.hk>; Mon, 3 Oct 1994
14 Date: Mon, 03 Oct 1994 08:29:37 +0800
15 From: NOME@hkucc.hku.hk
16 Subject: Mesino
17 To: MC3430@mclink.it
18 Message-id: <01HHU06GJ7MG0020RP@hkucc.hku.hk>
19 X-Envelope-to: MC3430@mclink.it
20 X-VMS-To: IN%"MC3430@mclink.it"
21 MIME-version: 1.0
22 Content-transfer-encoding: 7BIT
23
24 Dear Gino,
25 I was interested to hear that Mesino takes the
26 cassatio/ungrounded approach, and wonder what he
27 would have made of the `strengthened' Liar. If you
28 could send me your papers about Mesino, I'd be
29 grateful.
30 Best wishes
31 (Firma)
```

Esaminiamo la lettera più da vicino.
La parte iniziale (dalla riga 01 alla riga 08) riguarda l'identificazione di messaggio, mittente e destinatario all'interno di MC-link, il fornitore di connettività utilizzato in questo caso, e non appartiene dunque al messaggio come tale. Chi usa altri sistemi di accesso a Internet troverà che nei messaggi di posta elettronica da lui ricevuti questa sezione è diversa, o — più frequentemente — del tutto assente.
La sezione da riga 09 a riga 23 (chiamata 'header', intestazione; in italiano è a volte usato anche il termine 'busta') serve invece ad identificare il messaggio all'interno della rete Internet, specificandone fra l'altro mittente (a riga 15), destinatario (a riga 17), oggetto (a riga 16), data e ora di spedizione (a riga 14), e la 'strada' che il messaggio ha percorso nella rete per arrivare dal mittente al destinatario, con l'indicazione delle principali tappe fatte e dei relativi orari di ricezione

(da riga 9 a riga 13). La riga 18 fornisce un codice identificativo univoco del messaggio, le righe 19-22 forniscono ulteriori indicazioni delle quali in questa sede non ci preoccuperemo.
Il messaggio vero e proprio va da riga 24 a riga 31.
L'identificazione del mittente (riga 15) e del destinatario (riga 17) del messaggio sono fatte utilizzando il loro 'indirizzo di posta elettronica' (e-mail address).
La figura seguente fornisce un altro esempio: questa volta, si tratta di una lettera 'letta' attraverso un programma grafico avanzato, il già ricordato Eudora.



Il programma per la gestione della posta elettronica Eudora Light (versione 3.01)

Anche in questo caso, qualche nota di commento. Il messaggio è in italiano, e una prima cosa che può colpire è l'uso degli apostrofi al posto degli accenti. Perché e' al posto di è, liberta' al posto di libertà, e così via? La tastiera del computer non ha forse le sue brave lettere accentate?
Per comprendere i motivi della (corretta) sostituzione da parte del mittente del messaggio delle lettere accentate con lettere 'apostrofate', va notato che di norma i messaggi di posta elettronica devono comprendere solo caratteri compresi nel cosiddetto set ASCII 'ristretto'. Infatti, ogni carattere trasmesso per posta elettronica è composto di norma di 7 bit, e 7 bit (ciascuno dei quali può assumere uno dei due valori 0 o 1) permettono 27 = 128 combinazioni diverse. Il set ASCII 'esteso' comprende invece 256 caratteri, e presuppone una codifica a 8 bit (28 = 256). È facile capire che, se si vuole utilizzare la codifica basata su 7 bit per carattere, 128 caratteri del set ASCII esteso devono essere 'sacrificati' (si noti come la linea 22 del primo messaggio citato indichi proprio che vengono usati 7 e non 8 bit per carattere). Questo comporta, incidentalmente, che nei messaggi di posta elettronica 'normali' non è possibile inserire lettere accentate (che appartengono alla porzione superiore dell'ASCII alla quale siamo costretti a rinunciare). Occorrerà dunque sostituire le lettere accentate con la corrispondente lettera non accentata seguita da apostrofo (l'apostrofo rientra nell'ASCII ristretto, e viene dunque trasmesso senza difficoltà).
Se ci sono tutti questi problemi, perché non utilizzare l'ASCII esteso? Il problema è che i 128 caratteri 'superiori' o estesi possono variare da paese a paese (e la cosa è abbastanza comprensibile, dato che lingue diverse possono aver bisogno di caratteri diversi). Esistono standard internazionali assai diffusi sull'uso di questi 128 caratteri, ma nessuno è veramente universale: pensate che MS-DOS e Windows fanno al riguardo scelte diverse, il che spiega come mai a volte le lettere accentate di un file di testo creato in un ambiente risultino stranamente trasformate se il file è letto nell'altro.
Considerato che uno degli obiettivi della posta elettronica è proprio quello di non avere confini, risulterà chiaro come questa babele di codifiche rappresenti un ostacolo fastidioso, che viene spesso evitato nel modo più radicale: riducendo l'insieme dei caratteri accettati al solo ASCII stretto, a 7 bit: l'unico veramente universale.
Alcuni sistemi di spedizione 'intelligenti' riescono a evitare il problema, e parecchi programmi avanzati di gestione della posta elettronica (fra i quali Eudora) sono in grado di utilizzare una tabella

di caratteri 'standard' ad 8 bit e quindi di interpretare correttamente le lettere accentate. Ma al momento di spedire un messaggio, come facciamo a sapere con quale sistema sarà letto? E se il destinatario non disponesse che di un vecchio terminale non troppo sofisticato? Inoltre, nel suo viaggio attraverso la rete il messaggio potrebbe comunque incontrare server incapaci di gestire messaggi a 8 bit.
Probabilmente tra pochi anni questi problemi saranno solo un ricordo, ma per adesso le norme della buona educazione (e della praticità) suggeriscono di evitare l'uso delle lettere accentate.
Un altro interrogativo potrebbe sorgere sull'oggetto (subject) del messaggio: come mai non c'entra niente col contenuto? La risposta è semplice: molto spesso, si risponde a un messaggio usando l'opzione 'reply' del proprio programma di gestione della posta elettronica. E, per semplificarci la vita, quest'ultimo inserisce in tal caso automaticamente come oggetto del messaggio l'espressione "Re: xxxxxxxx", dove xxxxxxxx è l'oggetto del messaggio al quale si sta rispondendo, e 'Re:' indica appunto che si tratta di una replica. Se poi il destinatario della nostra risposta risponde a sua volta usando la funzione 'reply', si creano degli scambi epistolari sempre con lo stesso soggetto (ormai quasi tutti i sistemi evitano di costruire in questi casi catene del tipo "Re: Re: Re:..."). Naturalmente, col tempo gli argomenti discussi si spostano da quelli originali sui quali si era avviato lo scambio epistolare, e l'oggetto diviene incongruo. Se vogliamo evitarlo, basterà sostituire all'oggetto indicato automaticamente dal programma un nuovo oggetto, meglio rispondente al contenuto del messaggio.
Un'ultima nota: i due messaggi presi in esame sono stati letti utilizzando strumenti diversi, e questo spiega il loro diverso aspetto. Ma le informazioni che viaggiano su Internet sono sempre dello stesso tipo: una lunga catena di caratteri (o meglio: una lunga catena di 0 e 1 che codificano caratteri), 'impacchettata' e spedita seguendo criteri del tutto analoghi. Dobbiamo abituarci a svincolare l'aspetto esterno di un messaggio — che può dipendere dal programma usato per leggerlo, dal computer che stiamo adoperando, e da altri fattori accidentali — dal suo contenuto informativo.

8.1.3 Circolari

Di norma, tutti i sistemi capaci di inviare posta elettronica permettono anche di inviare, in maniera assai semplice, gli equivalenti informatici delle 'lettere circolari' — messaggi cioè con lo stesso testo e con più di un destinatario. In genere, ciò avviene aggiungendo al testo del messaggio un elenco di destinatari. Non serve invece replicare più volte il corpo del messaggio: sarà il sistema di gestione della posta elettronica che si preoccuperà di farlo per noi.

8.1.4 Il mondo delle liste

Finora, abbiamo considerato i semplici messaggi da persona a persona e le lettere circolari, che vanno da una persona a più persone. Un passo ulteriore avviene con le cosiddette 'liste', che permettono lo scambio di comunicazioni all'interno di un gruppo predefinito di persone. L'idea è semplice: supponiamo che fra gli utenti Internet ve ne siano alcuni che condividono un appassionato interesse per, ad esempio, le piante grasse, o la poesia romantica tedesca, o la musica di Debussy. Queste persone possono entrare in contatto reciproco e scambiarsi messaggi (in modo tale che ogni messaggio spedito da una di loro sia ricevuto da tutte le altre) iscrivendosi a una lista dedicata all'argomento di loro comune interesse.
Come suggerisce il nome, una lista non è altro che un elenco di indirizzi di posta elettronica. Un elenco ospitato da un nodo della rete (che fungerà dunque da 'server' della lista), ed al quale chiunque è interessato ad iscriversi alla lista può aggiungere automaticamente il proprio nome.
Proprio come una persona, una lista dispone di un indirizzo di posta elettronica, al quale vanno scritti i messaggi che vogliamo siano distribuiti agli iscritti. In sostanza, si tratta di una sorta di servizio gratuito di fotocopie e spedizione. Ogni messaggio spedito alla lista da uno qualunque degli iscritti viene automaticamente 'rimbalzato' a tutti gli altri.
A occuparsi di tutte le operazioni connesse alla gestione di una lista (o di più liste) — dall'aggiornamento dell'elenco degli iscritti all'inoltro automatico dei messaggi — è un programma denominato listserver, che risiede sullo stesso computer che ospita la lista. Come funziona un listserver? Semplice: ha anch'esso un proprio indirizzo di posta elettronica (diverso da quello della

lista!), al quale è possibile scrivere messaggi per iscriversi a una delle liste da esso gestita — o per dimettersene. Questi messaggi — normalissimi messaggi di posta elettronica, analoghi a quelli che scriveremmo a una persona — devono tuttavia avere una forma standard, in genere

SUBSCRIBE NOMELISTA

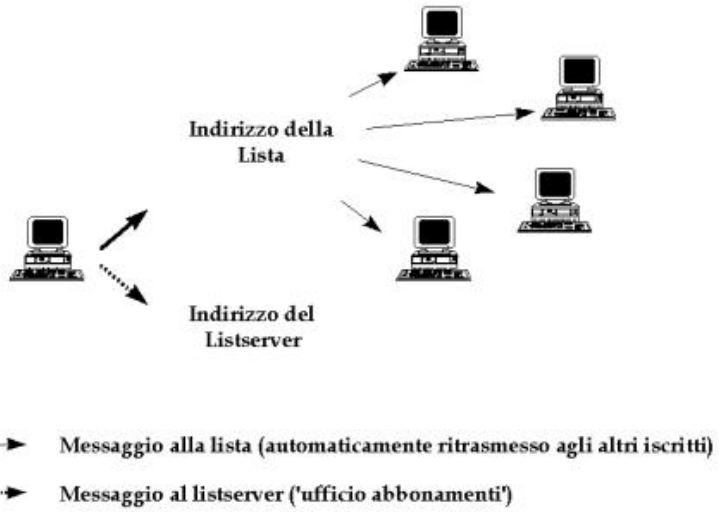
per iscriversi alla lista, e

UNSUBSCRIBE NOMELISTA

oppure

SIGNOFF NOMELISTA

per dimettersene. Per avere un elenco completo dei comandi riconosciuti dal listserver basta di norma mandare al suo indirizzo di posta elettronica un messaggio contenente la sola parola HELP.
Una volta ricevuta la nostra richiesta di iscrizione, il listserver aggiunge automaticamente il nostro nome all'elenco degli iscritti alla lista che ci interessa. D'ora in poi, riceveremo copia di ogni messaggio inviato alla lista da uno qualunque dei suoi membri.
È importante comprendere che il funzionamento delle liste si basa sull'uso di due distinti indirizzi di posta elettronica: quello della lista, a cui spedire i messaggi indirizzati a tutti gli iscritti, e quello del listserver, a cui spedire solo i messaggi che, utilizzando i comandi riconosciuti dal listserver, richiedono di effettuare operazioni amministrative quali l'iscrizione alla lista, le dimissioni, ecc. La situazione è analoga a quella di una rivista: se vogliamo che una nostra lettera sia pubblicata e letta da tutti gli abbonati, la invieremo alla rubrica delle 'lettere al direttore' (una lista è fatta tutta di 'lettere al direttore' — e, se la lista non ha un moderatore, tutte le lettere vengono automaticamente pubblicate!); se vogliamo abbonarci, disdire l'abbonamento, comunicare una variazione di indirizzo, ecc., manderemo invece una lettera alla segreteria abbonati. Così, la lettera 'da pubblicare' va all'indirizzo della lista, quella con richieste amministrative va all'indirizzo del listserver.



Rappresentazione schematica del funzionamento delle mail-list

Il primo esempio che abbiamo fatto è quello di una lista sulle piante grasse. Un esempio scherzoso? Per niente! Su Internet esiste effettivamente — assieme a migliaia di altre, che coprono praticamente ogni campo dello scibile umano — anche una lista sulle piante grasse.
L'elenco delle liste esistenti è sterminato, e cresce al ritmo di 2-3 liste al giorno. Alcune liste sono moderate, possiedono cioè un moderatore umano che decide quali messaggi far 'rimbalzare' dal listserver a tutti gli iscritti. Un moderatore è spesso necessario nel caso di liste con tematiche controverse — ad esempio politiche — per evitare che la lista sia soffocata da messaggi polemici, o addirittura (succede) pieni di insulti.
A puro titolo di esempio, riportiamo di seguito le indicazioni relative a qualche lista:

AMALGAM@ibmvm.rus.uni-stuttgart.de
Mailing list for information about dental amalgam
fillings and chronic mercury poisoning. It may be

of interest for people who have "silver" dental
fillings in their teeth.
BitNet users may subscribe by sending the following
command to
LISTSERV@ds0rus1i via mail or message:
SUBscribe AMALGAM Your_full_name
where "Your_full_name" is your real name, not your
login Id.
Non-BitNet users can join the list by sending the
above command as the only line in the text/body of
a message to
LISTSERV@ibmvm.rus.uni-stuttgart.de
Coordinator: Siegfried Schmitt
< UJ21@ibm3090.rz.uni-karlsruhe.dbp.de > < UJ21@dkauni2 >
AUSTEN-L on LISTSERV@MCGILL1
or LISTSERV@vm1.mcgill.ca
A moderated digest for readers of Jane Austen. If
you enjoy Jane Austen's novels and those of her
contemporaries, such as Fanny Burney, Maria Egeworth
and Maria Wollstonecraft, you might want to exchange
views with others on any aspect of her work and her
time.
Moderator: Dr. Jacqueline Reid-Walsh,
Department of English,
McGill University,
853 Sherbrooke St. West
Montreal, Quebec, H3A 2T6
Subscription requests and contributions should be
sent to: CCMW@MUSICA.MCGILL.CA
CRYONICS
Contact: ...att!whscad1!kqb -or- kqb@whscad1.att.com
(Kevin Q. Brown)
Purpose: Cryonic suspension is an experimental
procedure whereby patients who can no longer be kept
alive with today's medical abilities are preserved
at low temperatures for treatment in the future.
The list is a forum for topics related to cryonics,
which include biochemistry of memory, low
temperature biology, legal status of cryonics and
cryonically suspended people, nanotechnology and
cell repair machines, philosophy of identity, mass
media coverage of cryonics, new research and
publications, conferences, and local cryonics group
meetings.
- Kevin Q. Brown kqb@whscad1.ATT.COM
SCA@MC.LCS.MIT.EDU
Mailing list for members of or anyone interested in
the Society for Creative Anachronism. There is also
an "alt.sca" Newsgroup gatewayed with the mailing
list. All requests to be added to or deleted from
this list, problems, questions, etc., should be sent
to SCA-REQUEST@MC.LCS.MIT.EDU .

Gli esempi sono scelti a caso. Ci sono liste sulle piante carnivore e sui pesci tropicali, sui romanzi di Umberto Eco e sui racconti di fantasmi; liste su usi e costumi di un numero immenso di

popolazioni, dagli Oromo agli Eschimesi; liste su religioni di tutti i tipi (compresa qualcuna sviluppatasi su Internet); liste scientifiche, liste economiche, liste politiche; naturalmente, centinaia di liste riguardano l'informatica (liste per gli utilizzatori di un determinato programma, o di un determinato modello di computer). Vi sono liste pubbliche e liste riservate (ad esempio, liste destinate a tenere in contatto fra loro i dipendenti di un'azienda, magari sparsi per il mondo).
Fra le migliaia di liste disponibili su Internet, alcune sono a 'forte traffico' (potete aspettarvi di ricevere anche diverse decine di messaggi al giorno), altre sono tranquille (uno o due messaggi la settimana). Si tratta veramente di un mare di informazione, che si aggiunge a quello rappresentato dalle conferenze, sulle quali ci soffermeremo tra breve. Non stupisce che, parlando di Internet, si usino metafore quali 'esplorare' e 'navigare'!

8.1.5 Come trovo le liste che mi interessano?

La domanda sorge spontanea, davanti a un'offerta di informazione tanto abbondante e tanto disordinata.
Fino a un paio di anni fa, uno strumento utile era la 'lista di liste' reperibile un po' ovunque sulla rete. Ormai, si tratta di elenchi talmente estesi da risultare di lettura quasi impossibile. Comunque, alla URL http://www.neosoft.com/internet/paml/ trovate uno di questi elenchi in una forma accessibile, indicizzato per parole chiave.
Una buona strada per trovare liste (e i loro listserver) è quello di consultare elenchi 'settoriali' di liste: ne esistono numerosi (dall'agricoltura all'astronomia, dalla letteratura all'economia). Potete trovarli, insieme a un gran numero di elenchi di risorse 'settoriali' disponibili su Internet, all'indirizzo http://www.clearinghouse.net. Una lista di liste molto completa e divisa per settori, sulla quale effettuare ricerche, può essere scaricata dall'indirizzo http://www.internetdatabase.com/maillist.htm; si tratta di una vera e propria base di dati, che può essere aggiornata attraverso l'iscrizione (gratuita) a... una apposita lista, naturalmente!
Uno strumento ulteriore e assai potente per trovare liste su (praticamente) qualsiasi argomento è raggiungibile alla URL http://www.liszt.com; si tratta di una base di dati interrogabile direttamente via Internet, che vi consentirà di effettuare ricerche per parole chiave, contenute non solo nel nome della lista, ma (quando disponibile) anche nella sua descrizione. Un altro motore di ricerca su liste, decisamente meno completo ma talvolta utile, è all'indirizzo http://catalog.com/vivian /interest_group -search.html.
Infine, tenete presente che una conferenza preziosa (vedremo tra breve cosa sono le conferenze o newsgroup Internet) è quella denominata news.lists, che fornisce informazioni quotidiane sulle liste e sui newsgroup esistenti. A tale conferenza corrisponde la lista new-list, che ha il solo scopo di informare sulle nuove liste create in rete: è possibile ricevere tutte le informazioni necessarie ad iscriversi e utilizzare al meglio questa lista inviando un messaggio di posta elettronica all'indirizzo listserv@vm1.nodak.edu; il messaggio deve contenere solo le parole 'get new-list readme'.

8.1.6 Usare la posta elettronica per trasmettere file

Come si è accennato, la posta elettronica può divenire, con opportuni accorgimenti, anche uno strumento per la trasmissione di file binari: programmi, file di testo 'formattati' realizzati con programmi di word processing, immagini, ecc.
Le limitazioni imposte dalla necessità di usare il set ASCII stretto, già ricordate discutendo la difficoltà di trasmissione via posta elettronica di caratteri non standard come le lettere accentate, rendono impossibile la trasmissione di un file binario lasciandolo così com'è. Per poterlo spedire, occorre codificare il file in modo da utilizzare solo l'ASCII stretto. A questa 'riscrittura' (e alla relativa decodifica al momento della ricezione del file) possono provvedere vari strumenti: un programma di gestione di posta elettronica (in genere in modo per noi automatico e trasparente) o programmi appositi, da utilizzare al momento del bisogno.
La prima alternativa è decisamente preferibile. Gestori avanzati di posta elettronica (come Eudora, Pegasus, Netscape Messenger, Microsoft Internet Mail) permettono di indicare i file da spedire navigando attraverso gli abituali 'click' del mouse in una finestra che ci presenta il contenuto del nostro disco rigido. Si tratta di una funzione denominata file attachment, dato che il file che vogliamo spedire viene 'allegato' a una lettera di accompagnamento. Vedremo fra breve, considerando i principali programmi di gestione della posta elettronica, in che modo compiere, caso per caso, questa operazione.
Al momento della ricezione del messaggio, il file sarà decodificato automaticamente e salvato sul nostro disco rigido. Il salvataggio avviene di norma in una directory che avremo indicato, una volta per tutte, con l'impostazione iniziale del programma di gestione della posta elettronica. Se non riuscissimo a ritrovare i file 'attaccati' a un messaggio appena ricevuto, occorrerà quindi controllare le impostazioni di tale programma, e verificare quale sia la directory prescelta per il salvataggio dei file.
In genere, la codifica dei file avviene utilizzando il cosiddetto standard MIME (Multipurpose Internet Mail Extensions), anche se molti fra i programmi che esamineremo permettono anche la codifica e la decodifica nel formato BIN-HEX proprio del mondo Macintosh. L'utente non ha comunque bisogno di sapere nulla sul funzionamento di questi standard di codifica: è il programma a preoccuparsi di tutto.
La possibilità di codifica e decodifica automatica di un file è offerta anche da alcuni programmi 'a caratteri' per la gestione della posta, come pine, disponibile su molti sistemi Unix.
Se invece disponiamo di programmi meno sofisticati, dovremo codificare 'a mano' gli eventuali file da spedire. Un formato spesso usato in questi casi è uuencode/uudecode. Chi spedisce il file provvede, prima, a codificarlo attraverso uno dei numerosi programmi in grado di effettuare l'operazione di uuencoding; chi lo riceve, avrà bisogno di un programma che effettui l'uudecode. In genere, un programma uuencode si preoccupa anche, a richiesta, di 'spezzare' il file originario in più parti, per evitare problemi con quei sistemi che non permettono di spedire messaggi più lunghi di 20-30 Kb. In questo caso, oltre a decodificare il file, uudecode ne riunisce i pezzi. Un messaggio contenente un file 'uuencodato' ha una forma di questo tipo:

```
01 ------------ Part 1 of 3 ------------
02 begin 644 MENTAL.ZIP
03 M4$L#!!0``/>&#AL'1_>P54```"2@`,`34533TQ$148N1$]#U'T)
04 MG&1)66=T@\-T(!5!9DYE757%S!3U=W373/=TT57T=,,*Q"9&949
05 '5E>#,AQ>ZRHHB#Z`Q3&`W%%=]=K7?<05W;=55!`17%%!<]5%P6'
06 [\C,ZD%E?^M.SS^K*O.]>'%\\5WQ?5_^]OUU<>76&QXNZ+^Z*/Z[
.....
96 M8NBV$-\61PY#*_/A,GI(UDPYF`N3F_<ZT7]_&`,28]%ZEYL4U"\
97 MJ9B?3(?:Y2#SYE/%!K&*-6P:."\&3\/.$C'\;.RD8=9/.0\F9!3
98 -------- End of part 1 of 3 --------
```

La riga 1 informa che abbiamo a che fare con il primo messaggio relativo a un file 'spezzato' in tre messaggi: l'espressione 'begin' della riga 2 informa uudecode che a partire dalla riga seguente inizia la parte 'codificata' (alla fine del file, e quindi nel terzo dei nostri tre messaggi, si troverà la corrispondente istruzione 'end'). La riga 2 fornisce anche il nome del file che è stato codificato e che dovrà essere ricostituito (nel nostro caso, 'mental.zip').

8.2 I PROGRAMMI PER LA GESTIONE DELLA POSTA ELETTRONICA

8.2.1 Programmi con interfaccia a caratteri

Come si è già accennato, per utilizzare la posta elettronica non è necessario disporre di computer particolarmente sofisticati. Le funzioni di base (scrittura, spedizione, ricezione, lettura di un messaggio) possono infatti essere eseguite egregiamente attraverso programmi assai spartani, che utilizzino una interfaccia a caratteri.

In genere, chi — collegandosi alla rete da casa e via modem — fa uso di programmi di questo tipo, accede a Internet in modalità 'terminale': il suo computer diventa cioè una sorta di terminale remoto del sistema che fornisce la connettività (è un po' come se monitor e tastiera fossero collegati, anziché al computer di casa, direttamente a quello remoto). Il tipo di programma di gestione della posta elettronica utilizzato dipenderà quindi dall'ambiente di lavoro offerto dal computer al quale ci si collega. Se si tratta di un computer Unix, con ogni probabilità sarà presente almeno il più semplice fra i programmi di questo tipo, denominato — senza troppa originalità — mail.

Al momento della connessione, mail vi informerà dell'esistenza di posta in attesa nella vostra casella postale con il messaggio

You have new mail.

Se a questo punto digitate 'mail' e battete il tasto 'Invio', avrete un elenco dei messaggi in attesa abbastanza simile al seguente:

```
%mail
Mail version SMI 4.0 Tue Feb 25 11:48:20 1997
Type ? for help
"usr/spool/mail/roncagl": 4 messages 4 new
>N 1 nome1@suo.sistema Mon Feb 24 19:33 Come va?
 N 2 nome2@suo.sistema Mon Feb 24 21:11 Spedizione
 N 3 nome3@suo.sistema Mon Feb 24 22:40 Re:il senso della vita
 N 4 nome4@suo.sistema Sat Feb 24 23:03 New book
&
```

La e commerciale (&) indica che mail aspetta un vostro comando. Per sapere quali sono i principali comandi che avete a disposizione, basta chiedere aiuto con il comando '?'. Il simbolo '>' davanti al messaggio numero 1 indica che si tratta del messaggio 'attivo' — quello al quale si riferiranno i vostri eventuali comandi.

Per leggere un messaggio, è sufficiente indicarne il numero (compare dopo la N) e premere il tasto 'Invio'.

Tra i comandi utili, 'r' permette di rispondere al messaggio selezionato; una volta dato il comando 'r' (e premuto 'Invio') si può iniziare a scrivere la risposta. L'editor a disposizione per questa operazione è un editor di linea piuttosto rudimentale (ciò significa, ad esempio, che potete

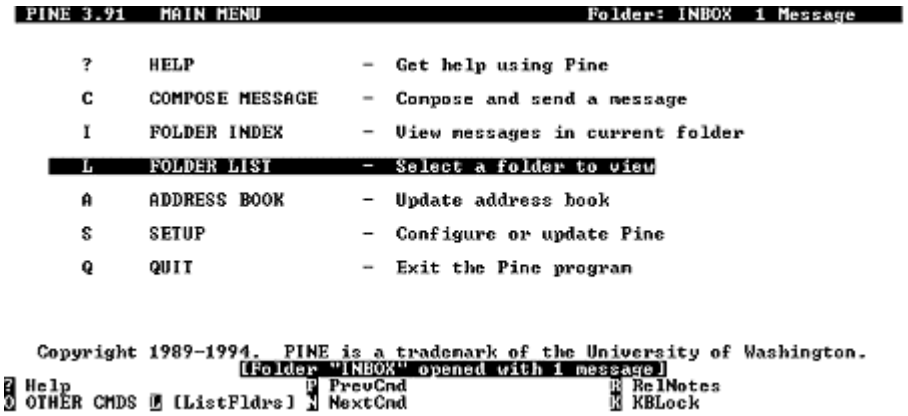
correggere, usando il tasto backspace, solo gli errori che si trovano sulla linea di testo sulla quale state lavorando), ma in fondo svolge le sue funzioni. Se non siete soddisfatti di quello che state scrivendo, potete abbandonare usando la combinazione di tasti 'Control-C'. Per indicare invece che avete finito di scrivere, e che il messaggio può essere spedito, basterà andare a capo, iniziare la nuova riga con un punto '.' e andare ancora a capo. Se volete spedire un messaggio nuovo (anziché rispondere a un messaggio che avete ricevuto) basterà richiamare il programma mail facendo seguire a 'mail' l'indirizzo di posta elettronica del destinatario, in questo modo:

- mail pippo@topolinia.net

Naturalmente voi userete l'indirizzo del vero destinatario! Potrete poi scrivere il messaggio, e terminarlo con il solito '.' su una riga vuota.
Fra gli altri comandi fondamentali, 's' seguito dal nome di un file salverà il messaggio corrente; se volete salvare più messaggi contemporaneamente, potete anche aggiungere, dopo la 's', i numeri dei messaggi da salvare. Ad esempio:

- s 2 4 ufficio

salverà i messaggi 2 e 4 in un file chiamato 'ufficio', dove potreste voler archiviare tutti i messaggi di lavoro. Il comando 'd' permette di cancellare i messaggi che non si ritenga di voler conservare; anche in questo caso, è possibile cancellare più messaggi indicandone i numeri.
I comandi disponibili sono parecchi e non possiamo in questa sede considerarli tutti, ma ricordate sempre il prezioso comando '?', e la regola secondo cui il miglior sistema per imparare è fare esperimenti.
Una variante abbastanza diffusa di mail è mailx; programmi più avanzati di gestione della posta elettronica (sempre disponibili sotto Unix) sono elm e pine. Elm è un programma flessibile, e può essere impostato per scrivere messaggi usando il vostro editor preferito (il cui nome va indicato nel file .elmrc; naturalmente si deve trattare di un editor disponibile sul sistema che state utilizzando). La schermata di elm presenta sempre, in basso, un elenco dei principali comandi disponibili; anche in questo caso, il comando '?' vi fornirà un aiuto. Per saperne di più su elm, potete procurarvi attraverso FTP sul sito rtfm.mit.edu, directory pub/usenet/news.answers/elm, il file 'FAQ', che contiene una presentazione completa del programma.
Pine è decisamente una delle migliori alternative fra i programmi di gestione della posta elettronica esistenti sotto Unix. Se è disponibile sul vostro sistema, potete attivarlo, al solito, digitando il suo nome: 'pine' 'Invio'.
La finestra iniziale del programma è quella riportata nella figura seguente.



Pine, uno dei migliori programmi per la gestione della posta elettronica sotto Unix

Se volete scrivere un messaggio (potete farlo dallo schermo principale con il comando 'C') pine vi offrirà, a differenza di mail, un buon editor di schermo (i cui comandi di base sono gli stessi del diffuso editor per Unix denominato pico). Potete scrivervi i vostri messaggi: una volta terminati, li spedirete con il comando 'Control-X'.
Pine permette di separare i messaggi in folder (cartelle) e crea automaticamente la cartella-base 'Inbox', nella quale sono conservati i messaggi che vi sono arrivati. 'Inbox' funziona come cartella

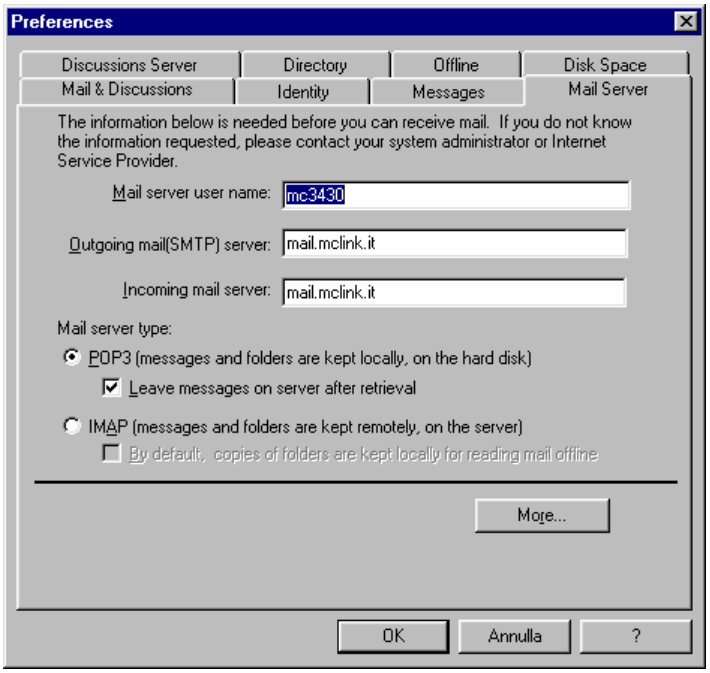
attiva quando entrate nel programma. Ciò significa che per vedere un elenco dei messaggi in attesa vi basterà dare il comando 'I', che porta a un indice della cartella attiva.
Tra i vantaggi di pine, è anche la possibilità di creare una rubrica di indirizzi, nella quale associare 'nickname' — cioè nomi abbreviati delle persone con le quali abbiamo uno scambio di corrispondenza frequente — e relativi indirizzi di posta elettronica. Una volta creata la rubrica, potrete ad esempio scrivere a pico.de.paperis@university.of.paperopoli.edu inserendo nel campo 'To:' solo il nome 'Pico'. Alla rubrica si arriva, partendo dalla schermata introduttiva, con il comando 'A' (address book).
Come si è accennato, pine rende assai facile la spedizione di file 'collegati' a un messaggio di posta elettronica. Nella pagina di composizione di un nuovo messaggio, dovete portarvi usando il tabulatore sul campo 'Attachment', e usare quindi il comando 'Control-j'. Il programma vi chiederà il nome del file da spedire, e un eventuale commento.
Attenzione, però: se vi collegate da casa e volete spedire un file, usando pine (a differenza di quanto accade con programmi che sfruttano un collegamento SLIP o PPP, come Eudora, Pegasus, Netscape Messenger o Microsoft Internet Mail) dovrete prima trasferirlo nella vostra directory sul sistema remoto. I comandi per compiere questa operazione dipenderanno dal programma di comunicazione che usate e da quelli disponibili sul sistema remoto, ed è quindi difficile dare indicazioni generali al riguardo: dovrete informarvi, magari chiedendo a un altro utente già esperto.

9. PROGRAMMI CON INTERFACCIA GRAFICA

Concettualmente non è così, ma in pratica la distinzione fra programmi 'grafici' e programmi 'a caratteri' tende spesso a coincidere con quella fra programmi che risiedono sul nostro computer e che sfruttano un protocollo di collegamento diretto a Internet, come PPP, e programmi che funzionano in realtà sul computer del nostro fornitore di connettività e che noi utilizziamo a distanza, come si è visto trasformando, attraverso un normale programma di comunicazione, il computer di casa in un terminale del sistema remoto.
Proprio per questo, i programmi 'grafici' in genere non sono solo più belli da vedere o più facili da usare, ma anche più potenti. Inoltre la maggior parte di questi programmi esistono in versioni assai simili sia per Windows che per Macintosh, semplificando non poco la vita degli utenti (e degli autori di manuali come questo!).
Va detto, peraltro, che le funzionalità di base offerte da questi programmi sono talmente standard da renderli assai simili l'uno all'altro.

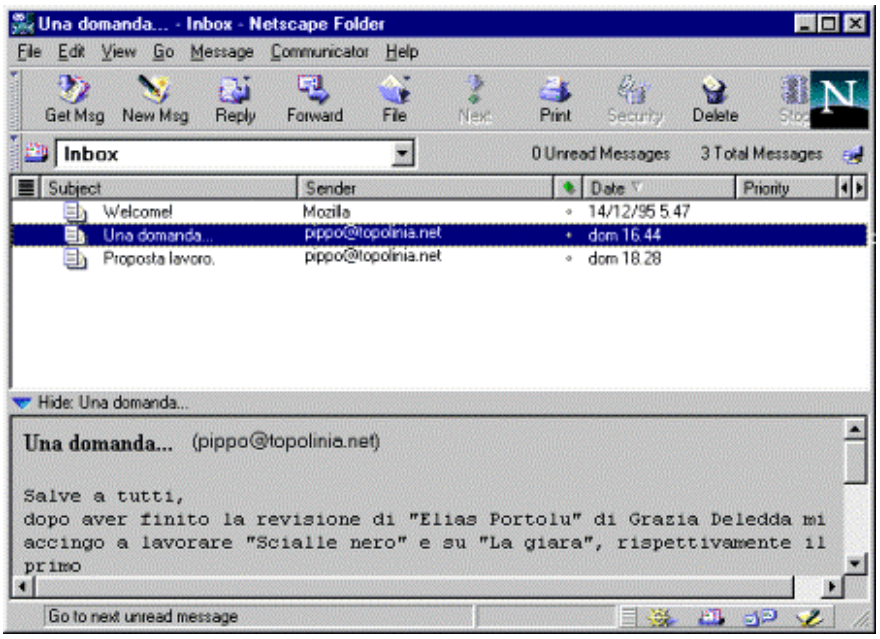
9.1.1 Netscape e la posta elettronica

A partire dalla versione 2.0, Netscape ha introdotto un modulo integrato per la gestione della posta elettronica che offre funzionalità di base abbastanza vicine a quelle offerte da programmi dedicati come Eudora e Pegasus. Con Netscape Communicator 4.0, questo modulo ha acquisito il nome di Netscape Messenger, assieme a numerose nuove funzionalità, fra le quali la possibilità di filtrare automaticamente i messaggi.
Per poterlo utilizzare, il primo passo consiste nella corretta impostazione dei parametri nella scheda 'Mail Server' della finestra 'Mail and Discussion Preferences' (ci si arriva dal menu 'Edit' del programma principale). Anche in questo caso, i dati fondamentali da indicare sono gli indirizzi del POP server e dell'SMTP server. Nella figura seguente troverete un esempio (tenendo sempre presente che dovrete sostituire agli indirizzi da noi forniti quelli indicati dal vostro fornitore di connettività). È probabile che la versione definitiva di Netscape 4 utilizzi al posto delle familiari schede un sistema 'ad albero' per la navigazione fra le varie schermate di configurazione. In tal caso, le preferenze dovrebbero essere raggiungibili tutte insieme attraverso la voce 'Preferences' del menu 'Edit'. I campi da riempire resteranno comunque presumibilmente gli stessi.



La finestra di configurazione della posta elettronica di Netscape

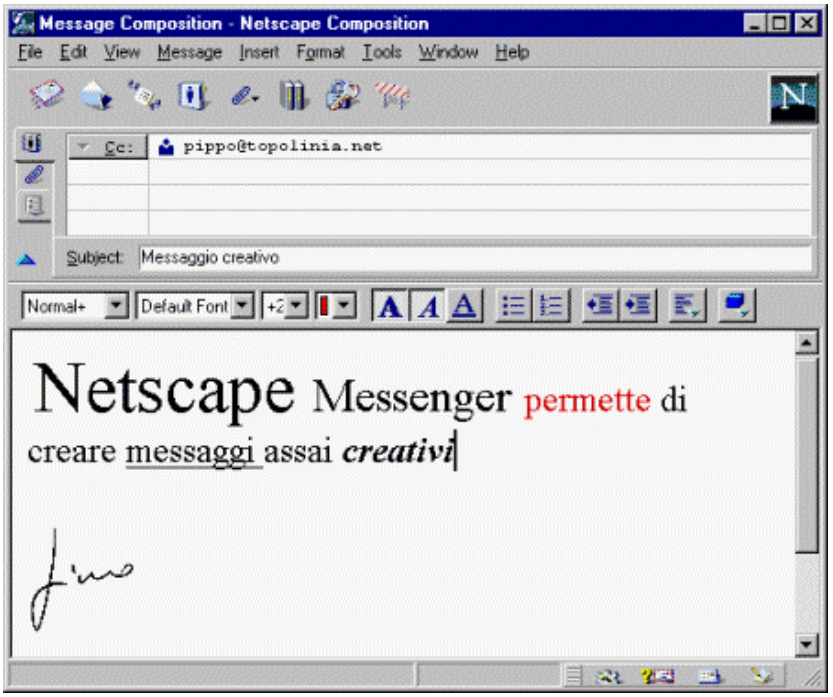
Una finestra analoga è presente nella versione precedente del programma, Netscape 3, anche se in questo caso la voce si chiama 'Mail and News Preferences' e compare nel menu 'Options'.
Oltre alla scheda 'Mail Server', dovremo compilare anche la scheda 'Identity', che richiede poche e intuitive notizie sul titolare dell'indirizzo, e offre la possibilità di predisporre un file di firma da accodare automaticamente a ogni messaggio. Volendo, si può preparare anche un vero e proprio 'biglietto da visita' che accompagnerà il messaggio, e che può contenere informazioni più complete su di voi e sulla vostra organizzazione. Quello dei 'biglietti da visita elettronici' è un settore relativamente nuovo, nel quale si sta combattendo in questo momento una lotta di standard. Tenete dunque presente, se ne usate uno, che potrebbe non essere letto correttamente da utenti che utilizzino programmi di gestione della posta elettronica diversi dal vostro.
Vediamo adesso come funziona la gestione vera e propria della posta elettronica. La finestra principale di Netscape Messenger è riportata nella figura seguente:



La finestra principale del modulo per la posta elettronica di Netscape 4.0 (versione beta 2)

Come si vede, la finestra comprende un elenco dei messaggi conservati nella cartella selezionata; l'elenco delle cartelle disponibili è raggiungibile attraverso un comodo menu a tendina, dalla piccola finestra orizzontale sotto la barra dei pulsanti (nell'immagine, ci troviamo nella cartella 'Inbox', corrispondente alla posta in arrivo). I pulsanti compresi nella barra superiore permettono, nell'ordine, di scaricare la posta in giacenza, scrivere un nuovo messaggio, rispondere al messaggio selezionato, farlo procedere (forward) verso un altro destinatario, archiviarlo in una cartella, passare al messaggio successivo (fra quelli non letti), stampare, attivare il 'security advisor' (che permette fra l'altro di crittografare i messaggi spediti, e di impostare una password per evitare che terzi che abbiano accesso al computer su cui lavoriamo possano accedere alla nostra posta), cestinare il messaggio corrente, interrompere il caricamento o la spedizione dei messaggi.
Sotto la barra dei pulsanti trova posto, come si è visto, l'indicazione della cartella (folder) che stiamo esaminando, e il numero di messaggi (non letti e complessivi) che essa contiene. Il bottone che compare in fondo a destra, proprio sotto la 'N' di Netscape, permette di accedere al message center, una rappresentazione gerarchica del sistema di cartelle e sottocartelle che abbiamo creato per la gestione della posta, integrato con i news server e i newsgroup che abbiamo eventualmente scelto di seguire.
L'elenco dei messaggi è organizzato in colonne verticali; la prima serve — volendo — a organizzare i messaggi ricevuti in thread' (catene) accomunate da uno stesso argomento: in sostanza, il programma genera automaticamente 'famiglie' di messaggi con lo stesso subject, o che siano l'uno la risposta all'altro. La seconda colonna comprende l'oggetto ('subject') del messaggio, la terza il mittente, la quarta permette di distinguere i messaggi letti (pallino piccolo) da

quelli non letti (rombo verde), ed eventualmente di marcare come non letto un messaggio letto, o come letto un messaggio non letto (basta fare click col mouse sul pallino o sul rombo corrispondente). Seguono colonne per la data, il livello di priorità del messaggio (se non compare nulla, si tratta di messaggi con priorità normale), i marcatori ('flag' — servono a raggruppare messaggi che ci interessa collegare per compiere su di essi operazioni comuni), lo status (sarà indicato, ad esempio, se abbiamo risposto al messaggio, o se lo abbiamo reindirizzato a qualcun altro) e la lunghezza del messaggio, il numero di messaggi non letti e complessivi che compongono una determinata catena.
Una menzione speciale merita il triangolino azzurro che compare nell'angolo in basso a sinistra della finestra con l'elenco dei messaggi: serve per passare dalla visualizzazione del solo elenco dei messaggi a una visualizzazione divisa in due aree: quella superiore per l'elenco dei messaggi, quella inferiore per il testo del messaggio selezionato, e viceversa.
Nella suddivisione dello schermo, Netscape 4 introduce in questo modo diverse novità rispetto al modulo di gestione della posta di Netscape 3. In quest'ultimo, lo schermo era normalmente diviso in tre aree (anche se si trattava di una impostazione che poteva essere modificata): in alto a sinistra l'elenco delle cartelle disponibili per l'archiviazione dei messaggi; in alto a destra l'elenco dei messaggi presenti nella cartella selezionata, al centro in basso il testo del messaggio selezionato.
Una delle caratteristiche più interessanti del modulo mail di Netscape è la sua capacità di ricevere e inviare messaggi scritti usando il linguaggio HTML, lo stesso — come vedremo — che permette di creare le pagine in rete su World Wide Web. Questo significa che potete dare ai vostri messaggi un aspetto ben più accattivante di quello tradizionale, cambiando ad esempio dimensioni, colore e tipi di carattere, inserendo immagini, ecc. E per farlo non avete bisogno voi stessi di conoscere la sintassi HTML. La finestra di creazione di un nuovo messaggio mette infatti a disposizione tutti i pulsanti ai quali ci ha abituato il nostro programma di videoscrittura: corsivi, grassetti, sottolineature, scelta del font, e così via. Sarà poi il programma a 'convertire' tutto questo in HTML, senza alcun intervento da parte nostra. In termini un po' più tecnici, questo significa che Netscape Messenger include le caratteristiche di un vero e proprio editor HTML in modalità WYSIWYG ('What You See Is What You Get'). Il che non deve stupire, dato che il modulo di gestione della posta eredita queste caratteristiche da Composer, l'editor HTML integrato in Netscape communicator).
La tendenza all'uso di HTML per la preparazione di messaggi di posta elettronica è probabilmente destinata a diffondersi: Internet Explorer 4 offre la stessa possibilità, ed è ragionevole pensare che anche programmi come Eudora dovranno adeguarsi ben presto, se vorranno restare competitivi.



La finestra per la composizione messaggi di Netscape

In questo momento, tuttavia, le possibilità aperte dall'uso di HTML nella creazione di messaggi di posta elettronica, pur se affascinanti, vanno usate con una certa cautela: il vostro corrispondente, infatti, potrà visualizzare correttamente un messaggio scritto in HTML solo a condizione di disporre anch'egli di un programma — come appunto Netscape Messenger o Microsoft Internet Mail — in grado di interpretarlo. In caso contrario, almeno parte del messaggio gli arriverà assai poco leggibile, 'ingolfata' dalle strane sigle tra parentesi acute dei marcatori HTML: si tratta di un problema che discuteremo più ampiamente tra breve, parlando dei client mail di casa Microsoft. Insomma, almeno per ora conviene sbizzarrirsi con le possibilità davvero notevoli della posta elettronica in HTML solo se si è sicuri che il nostro corrispondente utilizzi anch'egli un programma simile al nostro (una sicurezza che nella maggior parte dei casi non avremo affatto).

10. I PROGRAMMI MICROSOFT PER LA POSTA ELETTRONICA

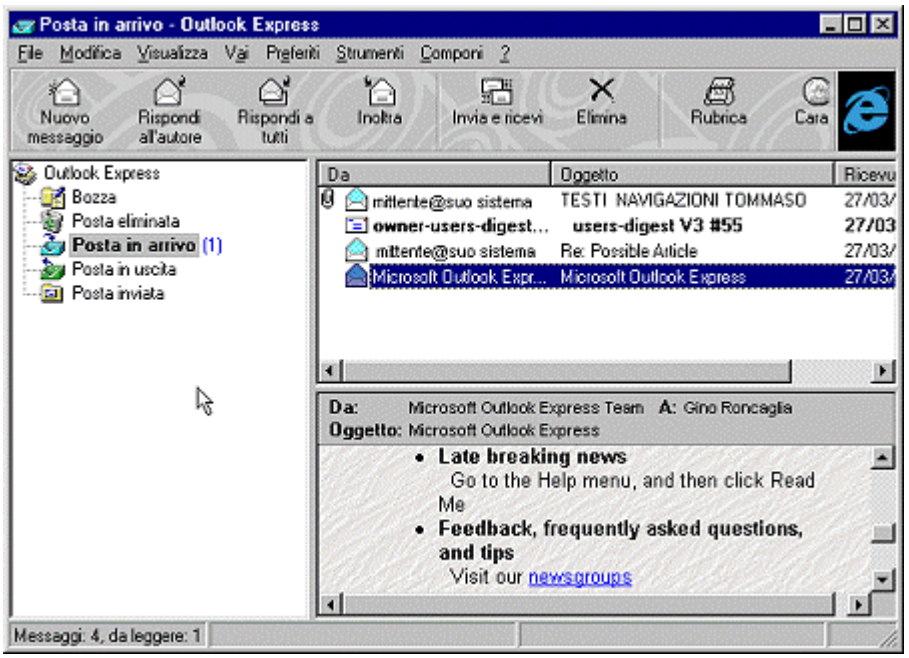
Nella versione 2.0, Explorer utilizzava ancora il client per la gestione della posta elettronica incorporato di serie in Windows 95 (denominato Microsoft Exchange), funzionale ma non particolarmente brillante. Nella versione 3 ha fatto la sua comparsa Internet Mail, più avanzato e intuitivo. Con il pacchetto Office 97 è poi stato distribuito Outlook, un programma estremamente sofisticato per la gestione di contatti e calendari e per la pianificazione collaborativa di attività. E anche Outlook comprendeva il suo bravo (e rinnovato) modulo di posta elettronica. Di Internet Explorer 4, infine, fa parte un modulo mail specifico, denominato Outlook Express, che non comprende le altre funzionalità proprie di Outlook, ma in compenso presenta una interfaccia ulteriormente rinnovata, e una procedura di configurazione particolarmente facile e intuitiva.
Per quanto riguarda Outlook, ricordiamo solo che la configurazione del gestore di posta elettronica si effettua attraverso l'opzione 'Servizi' del menu 'Strumenti'. Se l'opzione 'Posta Internet' non è fra quelle presenti, occorre aggiungerla (pulsante 'Aggiungi'): saremo guidati attraverso una procedura di installazione molto simile a quella già vista per Internet Mail. Se l'opzione è già presente, selezionandola e facendo click sul pulsante 'Proprietà' potremo modificarne la configurazione. Le informazioni da immettere sono sempre le solite, occorre solo fare attenzione al fatto che la configurazione del SMTP server (se diverso dal server POP 3) va effettuata attraverso il bottone 'Opzioni avanzate'.

Configurazione della posta Internet in Microsoft Outlook (versione fornita con Office 97)

Internet Explorer 4, come si è accennato, comprende un proprio programma per la gestione della posta elettronica, denominato Outlook Express. Una volta installato, Outlook Express è sempre disponibile attraverso una icona nella barra delle applicazioni di Windows 95/98, a fianco del menu 'Avvio'.

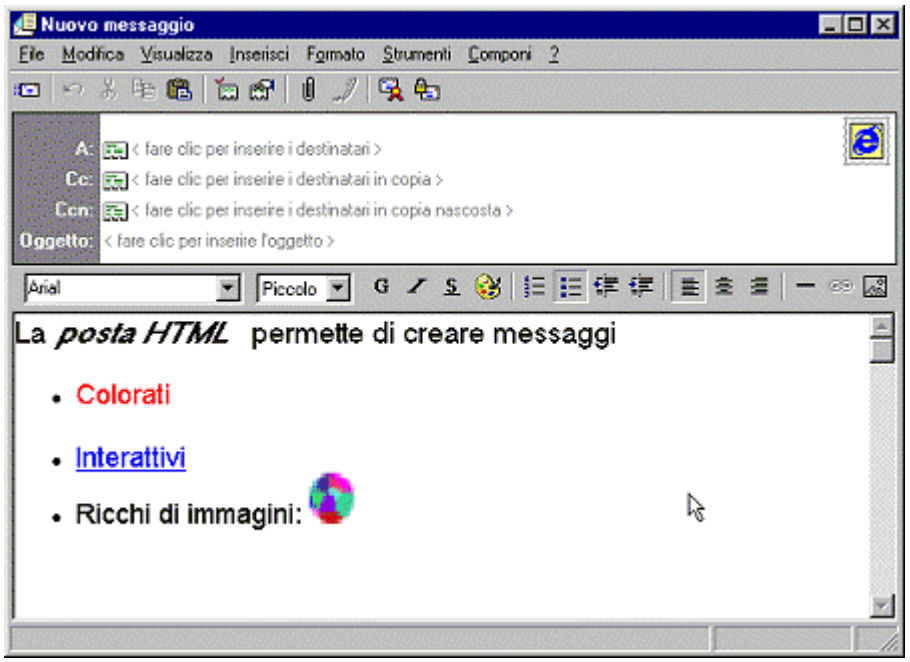
Explorer: le icone per la gestione della posta elettronica e la navigazione in rete incluse nella barra delle applicazioni

I dati di configurazione del programma ci vengono anche in questo caso chiesti automaticamente alla sua prima esecuzione, e possono comunque essere modificati in ogni momento dalla voce 'Account…' del menu 'Strumenti' (bisogna selezionare l'account che desideriamo modificare, e fare click sul bottone 'Proprietà'). Una caratteristica interessante di Outlook Express è la sua capacità di gestire più account di posta elettronica contemporaneamente: per aggiungerne di nuovi, si userà il pulsante 'Aggiungi', sempre nella scheda 'Account..' del menu 'Strumenti'.
Una opzione di configurazione decisamente importante è quella che riguarda il 'formato di invio messaggi', compresa nella scheda 'Invio' nella voce 'Opzioni per la posta elettronica' del menu 'Strumenti': attraverso di essa è infatti possibile decidere se inviare la nostra posta in formato HTML o come puro testo. Abbiamo già discusso i vantaggi e gli svantaggi delle due alternative. Anche se è probabile che il formato HTML tenderà nei prossimi mesi a diffondersi anche per la trasmissione di posta elettronica, è per ora preferibile selezionare il bottone 'Testo normale', per evitare di disorientare i nostri corrispondenti che usassero programmi di gestione della posta elettronica inadatti alla visualizzazione HTML. Va considerato, comunque, che il formato di spedizione usato da Outlook Express (MIME HTML) è tale da evitare confusioni eccessive: il messaggio infatti conterrà prima l'informazione solo testuale, poi la stessa informazione ripetuta in formato HTML. Se il ricevente usa un programma di gestione della posta elettronica 'primitivo', potrà leggere facilmente la prima parte del testo, e ignorare la seconda; se usa un programma in grado di gestire gli attachment, potrà leggere il messaggio testuale e (se lo desidera) visualizzare a parte, in un browser, la sua versione HTML; se infine usa un programma in grado di interpretare il MIME HTML (in sostanza, i client mail di Explorer o Netscape 4), vedrà direttamente il file HTML, con tutti i suoi… effetti speciali.
Sempre la voce 'Opzioni per la posta elettronica' permette di configurare in maniera estremamente semplice le firme, l'eventuale cifratura dei messaggi (compresa addirittura l'emissione di un eventuale 'certificato di autenticità'), il controllo di ortografia, il controllo periodico della posta in arrivo, e numerose altre utili possibilità.
L'interfaccia utente di Outlook express è semplice e funzionale (figura 29): barra dei menu, barra dei pulsanti, e nella porzione principale tre cornici: una cornice verticale dedicata a una rappresentazione ad albero delle varie cartelle per la posta (se ne possono aggiungere attraverso la voce 'Nuovo…' del menu 'File'), una cornice superiore destra con l'elenco dei messaggi compresi nella cartella selezionata, e una cornice inferiore destra con il testo del messaggio selezionato. Il supporto per HTML è pieno, e possono essere inviati messaggi comprendenti immagini, sfondi, liste, tabelle, link attivi. È possibile gestire anche sofisticati filtri sulla posta in arrivo, compresi la generazione e l'invio automatico di messaggi di risposta: le relative regole vanno fornite in una scheda assai intuitiva, raggiungibile attraverso la voce 'Regole posta in arrivo' del menu 'Strumenti'.



Interfaccia utente di outlook Express, il client mail di Explorer 4

Quanto alla creazione di nuovi messaggi, il relativo editor ha due volti: più semplice e spartano se abbiamo deciso di rinunciare alle possibilità di formattazione offerte da HTML, e arricchito da una serie di bottoni per facilitare la formattazione del testo, la creazione di liste, l'inserimento di immagini, in caso contrario.



Explorer: Editor HTML per i messaggi di posta elettronica

10.1.1 POSTA VOCALE E MESSAGGI VIDEO

Nel corso del 1996, Internet è stata percorsa da una vera e propria 'ventata multimediale', che non poteva naturalmente trascurare il settore della posta elettronica. Sono così apparsi alcuni programmi capaci di trasformare una tradizionale e-mail in uno strumento comunicativo di tipo nuovo, aggiungendovi le funzionalità di 'voice-mail' e addirittura di 'video-mail'.

Di cosa si tratta? In sostanza, l'idea è quella di utilizzare la già ricordata possibilità di collegare un file a un messaggio di posta elettronica ('file attachment') per spedire assieme al messaggio testuale vero e proprio anche un file audio, con registrati i nostri saluti o la nostra comunicazione 'in voce' (o in video).
I programmi di gestione di questa 'posta multimediale' si occuperanno sia di preparare i messaggi da spedire, sia di far ascoltare (ed eventualmente vedere) i messaggi ricevuti. Naturalmente nel caso della posta vocale sia al mittente che al destinatario servirà un computer dotato di scheda sonora con casse e microfono — e nel caso dei messaggi video almeno il mittente dovrà disporre anche di una telecamera interfacciata con il computer, per acquisire il brano video da spedire (lo standard in questo campo è l'economicissima Connectix Quickcam, che si collega alla porta parallela del computer).
Si tratta solo di un gioco divertente, o di qualcosa di più? Al momento, questa 'posta multimediale' presenta alcuni inconvenienti non da poco: la dimensione dei file contenenti filmati video rende la spedizione di un brano di durata superiore a qualche secondo assolutamente proibitiva, e gli stessi file audio, nonostante l'uso di sofisticate tecniche di compressione, rischiano di 'pesare' non poco sulla capienza della nostra casella postale. Va detto, però, che in prospettiva strumenti di questo tipo potranno trovare senz'altro il loro campo di applicazione: anche senza considerare la prevedibile evoluzione futura di Internet in termini di velocità delle linee, basti pensare alle reti Intranet, nelle quali i limiti di velocità e di dimensione dei file sono di norma assai meno rigidi.
Diamo dunque un'occhiata un po' più da vicino almeno ad uno di questi programmi; abbiamo scelto allo scopo Internet Voice Mail, della VocalTec, quello probabilmente più diffuso in rete. Lo trovate sul sito della casa produttrice (http://www.vocaltec.com), e potrete usarlo per inviare un massimo di 10 messaggi (per superare questo limite occorre acquistare la versione commerciale del programma, che costa circa 30 dollari).
L'uso è semplicissimo: al momento dell'installazione, il programma vi chiederà i soliti dati relativi al vostro indirizzo di posta elettronica e al server SMTP da utilizzare per l'invio dei messaggi. La finestra principale di Internet Voice Mail è quella che vedete raffigurata qui sotto: la sezione 'Address' serve a indicare l'indirizzo e-mail del destinatario o dei destinatari del messaggio, la sezione 'Voice' fornisce dei familiari pulsanti simil-registratore per registrare e riascoltare il messaggio vocale, che andrà poi salvato (sarà automaticamente compresso in un formato proprietario) e inserito, attraverso il pulsante 'Attach', nella sezione File. La finestra inferiore consente di aggiungere del normale testo scritto. Attraverso la voce 'Attach Player' del menu 'Options' è possibile inserire nel messaggio anche il piccolo programma — liberamente distribuibile — che servirà al nostro corrispondente per ascoltare il messaggio audio (naturalmente, occorrerà spedire questo programma solo se il nostro corrispondente non ne dispone già, e solo la prima volta).

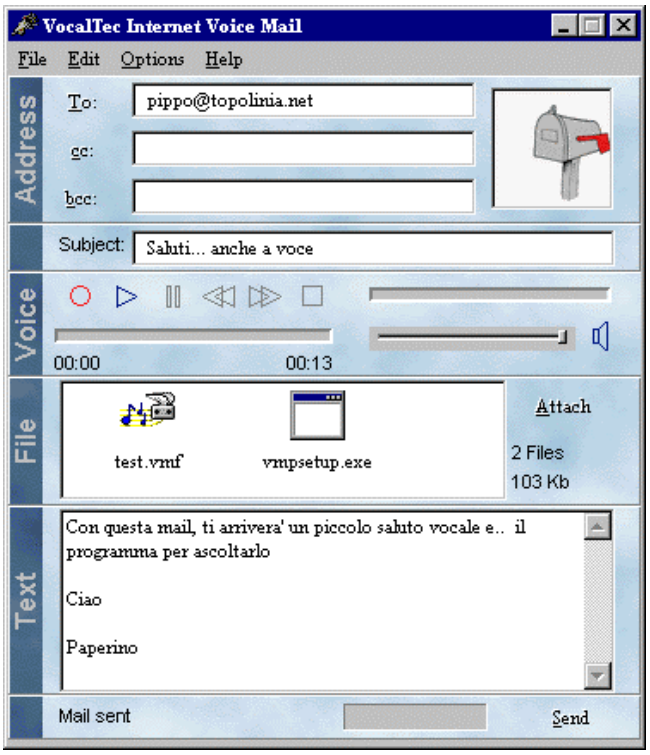


Figura 31 La finestra principale di Internet Voice Mail 3.0

Le capacità di compressione di Internet Voice Mail sono davvero notevoli: una decina di secondi di sonoro 'pesano' circa 20 Kb (una dimensione abbastanza ragionevole). Quanto al programma player, occupa esattamente 80 Kb nella versione Windows, e 114 Kb nella versione Mac: è dunque anch'esso di dimensioni assai contenute.
Per quanto riguarda invece i programmi per la spedizione di messaggi video, al momento il più diffuso è probabilmente QuickCards, della Connectix: per informazioni, il sito è http://www.quickcam.com.
Ricordiamo che i programmi dei quali abbiamo parlato in questa sezione permettono l'invio di messaggi audio (o audio-video) sfruttando il meccanismo della posta elettronica, e dunque 'in differita': non si tratta dunque di conversazioni o videoconferenze in tempo reale. Va da sé che i vantaggi della 'differita' risiedono nel fatto che non è necessario che voi e il vostro corrispondente siate collegati a Internet esattamente nello stesso momento — e che lo svantaggio principale risiede appunto nel fatto che non è possibile una vera e propria conversazione 'in diretta'. Va infine notato che un'alternativa all'uso di questi programmi è rappresentata (o lo sarà ben presto) dall'inserimento del contenuto multimediale che vogliamo spedire (video, audio, immagini) all'interno di un messaggio postale in formato HTML, usando programmi come i già ricordati Netscape Messenger o Microsoft Outlook Express.
Resta un interrogativo di fondo: veramente il messaggio vocale è preferibile a quello testuale — e davvero un'immagine vale mille parole? Da parte nostra, dobbiamo confessare una certa predilezione per l'arte sottile di allineare parole scritte, sia che lo si faccia sulla carta, sia che lo si faccia sullo schermo di un computer. Ma occorre riconoscere che la tesi diffusa secondo cui Internet e la posta elettronica hanno dato il via a una rivalutazione della scrittura, potrebbe rivelarsi prematura. Nel mondo delle comunicazioni digitali in rete la scrittura sarà uno fra i molti stili comunicativi usati — e vi sarà posto per messaggi vocali che ricorderanno un po' la nostra vecchia segreteria telefonica, e per gli scontati filmati del bimbo che spegne le candeline sulla torta di compleanno, o delle vacanze del più antipatico dei nostri cugini. Che ci piaccia o no.

11. IL WWW

11.1 INTRODUZIONE

World Wide Web (cui ci si riferisce spesso con gli acronimi WWW o W3) è stato l'ultimo servizio informativo a venire alla ribalta su Internet. Ma il successo della 'ragnatela mondiale' è stato tale che attualmente, per la maggior parte degli utenti, essa coincide con la rete stessa. Sebbene questa convinzione sia tecnicamente scorretta, è indubbio che gran parte dell'esplosione del 'fenomeno Internet' a cui abbiamo assistito in questi ultimi anni sia legata proprio alla diffusione di questo strumento.
La storia di World Wide Web inizia nel maggio del 1990, quando Tim Berners Lee, un ricercatore del CERN di Ginevra — il noto centro ricerche di fisica delle particelle — presenta ai dirigenti dei laboratori una relazione intitolata "Information Management: a Proposal". La proposta di Berners Lee ha l'obiettivo di sviluppare un sistema di pubblicazione e reperimento dell'informazione distribuito su rete geografica che tenesse in contatto la comunità internazionale dei fisici. Nell'ottobre di quello stesso anno iniziano le prime sperimentazioni.
Per alcuni anni, comunque, World Wide Web resta uno strumento alquanto esoterico. L'impulso decisivo al suo sviluppo, infatti, viene solo agli inizi del 1993, dal National Center for Supercomputing Applications (NCSA) dell'Università dell'Illinois. Basandosi sul lavoro del CERN, Marc Andressen (che pochi anni dopo fonderà con Jim Clark la Netscape Communication) ed Eric Bina sviluppano una interfaccia grafica multipiattaforma per l'accesso ai documenti presenti su World Wide Web, il famoso Mosaic, e la distribuiscono gratuitamente a tutta la comunità di utenti della rete. World Wide Web, nella forma in cui oggi lo conosciamo, è il prodotto di questa virtuosa collaborazione a distanza. Con l'introduzione di Mosaic, in breve tempo il Web si impone come il servizio più usato dagli utenti della rete, e inizia ad attrarne di nuovi.
Il successo di World Wide Web ha naturalmente suscitato l'interesse di una enorme quantità di nuovi autori ed editori telematici, interesse che ha determinato dei ritmi di crescita più che esponenziali. Nel 1993 esistevano solo duecento server Web: oggi ce ne sono oltre dieci milioni.
Su World Wide Web è possibile trovare le pagine di centri di ricerca universitari che informano sulle proprie attività e mettono a disposizione in tempo reale pubblicazioni scientifiche con tanto di immagini, grafici, registrazioni; quelle dei grandi enti che gestiscono Internet, con le ultime notizie su protocolli e specifiche di comunicazione, nonché le ultime versioni dei software per l'accesso alla rete o per la gestione di servizi; ma è possibile trovare anche riviste letterarie, gallerie d'arte telematiche, musei virtuali con immagini digitalizzate dei quadri, biblioteche che mettono a disposizione rari manoscritti altrimenti inaccessibili; ed ancora informazioni sull'andamento della situazione meteorologica, con immagini in tempo reale provenienti dai satelliti, fototeche, notizie di borsa aggiornate in tempo reale e integrate da grafici... ma è meglio fermarci qui, perché parlando di World Wide Web ci troviamo nella situazione di Achille nel ben noto paradosso di Zenone: ogni giorno nasce una nuova fonte di informazioni, ed ogni enumerazione sarebbe incompleta non appena terminata.
Naturalmente si sono accorte delle potenzialità del Web anche le grandi e piccole imprese: per molti analisti economici Internet è la nuova frontiera del mercato globale. Prima sono arrivate le grandi ditte produttrici di hardware e software, dotate ormai tutte di un proprio sito Web attraverso il quale fornire informazioni ed assistenza sui propri prodotti, annunciare novità, e (cosa assai utile dal punto di vista degli utenti) rendere disponibili aggiornamenti del software. Poi sono arrivate anche pizzerie e negozi di dischi, agenti immobiliari ed artigiani della ceramica, librerie e cataloghi di alimentazione naturale… si vende via Internet, si acquista (in genere) con carta di credito.
Le caratteristiche che hanno fatto di World Wide Web una vera e propria rivoluzione nel mondo della telematica possono essere riassunte nei seguenti punti:

- la sua diffusione planetaria
- la facilità di utilizzazione delle interfacce
- la sua organizzazione ipertestuale
- la possibilità di trasmettere/ricevere informazioni multimediali

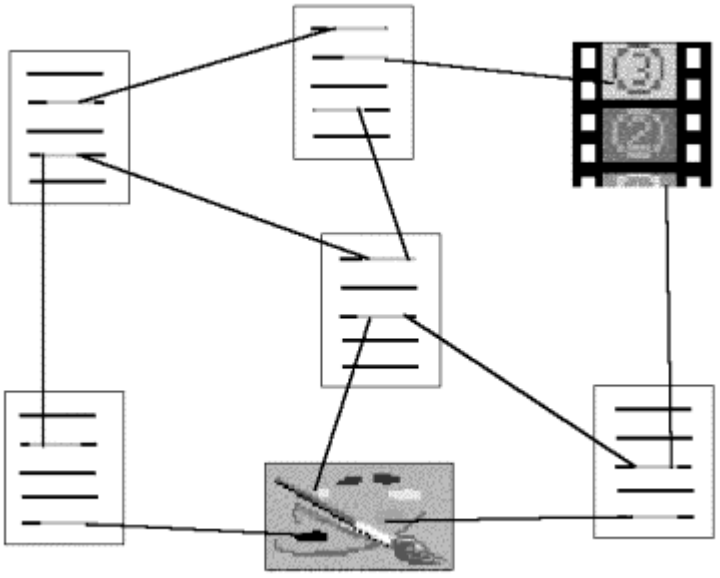
- le semplicità di gestione per i fornitori di informazione.

Dal punto di vista dell'utente finale Web si presenta come un illimitato universo di documenti multimediali integrati ed interconnessi tramite una rete di collegamenti dinamici. Uno spazio informativo in cui è possibile muoversi facilmente alla ricerca di informazioni, testi, immagini, dati, curiosità, prodotti. Non solo: come abbiamo avuto modo di imparare nei capitoli precedenti, un client Web è in grado di accedere in maniera del tutto automatica a tutte le risorse e i servizi presenti su Internet: gopher, FTP, collegamenti telnet, newsgroup... è insomma il più potente e amichevole strumento di navigazione nel ciberspazio.
Dal punto di vista dei fornitori di informazione il Web è uno strumento per la diffusione telematica di documenti elettronici multimediali, decisamente semplice da utilizzare, poco costoso e dotato del canale di distribuzione più vasto e ramificato del mondo.

11.2 DUE CONCETTI IMPORTANTI: MULTIMEDIA E IPERTESTO

Tra i diversi aspetti innovativi di World Wide Web, come si accennava, i più notevoli sono decisamente la organizzazione ipertestuale e la possibilità di trasmettere informazioni integralmente multimediali.
Ipertesto e multimedia: ormai da diversi anni queste due parole, uscite dal ristretto ambiente specialistico degli informatici, ricorrono sempre più spesso negli ambiti più disparati, dalla pubblicistica specializzata fino alle pagine culturali dei quotidiani. Questo paragrafo intende fornire, in poche righe, una breve introduzione a questi concetti: alcuni minimi strumenti terminologici e teorici necessari per poter comprendere il funzionamento di World Wide Web.
In primo luogo è bene distinguere il concetto di multimedialità da quello di ipertesto. I due concetti sono spesso confusi, ma mentre il primo si riferisce agli strumenti della comunicazione, il secondo riguarda la sfera più complessa della organizzazione dell'informazione.
Con multimedialità, dunque, ci si riferisce alla possibilità di utilizzare contemporaneamente, in uno stesso messaggio comunicativo, più media e più linguaggi. È evidente che una certa dose di multimedialità è intrinseca in tutte le forme di comunicazione che l'uomo ha inventato ed utilizzato, a partire dalla complessa interazione tra parola e gesto, fino alla invenzione della scrittura, dove il linguaggio verbale si fonde con l'iconicità del linguaggio scritto (si pensi anche — ma non unicamente — alle scritture ideografiche), e a tecnologie comunicative come il cinema o la televisione. Nondimeno l'informatica — e la connessa riduzione di linguaggi diversi alla 'base comune' rappresentata dalle catene di 0 e 1 del mondo digitale — ha notevolmente ampliato gli spazi 'storici' della multimedialità. Infatti attraverso la codifica digitale si è oggi in grado di immagazzinare in un unico oggetto informativo, che chiameremo documento, pressoché tutti i media e i linguaggi comunicativi: testo, immagine, suono, parola, video.
I documenti multimediali sono oggetti informativi complessi e di grande impatto. Ma più che nella possibilità di integrare in un singolo oggetto diversi media, il nuovo orizzonte aperto dalla comunicazione su supporto digitale risiede nella possibilità di dare al messaggio una organizzazione molto diversa da quella a cui siamo abituati da ormai molti secoli. È in questo senso che la multimedialità informatica si intreccia profondamente con gli ipertesti, e con l'interattività. Vediamo dunque cosa si intende con il concetto di ipertesto.
La definizione di questo termine potrebbe richiedere un volume a parte (ed esistono realmente decine di volumi che ne discutono!). La prima formulazione moderna dell'idea di ipertesto si trova in un articolo del tecnologo americano Vannevar Bush, As We May Think, apparso nel 1945, dove viene descritta una complicata macchina immaginaria, il Memex (contrazione di Memory extension). Si trattava di una sorta di scrivania meccanizzata dotata di schermi per visualizzare e manipolare documenti microfilmati, e di complicati meccanismi con cui sarebbe stato possibile costruire legami e collegamenti tra unità informative diverse. Secondo Bush un dispositivo come questo avrebbe aumentato la produttività intellettuale perché il suo funzionamento imitava il meccanismo del pensiero, basato su catene di associazioni mentali.
La sintesi tra le suggestioni di Bush e le tecnologie informatiche è stata opera di Ted Nelson, che ha anche coniato il termine 'ipertesto', agli inizi degli anni sessanta. Nel suo scritto più famoso e importante, Literary Machines — un vero e proprio manifesto dell'ipertestualità — questo geniale ed anticonformista guru dell'informatica statunitense descrive un potente sistema ipertestuale,

battezzato Xanadu. Nella utopica visione di Nelson, Xanadu era la base di un universo informativo globale ed orizzontale — da lui definito docuverse (docuverso) — costituito da una sconfinata rete ipertestuale distribuita su una rete mondiale di computer. Il progetto Xanadu non è mai stato realizzato concretamente, malgrado i molti tentativi a cui Nelson ha dato vita. Ma le sue idee sono confluite molti anni più tardi nella concezione di World Wide Web.
In questa sede non possiamo affrontare compiutamente tutti gli aspetti teorici e pratici connessi con questo tema, ma solo fornire alcuni elementi esplicativi. In primo luogo, per comprendere cosa sia un ipertesto è opportuno distinguere tra aspetto logico-astratto e aspetto pratico-implementativo. Dal punto di vista logico un ipertesto è un sistema di organizzazione delle informazioni (testuali, ma non solo) in una struttura non sequenziale, bensì reticolare.
Nella cultura occidentale, a partire dalla invenzione della scrittura alfabetica, e in particolare da quella della stampa, l'organizzazione dell'informazione in un messaggio, e la corrispondente fruizione della stessa, è essenzialmente basata su un modello lineare sequenziale, su cui si può sovrapporre al massimo una strutturazione gerarchica. Per capire meglio cosa intendiamo basta pensare ad un libro, il tipo di documento per eccellenza della modernità: un libro è una sequenza lineare di testo, eventualmente organizzato come una sequenza di capitoli, che a loro volta possono essere organizzati in sequenze di paragrafi, e così via. La fruizione del testo avviene pertanto in modo sequenziale, dalla prima all'ultima pagina. Certo sono possibili deviazioni (letture 'a salti', rimandi in nota), ma si tratta di operazioni 'innestate' in una struttura nella quale prevale la linearità. L'essenza stessa della razionalità e della retorica occidentale riposa su una struttura lineare dell'argomentazione.
Un ipertesto invece si basa su un'organizzazione reticolare dell'informazione, ed è costituito da un insieme di unità informative (i nodi) e da un insieme di collegamenti (detti nel gergo tecnico link) che da un blocco permettono di passare ad uno o più altri blocchi. Se le informazioni che sono collegate tra loro nella rete non sono solo documenti testuali, ma in generale informazioni veicolate da media differenti (testi, immagini, suoni, video), l'ipertesto diventa multimediale, e viene definito ipermedia. Una idea intuitiva di cosa sia un ipertesto multimediale può essere ricavata dalla figura seguente.



Un piccolo schema di ipertesto multimediale (ipermedia)

I documenti, l'immagine e il filmato sono i nodi dell'ipertesto, mentre le linee rappresentano i collegamenti (link) tra i vari nodi: il documento in alto, ad esempio, contiene tre link, da dove è possibile saltare ad altri documenti o alla sequenza video. Il lettore (o forse è meglio dire l'iper-lettore), dunque, non è vincolato dalla sequenza lineare dei contenuti di un certo documento, ma può muoversi da una unità testuale ad un'altra (o ad un blocco di informazioni veicolato da un altro medium) costruendosi ogni volta un proprio percorso di lettura. Naturalmente i vari collegamenti devono essere collocati in punti in cui il riferimento ad altre informazioni sia semanticamente rilevante: per un approfondimento, per riferimento tematico, per contiguità analogica. In caso

contrario si rischia di rendere inconsistente l'intera base informativa, o di far smarrire il lettore in peregrinazioni prive di senso.
Dal punto di vista della implementazione concreta, un ipertesto digitale si presenta come un documento elettronico in cui alcune porzioni di testo o immagini presenti sullo schermo, evidenziate attraverso artifici grafici (icone, colore, tipo e stile del carattere), rappresentano i diversi collegamenti disponibili nella pagina. Questi funzionano come dei pulsanti che attivano il collegamento e consentono di passare, sullo schermo, al documento di destinazione. Il pulsante viene 'premuto' attraverso un dispositivo di input, generalmente il mouse o una combinazioni di tasti, o un tocco su uno schermo touch-screen.
In un certo senso, il concetto di ipertesto non rappresenta una novità assoluta rispetto alla nostra prassi di fruizione di informazioni testuali. La struttura ipertestuale infatti rappresenta una esaltazione 'pluridimensionale' del meccanismo testo/nota/riferimento bibliografico/glossa, che già conosciamo sia nei manoscritti sia nelle pubblicazioni a stampa. In fondo, il modo di lavorare di uno scrittore nella fase di preparazione del suo materiale è quasi sempre ipertestuale, così come l'intertestualità soggiacente alla storia della letteratura ed allo sviluppo dei generi (dove "letteratura" e "generi" vanno presi nel loro senso ampio di produzione testuale, non esclusivamente dotata di valore estetico) costituisce un ipertesto virtuale che si genera nella mente di autore e lettore. Tuttavia, le tecnologie informatiche consentono per la prima volta di portare almeno in parte in superficie questo universo pre-testuale e post-testuale, per farlo diventare una vera e propria forma del discorso e dell'informazione.
L'altro aspetto che fa dell'ipertesto elettronico uno strumento comunicativo dalle enormi potenzialità è la interattività che esso consente al fruitore, non più relegato nella posizione di destinatario più o meno passivo del messaggio, ma capace di guidare e indirizzare consapevolmente il suo atto di lettura.
L'incontro tra ipertesto, multimedialità e interattività rappresenta dunque la nuova frontiera delle tecnologie comunicative. Il problema della comprensione teorica e del pieno sfruttamento delle enormi potenzialità di tali strumenti, specialmente in campo didattico, pedagogico e divulgativo (così come in quello dell'intrattenimento e del gioco), è naturalmente ancora in gran parte aperto: si tratta di un settore nel quale vi sono state negli ultimi anni — ed è legittimo aspettarsi negli anni a venire — innovazioni di notevole portata.
World Wide Web è una di queste innovazioni: si tratta infatti di un sistema ipermediale; con la particolarità che i diversi nodi della rete ipertestuale sono distribuiti sui vari host che costituiscono Internet. Attivando un singolo link si può dunque passare a un documento che si trova su un qualsiasi computer della rete. In questo senso utilizzare uno strumento come Web permette di effettuare una vera e propria navigazione nel ciberspazio, una navigazione che riconsegna il timone nelle mani del (iper)lettore.

11.3 COME FUNZIONA WORLD WIDE WEB

Il funzionamento di World Wide Web non differisce molto da quello delle altre applicazioni Internet. Anche in questo caso il sistema si basa su una interazione tra un client ed un server. Il protocollo di comunicazione che i due moduli utilizzano per interagire si chiama HyperText Transfer Protocol (HTTP). La unica — ma importante — differenza specifica è la presenza di un formato speciale in cui debbono essere memorizzati i documenti inseriti su Web, denominato HyperText Markup Language (HTML).
I client Web sono gli strumenti di interfaccia tra l'utente ed il sistema; le funzioni principali che svolgono sono:

- ricevere i comandi dell'utente
- richiedere ai server i documenti
- interpretare il formato e presentarlo all'utente.

Nel gergo telematico questi programmi vengono chiamati anche browser, dall'inglese to browse, scorrere, poiché essi permettono appunto di scorrere i documenti. Nel momento in cui l'utente attiva un collegamento — agendo su un link o specificando esplicitamente l'indirizzo di un documento — il client invia una richiesta ('request') ad un determinato server con l'indicazione del file che deve ricevere.

Il server Web, o più precisamente server HTTP, per contro si occupa della gestione, del reperimento e del recapito dei singoli documenti richiesti dai client. Naturalmente esso è in grado di servire più richieste contemporaneamente. Ma un server può svolgere anche altre funzioni. Una tipica mansione dei server HTTP è la interazione con altri programmi, interazione che permette di produrre documenti in modo dinamico. Vediamo di capire meglio di cosa si tratta.
Un documento Web è ovviamente un file, che una volta preparato e messo in linea rimane a disposizione degli utenti 'così com'è', fino a quando il gestore di sistema non decide di modificarlo o di rimuoverlo. Ci sono però dei casi in cui sarebbe necessario poter cambiare il contenuto di un documento in maniera dinamica, a scadenze prefissate o come risultato di una determinata operazione: ad esempio ogni volta che si verifica un accesso, o aggiornando automaticamente i dati contenuti in una tabella dopo che un programma di calcolo ha ricalcolato le corrispettive funzioni; o quando si devono inviare, inseriti in un opportuno contesto, i risultati di una ricerca su un database. Il server Web è in grado di effettuare queste operazioni attraverso la cosiddetta Common Gateway Interface (CGI), ovvero una serie di comandi standard grazie ai quali può comunicare con altre applicazioni e programmi (ad esempio fare una ricerca automatica su un database) e produrre istantaneamente dei documenti Web adeguati alla operazione compiuta (ad esempio, contenenti i risultati della ricerca). Naturalmente questo avviene in modo del tutto trasparente all'utente finale.
Un'altra tipica funzione svolta dal server è la gestione di transazioni economiche, quali la registrazione di un acquisto fatto con carta di credito. Dal punto di vista tecnico questa operazione non differisce molto dalla normale consultazione o aggiornamento di un database. Ma ovviamente i problemi di affidabilità e di sicurezza in questo caso sono molto più rilevanti: in fondo sentirsi dire che Manzoni ha scritto il Decameron sarebbe considerato da molti meno grave che ritrovarsi un addebito di un milione di dollari per l'acquisto di un libro, o scoprire che il nostro numero di carta di credito è finito nelle mani di un abile truffatore informatico. Per questo sono stati sviluppati dei server HTTP specializzati nella gestione di transazioni economiche sicure attraverso complesse tecnologie di criptazione di dati.

11.4 UNIFORM RESOURCE LOCATOR

Un aspetto particolare del funzionamento di World Wide Web è la tecnica di indirizzamento dei documenti, ovvero il modo in cui è possibile far riferimento ad un determinato documento tra tutti quelli che sono pubblicati sulla rete.
La soluzione che è stata adottata per far fronte a questa importante esigenza si chiama Uniform Resource Locator (URL). La 'URL' di un documento corrisponde in sostanza al suo indirizzo in rete; ogni risorsa informativa (computer o file) presente su Internet viene rintracciata e raggiunta dai nostri programmi client attraverso la sua URL. Prima della introduzione di questa tecnica non esisteva alcun modo per indicare formalmente dove fosse una certa risorsa informativa su Internet.
Una URL ha una sintassi molto semplice, che nella sua forma normale si compone di tre parti:
tiposerver://nomehost/nomefile
La prima parte indica con una parola chiave il tipo di server a cui si punta (può trattarsi di un server gopher, di un server http, di un server FTP, e così via); la seconda indica il nome simbolico dell'host su cui si trova il file indirizzato; al posto del nome può essere fornito l'indirizzo numerico; la terza indica nome e posizione ('path') del singolo documento o file a cui ci si riferisce. Tra la prima e la seconda parte vanno inseriti i caratteri '://'. Un esempio di URL è il seguente:
http://www.liberliber.it/index.html
La parola chiave 'http' segnala che ci si riferisce ad un server Web, che si trova sul computer denominato 'www.liberliber.it', dal quale vogliamo che ci venga inviato il file in formato HTML il cui nome è 'index.html'. Mutando le sigle è possibile fare riferimento anche ad altri tipi di servizi di rete Internet:

- 'ftp' per i server FTP
- 'gopher' per i server gopher
- 'telnet' per i server telnet
- 'wais' per i server WAIS.

Occorre notare che questa sintassi può essere utilizzata sia nelle istruzioni ipertestuali dei file HTML, sia con i comandi che i singoli client, ciascuno a suo modo, mettono a disposizione per raggiungere un particolare server o documento. È bene pertanto che anche il normale utente della rete Internet impari a servirsene correttamente.

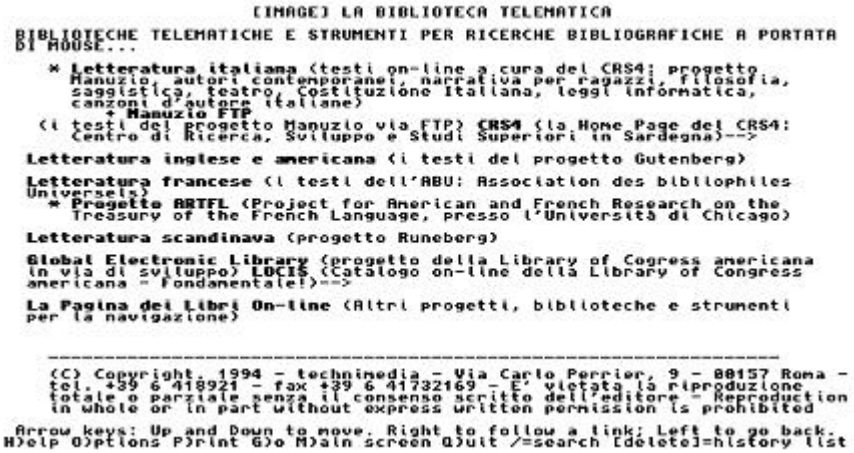
11.5 ALCUNI PROGRAMMI PER L'USO DI WORLD WIDE WEB

Lo strumento principale per la navigazione nelle pagine del World Wide Web è, abbiamo ricordato più volte, un 'browser', ovvero un programma in grado di richiedere la pagina che desideriamo raggiungere al server remoto che la ospita, riceverla e visualizzarla correttamente (testo, immagini, collegamenti ipertestuali, sfondi... il tutto impaginato seguendo le istruzioni fornite, sotto forma di marcatori HTML, da chi ha creato quella determinata pagina). I primi browser Web (come Mosaic) sono nati nei laboratori di ricerca delle università. L'esplosione del fenomeno Internet, in gran parte legata proprio a World Wide Web, ha determinato il moltiplicarsi delle iniziative per sviluppare nuovi programmi, o migliorare quelli esistenti, e in particolare ne ha mostrato le potenzialità commerciali. Questo ha attirato l'attenzione di molte case produttrici di software, e ha indotto moltissimi dei pionieri universitari a fondarne di nuove (il caso più clamoroso è quello della più volte citata Netscape Corporation). Attualmente in questo settore si sta combattendo una delle battaglie strategiche per il futuro dell'informatica e della telematica.
Conseguentemente i programmi per accedere a World Wide Web oggi disponibili sono abbastanza numerosi, alcuni gratuiti, altri venduti con particolari formule commerciali. Come per gli altri servizi di rete visti finora, esistono browser per tutte le più diffuse piattaforme e sistemi operativi.
L'utilizzazione di questi programmi, in linea di massima, è piuttosto facile: basta un semplice click del mouse, per collegarsi con un computer che è all'altro capo del mondo. Inoltre, come abbiamo già visto, un buon client Web può accedere in maniera del tutto trasparente ai server FTP e gopher, mostrare i messaggi dei newsgroup, gestire la posta elettronica, e come vedremo le versioni più recenti possono anche ricevere automaticamente 'canali' informativi attraverso il meccanismo dell'information push. Un client Web può insomma integrare fra loro le principali funzionalità messe

a disposizione da Internet. Ricordiamo che è possibile usare un browser grafico solo se si dispone di una connessione diretta alla rete, oppure di un collegamento con i protocolli PPP o SLIP. Una volta attivato il collegamento alla rete, basta avviare il client sul proprio computer e iniziare la navigazione tra i milioni di server Web sparsi su Internet.
Nelle pagine che seguono passeremo in rassegna alcuni tra i più diffusi browser, mostrandone le funzionalità principali. La nostra scelta è stata orientata dal livello tecnologico e dalla diffusione dei programmi rilevata al momento di scrivere il manuale. Ma ricordate che in questo campo qualsiasi tentativo di sistematizzazione è vano. Ogni consiglio su quale client scegliere, ogni illustrazione particolareggiata di uno di essi, rischia una rapidissima obsolescenza. L'unico consiglio che ci sentiamo di dare senza timore è questo: la via migliore per imparare ad utilizzare tutti gli strumenti del mondo di Internet è quella di usarli, spinti da una buona dose di curiosità. O, per dirla con Galileo, "provando e riprovando".

11.6 PROGRAMMI CON INTERFACCIA A CARATTERI

Ovviamente, per utilizzare un sistema informativo come World Wide Web e per sfruttare pienamente le sue caratteristiche ipertestuali e multimediali, è necessario adoperare un client con una interfaccia grafica. Ma l'esperienza di navigare su World Wide Web, sebbene in maniera estremamente limitata, può essere provata anche da chi non dispone di collegamenti diretti o SLIP/PPP. Esistono infatti dei browser basati su interfaccia a caratteri che possono essere utilizzati anche attraverso una semplice connessione terminale ad un host di Internet. È sufficiente un qualsiasi programma di comunicazione con VT100 o VT102, due emulazioni terminale diffusissime, ed un modem, anche non particolarmente veloce, per collegarsi con l'host.
Naturalmente è necessario che sull'host al quale ci si connette sia installata una versione del client. Per sapere se il proprio fornitore di accesso alla rete ne dispone, occorre chiedere direttamente al sistemista, o all'assistenza clienti nel caso di un provider commerciale.
Se non fosse disponibile un client locale, si può ricorrere ad alcuni host che consentono un libero accesso, attraverso una semplice connessione telnet, ad un client Web. Potete ad esempio collegarvi via telnet all'indirizzo telnet.w3.org. Vi troverete il client WWW a caratteri sviluppato nei laboratori del CERN di Ginevra. Ma il miglior client a caratteri per muoversi su World Wide Web è probabilmente Lynx. Il programma è stato scritto da tre programmatori dell'Università del Kansas, Michael Grobe, Lou Montulli e Charles Rezac, e ne esistono versioni per molte piattaforme, compresa una per DOS. Vediamolo un po' più da vicino. Nella figura seguente potete vedere una schermata di Lynx in ambiente Unix, di gran lunga la versione più usata.



Una schermata di Lynx

Come si può notare alcune parole sono in grassetto: sono altrettanti bottoni di voci attive. A seconda della configurazione del terminale i link potrebbero essere visualizzati in reverse, o con un colore diverso. Nella parte bassa dello schermo c'è un elenco dei comandi principali.

Il posizionamento del cursore su un link avviene con i tasti 'Freccia su' e 'Freccia giù', e l'attivazione con il tasto 'Invio' oppure 'Freccia a destra'. Se volete tornare a una delle pagine Web già visitate basta premere il tasto 'Freccia a sinistra', e Lynx farà un passo indietro.
Ci sono anche altri comandi molto utili: il tasto 'Del' o Backspace', ad esempio, visualizza un elenco di tutti i link raggiunti durante la sessione.
Il tasto '/' consente di effettuare una ricerca nel testo della pagina Web; è molto utile se la struttura della pagina è complessa e lunga. Con il tasto 'H' (help), vengono visualizzati manuali, e quanto altro possa servire per saperne di più.
Abbiamo detto che per attivare una voce contenuta in una pagina WWW basta selezionarla con la tastiera. Il client provvederà a prelevare le informazioni associate alla voce, collegandosi automaticamente con un altro computer se le informazioni richieste sono memorizzate altrove. Se conosciamo già l'indirizzo della pagina alla quale ci vogliamo collegare, con il comando 'G' (go) possiamo attivare direttamente il collegamento. Premuto il tasto non dovremo fare altro che fornire la URL del documento o della risorsa con cui vogliamo collegarci.
Questo modo di navigare su WWW non ha certamente le potenzialità dei browser grafici, che permettono la ricezione di immagini, mappe sensibili, suoni, video, oltre a presentare il testo su schermate grafiche con cui si può interagire attraverso il mouse. Va considerato, inoltre, che l'uso sempre più diffuso di schermate divise in più riquadri (frame) mette spesso i browser testuali del tutto fuori gioco. Un client a caratteri consente — in caso di necessità — un primissimo avvicinamento all'affascinante mondo di World Wide Web, ma, una volta iniziata l'esplorazione, vorrete sicuramente proseguirla dotandovi di strumenti più adeguati.

11.7 LA FAMIGLIA DEI BROWSER GRAFICI

La famiglia dei browser grafici è ormai numerosissima. Nella nostra rassegna esamineremo i due programmi attualmente più evoluti e diffusi: Netscape Navigator (nelle versioni 3 e 4, il recentissimo Communicator), prodotto dalla omonima giovane azienda americana, che è il browser di maggiore successo in questo momento (si calcola che venga usato da circa il 70% degli utenti di Internet), e Microsoft Internet Explorer, il browser sviluppato dalla potente azienda di Bill Gates, che sta conquistando rapidamente una importante fetta di mercato e la cui versione 4, altamente innovativa, costituisce una delle maggiori novità del 1997.
Mosaic continua ad evolversi, e proprio a inizio 1997 ne è uscita la versione 3; come le precedenti, tuttavia, anch'essa non è in grado di visualizzare alcune caratteristiche ormai entrate a far parte di moltissimi siti Web: dalle pagine con frames alle gif animate. Abbiamo quindi deciso di non dedicare a Mosaic una sezione autonoma; va comunque ricordato che Mosaic continua ad essere un buon programma, con soluzioni talvolta assai innovative. Nell'ultima versione, ad esempio, è possibile salvare separatamente intere sessioni di navigazione, assegnando un nome a ciascuna; sono inoltre disponibili il 'Presentation Mode', che permette di allargare la finestra del documento a tutto schermo trasformando Mosaic in un vero e proprio proiettore di presentazioni, e il Mosaic Autosurf', che permette di effettuare la navigazione automatica di uno o più siti, specificando attraverso una finestra di dialogo fino a quale profondità seguire i link. Per ulteriori informazioni su Mosaic, il riferimento d'obbligo è la home page ufficiale del programma, disponibile alla URL http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/NCSAMosaicHome.html.

Il 'papà' dei browser Web: Mosaic

Di Netscape e Internet Explorer abbiamo già avuto occasione di parlare, esaminandone le notevoli funzionalità di programmi 'multiuso', capaci di offrire efficienti moduli client per la gestione della posta elettronica e dei newsgroup, e per il trasferimento di file via FTP. In queste pagine ci occuperemo finalmente della loro caratteristica più importante, quella di strumento di consultazione delle pagine Web.
Entrambi i programmi sono in grado di interpretare uniformemente la maggior parte delle istruzioni previste nelle più recenti specifiche 3.2 del linguaggio HTML. Invece esiste una certa difformità sul supporto delle estensioni a questo insieme, alimentata dalla guerra commerciale esistente fra la Microsoft e la Netscape.
Prima di vedere più da vicino il funzionamento dei due programmi, esamineremo alcune caratteristiche che sono comuni a tutti i browser grafici dell'ultima generazione, compresi naturalmente quelli che citeremo in questo manuale.

Netscape

Cominciamo con gli elementi dell'interfaccia utente; l'immagine si riferisce a Netscape, ma quanto diremo si applica nelle grandi linee agli altri browser). In primo luogo la barra del titolo, nella parte superiore della finestra, permette di leggere il titolo del documento. Ci sono poi la consueta barra dei menu, quella dei pulsanti, a cui si aggiungono una barra che mostra la URL del documento visualizzato, e una barra dei siti di uso frequente.
Il documento Web viene reso nella finestra principale in modalità grafica. Le varie sezioni del testo sono formattate con stili e tipi di carattere diversi. In particolare le porzioni di testo che attivano i link sono evidenziate dal cambiamento di colore del carattere, eventualmente associato alla sottolineatura. Il colore standard dei link disponibili in una pagina è il blu; ma la maggior parte dei browser è in grado di interpretare le istruzioni del linguaggio HTML che consentono di ridefinire il colore dei link. Per attivare un collegamento è sufficiente posizionare il puntatore su una porzione di testo o su una immagine attivi (e cioè collegati ipertestualmente ad altri documenti in rete), e premere il tasto sinistro del mouse (l'unico tasto nel caso dei computer Macintosh). In genere, nel momento in cui il cursore transita su una porzione di testo o su un'immagine attivi, la sua forma cambia da quella di una freccia a quella di una manina che indica.
Oltre ai link ipertestuali all'interno del documento, i browser mettono a disposizione una serie di strumenti di supporto alla navigazione. Le altre operazioni fondamentali che l'utente può effettuare sono le seguenti:

- indicare direttamente il documento o il server al quale collegarsi, digitando la URL corrispondente all'interno di una apposita finestra di dialogo, o direttamente nella barra della URL
- tornare indietro di un passo, ripercorrendo in senso inverso la catena di link seguita, o procedere seguendola in avanti
- vedere la storia di una navigazione (history), ovvero la sequenza dei link seguiti durante la navigazione, ed eventualmente ritornare direttamente ad una pagina già visitata
- tornare alla home page, ovvero alla pagina adottata come 'partenza standard' dal browser (questa pagina è configurabile dall'utente)
- costruire una lista di segnalibri (che Netscape chiama bookmarks e Internet Explorer favorites nella versione inglese e preferiti in quella italiana) con gli indirizzi più usati, facilmente aggiornabile ed eventualmente strutturabile, in cui l'utente annota i siti che ritiene di voler visitare nuovamente in futuro.

Queste funzioni sono attivabili attraverso la barra di pulsanti o i comandi dei menu a tendina. La lista dei segnalibri, che abbiamo già visto nei client gopher, è uno degli strumenti più utili. Si tratta di una lista di puntatori che può essere richiamata, in qualsiasi client, tramite un menu a tendina o una apposita finestra. Le voci dei segnalibri contenute nel menu corrispondono ai titoli delle pagine nella barra del titolo. Ogni utente dovrebbe avere cura di costruire una lista adatta alle proprie esigenze, e dovrebbe sfoltirla periodicamente dalle voci non più interessanti, per preservarne la natura di strumento di rapida consultazione. Sia Netscape che Internet Explorer consentono di personalizzare la propria lista di segnalibri, strutturandola in cartelle e sottocartelle.
Oltre ai comandi per la navigazione sono disponibili anche alcune funzionalità standard: la memorizzazione su disco del documento corrente, la stampa, la visualizzazione del file sorgente in formato HTML.
In generale i browser, oltre al formato HTML, sono in grado di visualizzare autonomamente i file di testo in semplice formato ASCII non marcato, ed almeno i due formati di file grafici più diffusi su Internet: il GIF e il JPEG, integrando le immagini all'interno del documento.
Se il file che viene ricevuto dalla rete è in un formato che il browser non sa interpretare direttamente, ma che comunque 'conosce' perché associato a un altro programma disponibile nel sistema, esso può avviare automaticamente delle applicazioni di supporto in grado di interpretarlo: se si tratta di un file sonoro verrà avviato un riproduttore di suoni, se si tratta di un video verrà avviato un programma di riproduzione video, e così via. L'utente può aggiungere quanti visualizzatori esterni desidera, attraverso le procedure di configurazione di ogni singolo browser. Qualora non fosse disponibile un programma per un dato formato, è possibile memorizzare il file sull'hard disk locale. Una grande novità nella gestione di formati di file non standard è stata introdotta da Netscape

e ripresa da Internet Explorer: si tratta dei plug-in, dei moduli software che si integrano pienamente con il browser.
La maggior parte dei browser condividono anche alcune caratteristiche tecnologiche che rendono più efficiente l'accesso on-line alle pagine, specialmente per chi usa una linea telefonica:

- gestione avanzata di testi e immagini
- uso di memoria di deposito locale, detta cache
- interazione con un proxy server

La prima caratteristica si riferisce al modo in cui il browser gestisce i file che vengono inviati dal server remoto, e alle precedenze nella composizione a video della pagina. Come abbiamo detto i file HTML sono dei semplici file in formato ASCII. Questo significa che un documento testuale su Web, anche se molto lungo, ha una dimensione in byte molto contenuta. I file grafici invece, anche se usano uno dei cosiddetti algoritmi di compressione, sono molto più esosi nell'occupazione di spazio. Quando una pagina Web viene inviata, il file di testo arriva quindi molto più velocemente dei file grafici eventualmente a corredo. Per evitare tempi morti, e poiché si può assumere che un utente sia, in genere, interessato alla lettura del testo prima che alla visione delle immagini, molti browser cominciano subito a visualizzare il testo, anche prima che tutte le immagini vengano ricevute completamente. E il testo stesso viene visualizzato progressivamente, man mano che arrivano i dati, senza aspettarne la ricezione completa. Questo meccanismo aumenta notevolmente la velocità di una navigazione.
La memoria di deposito, o cache memory, è invece una sorta di duplicato locale di piccole sezioni del World Wide Web. L'uso della cache permette di velocizzare un eventuale nuovo accesso a pagine già visitate precedentemente, o a file già caricati. Ogni volta che il browser riceve dalla rete una pagina, fa una copia di tutti i file che la compongono sul disco rigido locale. Se nel seguito della navigazione l'utente contatta di nuovo quella medesima pagina, il programma carica i file memorizzati nella cache, piuttosto che richiederli al server remoto. Il meccanismo funziona anche se lo stesso file ricorre in più pagine: ad esempio le icone che si ripetono su tutte le pagine di un certo sito. La disponibilità e la dimensione della memoria cache sono modificabili attraverso i comandi di configurazione del browser (lo vedremo nei casi specifici). Dopo un determinato periodo di tempo, o quando lo spazio disponibile sul disco viene esaurito, il browser cancella i file più vecchi, per fare spazio a quelli nuovi.
I proxy server estendono il meccanismo della memoria cache locale. Un proxy server è un software che viene di norma installato su uno dei computer di una rete locale collegata ad Internet. La sua funzione è quella di conservare in un apposito archivio una copia di ogni file richiesto dagli utenti che accedono alla rete (l'archivio può avere dimensioni variabili a seconda della capacità di memoria del sistema su cui risiede). Quando un utente richiede di accedere ad una data risorsa, il suo browser contatta in primo luogo il proxy server (come dice il nome, prossimo, e dunque molto più veloce): se le informazioni sono già presenti nella memoria locale, il proxy le invia senza stabilire il collegamento con i computer remoti (o stabilendo un collegamento assai rapido al solo scopo di verificare che i file richiesti non siano nel frattempo stati modificati); altrimenti effettua la nomale procedura di trasferimento remoto, e prima di recapitare i dati al computer chiamante, ne conserva una copia.
L'uso del proxy server ha naturalmente senso solo se esso si trova sulla stessa sottorete del client. Si dimostra particolarmente utile per i provider che forniscono collegamenti SLIP/PPP, poiché consente di aggirare in parte i rallentamenti della rete Internet, garantendo nel contempo un'alta velocità di utilizzo all'utente finale e un minore flusso di dati sui canali pubblici, con vantaggio per tutti. Per il momento solo alcuni fornitori commerciali offrono questo tipo di servizio. Per fare in modo che il browser sfrutti questa tecnologia, qualora fosse disponibile, occorre configurarlo adeguatamente: vedremo in seguito come farlo nel caso dei due programmi presi in considerazione in questa sede.

12. SICUREZZA SU INTERNET

Internet è un insieme di decine di migliaia di reti IP interconnesse che va crescendo a una velocità straordinaria. Secondo i dati raccolti da Network Wizards, nel luglio del 1993 c'erano 1,766 milioni di

host e 26000 domini; nel luglio 1995, gli host erano 6,642 milioni e i domini 120000, con una crescita del 400% circa in due anni.
Il numero di incidenti correlati con la sicurezza su Internet è cresciuto di conserva. Secondo InfoSec (1994), il numero di incidenti su Internet è aumentato dai circa 200 nel 1990 a circa 1300 nel 1993, con una crescita approssimativa del 600% in tre anni.
Questo capitolo considera diversi aspetti della sicurezza su Internet. Innanzitutto, è opportuno riassumere qualche nozione sul protocollo TCP/IP con i problemi di sicurezza a esso correlati. Si procederà quindi con una trattazione dei sistemi di sicurezza per le tre aree principali di utilizzo di Internet; in particolare, verranno descritti i meccanismi di sicurezza per la posta elettronica (e-mail), per il World Wide Web e per il commercio elettronico.

12.1 TCP/IP

Il TCP/IP è in realtà un insieme di protocolli di rete e di applicazioni. Originariamente, il TCP/IP fu sviluppato sotto gli auspici dell'U.S. Defense Advanced Research Projects Agency (agenzia dei progetti di ricerca avanzata del Ministero della Difesa statunitense) e fu sviluppato in ARPANET nel 1983. Il TCP/IP è inoltre uno dei protocolli di rete pià diffusi, esistente in pratica su tutti i tipi di reti.
Il termine TCP/IP è una combinazione di TCP, che significa Transfer Control Protocol (protocollo di controllo trasferimenti), e IP, cioè Internet Protocol (protocollo Internet). La descrizione del protocollo TCP/IP è, per forza di cose, molto breve; ulteriori informazioni possono essere reperite in molti libri, ad esempio Comer (1991) e IBMTCP (1990).
I protocolli del TCP/IP possono essere suddivisi in quattro livelli generarchici (riportati in molta letteratura informatica anche come strati). Partendo dal livello inferiore, il livello dell'interfaccia di rete serve per fornire i driver di periferica necessari a interfacciarsi con l'hardware di comunicazione. Il TCP/IP non specifica alcun protocollo particolare per questo livello, ma consente di utilizzare praticamente qualsiasi interfaccia di rete, come Token Ring, Ethernet e X.25.
Il livello internetwork consiste del protocollo Internet (IP) e di Internet Control Message Protocol (ICMP, protocollo di controllo messaggi Internet).Gli indirizzi fisici vengono utilizzati per la comunicazione al livello dell'interfaccia di rete, mentre al livello internetwork e a quelli superiori vengono utilizzati solamente gli indirizzi IP. Il livello trasporto consiste di protocolli orientati alla connessione (TCP) o privi di connessione (UDP). Il livello applicazioni consiste di varie applicazioni o protocolli di alto livello di alto livello che utilizzano il TCP/IP. I protocolli di più alto livello comprendono TELNET ed FTP (File Transfer Protocol, protocollo di trasferimento file).

12.2 PROTOCOLLO INTERNET (IP)

Il protocollo Internet serve a effettuare un multiplexing dei pacchetti di dati provenienti dai livelli più alti. Ciascun pacchetto consiste di un indirizzo di origine a 32 bit, oltre che di un indirizzo di destinazione e di checksum per l'intestazione. Il protocollo IP non è in grado di garantire che un pacchetto venga inoltrato, né che venga inoltrato una volta soltanto; inoltre, non garantisce nemmeno che , durante la trasmissione, non vengano introdotti errori.
Ciascun pacchetto è un'unità di trasmissione a sè stante; un pacchetto lungo può essere spessato in due o più pacchetti più brevi, per facilitarne la trasmissione. Il pacchetto viene inoltrato da un nodo determinato, basandosi sulle informazioni di instradamento (routing) in esso contenute. Un nodo sovraccaricato può reinstradare il pacchetto o rilasciarlo; da ciò consegue che il protocollo IP non è in grado di garantire in alcun modo l'affidabilità della trasmissione, né il controllo di flusso o la correzione d'errore: queste sono sutte caratteristiche gestite da un protocollo di livello più alto, come il TCP. Il TCP assicura che vengano inoltrati pacchetti completi e che i pacchetti non vengano modificati durante la trasmissione.
In ultimo, il protocollo IP non garantisce che l'indirizzo di origine sia veramente quello del nodo che ha dato origine al pacchetto. Molti sistemi operativi verificano che il pacchetto porti con sé l'indirizzo di origine corretto, ma non esiste alcuna garanzia che l'indirizzo di origine sia valido. Il risultato è che un host che desideri introdursi in un sistema può in realtà utilizzare l'indirizzo di origine di un host legittimo e farsi passare per questo. Questo difetto è stato all'origine dell'attacco spoofing.

12.3 INDIRIZZI IP

Ciascun indirizzo IP è lungo 32 bit. I 32 bit vengono assegnati secondo la classe della rete, come si può vedere nella Figura 6.2. La classe della rete è indicata dai 4 bit più a sinistra. Una rete di classe A consente più di 16 milioni di host, mentre una di classe C non ne consente più di 254 (gli indirizzi host composti totalmente da 0 o 1 sono riservati). La classe più comune è la classe B, con la quale una rete può presentare circa 65000 host. In questa classe è però consentito un massimo di 16384 reti, dati gli indirizzi a 14 bit della rete stessa; ciò significa che gli indirizzi di rete appartenenti a questa classe stanno terminandoe sista già pensando alla progettazione di un nuovo metodo di indirizzamento. Gli indirizzi di classe D sono riservati ai broadcast.
Generalmente, gli indirizzi IP vengono indicati separandoli con punti. I quattro byte sono scritti nella forma *x.y.w.z;*ciascuna delle lettere rappresenta otto bit dell'indirizzo a 32 bit. Ad esempio, l'indirizzo:

128.5.7.9
si traduce in:
10000000 00000101 00000111 00001001

I due bit più a sinistra specificano la classe di rete. Come si vede nella Figura 6.2, un 10 indica una rete di classe B. l'indirizzo di rete è 5, che si ricava dai 14 bit che si trovano subito dopo i due iniziali. L'indirizzo host è 79 esadecimale, che si ricava dai due byte inferiori del campo di indirizzo.

12.4 INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

Il protocollo IP viene utilizzato per svolgere i servizi di datagramma in un insieme di reti interconnesse. L'host che realizza la connessione tra due reti viene chiamato *gateway*. ICMP è un meccanismo che consente a un gatewau di riferire le condizioni di errore alla sorgente che ha originato il messaggio. ICMP viene considerato una parte integrante del protocollo IP e deve essere implementato su qualsiasi modulo IP. ICMP serve esclusivamente a riferire le condizioni di errore; anche se in alcuni casi vengono suggerite tecniche che potrebbero servire per rimediare all'errore occorso, ICMP non è pensato per rendere più affidabile il protocollo IP. Per un pacchetto frammentato, ICMP indica soltanto gli errori che corrispondono a frammenti di pacchetti pari a zero. ICMP può riportare gli errori su qualsiasi datagramma IP, tranne i pacchetti ICMP, per evitare ripetizioni infinite. È compito dell'host che ha originato il messaggio riferire gli errori alle singole applicazioni e intraprendere le azioni correttive opportune.

12.5 USER DATAGRAM PROTOCOL (UDP)

UDP è un protocollo indipendente dalla connessione. Non serve per avere una maggiore affidabilità nella trasmissione dei pacchetti, né per il controllo di flusso o per la correzione d'errore. UDP serve solamente come multiplexer/demultiplexer per l'invio di datagrammi IP da e verso le applicazioni. Questo protocollo consente di risparmiare il tempo normalmente necessario per attivare una connessione TCP; data la sua semplicità d'uso, UDP è particolarmente adatto per applicazioni di ricerca quando il numero di messaggi scambiati è limitato.
Un'applicazione in TCP/IP viene identificata univocamente da una coppia:
socket = <*Idirizzo IP, numero di porta*>
Questa coppia viene chiamata anche *indirizzo socket.* L'indirizzo IP identifica l'host della rete; il numero di porta è un campo di 16 bit che identifica quale applicazione o protocollo di livello superiore deve ricevere il pacchetto IP. È possibile accedere a un'applicazione TCP/IP di alto livello, come TELNET o FTP, attraverso un numero di porta fisso, quale che sia l'implementazione del TCP/IP. Ad esempio, il numero di porta per l'FTP è 20 per i dati e 21 per il controllo, TELNET è 23, SMTP è 25 e DNS è 53.

12.6 TRANSPORT CONTROL PROTOCOL (TCP)

Il protocollo TCP serve per ottenere una connessione virtuale affidabile per i processi dell'utente. Questo protocollo è in grado di ritrasmettere pacchetti danneggiati o persi; i paccheti frammentati vengono ricostituiti nella sequenza corretta, in modo tale che possano poi essere inoltrati al nodo destinatario. In pratica, il TCP offre affidabilità, controllo di flussoe multiplexing. Ciascun messaggio

TCP utilizza un circuito virtuale, il quale consiste dell'indirizzo host e del numero di porta dell'host di origine e di quello di destinazione:
<host_locale, porta_locale, host_remoto, porta_remota>
Questi quattro valori definiscono in maniera univoca un circuito virtuale. Un server resta in ascolto di un particolare numero di porta; qualsiasi pacchetto arrivi a quel numero di porta, viene ricevuto dal server come richiesta di servizio. I processi client richiedono di rado un numero di porta specifico, sebbene possano farlo; normalmente, ricevono i pacchetti sul numero di porta che l'host locale decide di assegnare loro.

12.7 TELNET

Il protocollo TELNET serve per garantire ai client un'interfaccia standard che consenta di accedere ai servizi di un host remoto. La parte forndamentale del protocollo è il fatto che il client appare all'host remoto come se si trattasse di un terminale connesso localmente. Sul client si trova un client TELNET, mentre sull'host remoto, dove risiede il server a cui si desidera accedere, si trova un server TELNET. Quando l'utente chiama TELNET, il client TELNET sull'host dell'utente invia una richiesta di connessione al server TELNET dal lato dell'host remoto. Stabilita la connessione, il client TELNET trasferisce ogni pressione di tasto sul server TELNET, il quale a sua volta inoltra le informazioni provenienti dal client TELNET all'host operativo locale, e viceversa; il client TELNET è infatti in grado di leggere e analizzare le pressioni di tasto provenienti dal server TELNET, visualizzando all'utente il risultato.
TELNET prevede due insiemi di funzioni. Per prima cosa, definisce un terminale di rete virtuale (NVT, Network Virtual Terminal); ogni programma client o server TELNET viene mappato in questo NVT. In secondo luogo, TELNET consente a ciascuna coppia client/server di negoziare diverse opzioni. Ad esempio, TELNET consente di utilizzare un insieme di caratteri a 7 bit ASCII o a 8 bit EBCDIC. I client e i server possono negoziare queste opzioni scambiandosi verbi come Do, Don't, Will, Won't.

12.8 FILE TRANSFER PROTOCOL (FTP)

Il protocollo FTP viene utilizzato per trasferire i file da un host TCP/IP a un altro, utilizzando il protocollo TCP per assicurare un trasferimento di dati affidabile tra i due capi della comunicazione. Il trasferimento di file può avvenire in entrambe le direzioni; il client può quindi inviare un file al server, oppure può richiedere al server l'invio di un file. Un trasferimento di file con FTP avviene come illustrato di seguito

1. L'utente digita ftp insieme con il nome dell'host dove si trova il server FTP; questo richiede all'utente di immettere il proprio ID e la propria password.
2. L'utente digita ID e password, informazioni che il server FTP utilizza per autenticare l'utente.
3. L'utente può immettere il sottocomando GET per cpiare un file dall'host remoto sul file system locale.
4. L'utente può immettere il sottocomando PUT per copiare un file dal file system locale sull'host remoto.Questi sottocomandi contengono il nome del file sull'host di origine e il nuovo node che il file deve aver sull'host di destinazione.
5. Per terminare il trasferimento, l'utente immette il comando QUIT.

FTP è una delle applicazioni più utilizzate sulle reti TCP/IP. La maggior parte degli FTP è costituita dai cosiddetti *FTP anonimi.* Con un FTP anonimo, qualsiasi utente può copiare i file dal server FTP, in questo caso, l'ID dell'utente è *anonymous*, mentre la password è molto spesso, costituita dall'indirizzo di posta elettronica, nella forma *utente@ host.* Un FTP anonimo consente ai siti di garantire un accesso libero ai file per gli utenti di Internet; in questo modo, il server FTP offre un accesso diretto agli utenti di Internet, pur restando protetto il resto della rete privata, attraverso l'installazione di un firewall o di un altro gateway di sicurezza.

12.9 DOMAIN NAME SYSTEM (DNS)

Domain Name System (DNS, sistema di denominazione dei domini) consente l'utilizzao di nomi simbolici invece di indirizzi IP. Ad esempio, invece di immettere:

telnet 128.5.7.13

è possibile immettere:

telnet ediventi.it

in cui ediventi è il nome di un'azienda.
Il livello più elevato nella gerarchia dNS è il nome del dominio; la Tabella mostra alcuni esempi.
Esempi di nomi di dominio

NOME	DOMINIO
edu	Istituzione scolastica
gov	Istituzione statale
com	Azienda commerciale
mil	Gruppi militari

NOTA:*Si tenga comunque presente che questi nomi di dominio vengono in genere adottati soltanto negli Stati Uniti; gli altri Paesi utilizzano solitamente una sigla di due lettere che li identifica. Ad esempio, l'Italia utilizza la sigla it, la Francia fr, la Gran Bretagna uk e così via.*

Ad esempio, l'indirizzo simbolico:

avahuja @ eos.ncsu.edu

indica l'utente A. V. Ahuja, al sottodominio eos all'interno di NCSU (North Carolina State University), che è un'istituzione scolastica.
Infine, vengono presentati brevemente altri protocolli TCP/IP. Un *Name Server* serve per eseguire la traduzione da nomi simbolici in indirizzi IP, per ciascun ramo dell'albero gerarchico del nome di dominio è installato un name server. *SMTP* (Simple Message Transfer Protocol) serve per lo scambio di messaggi tra host TCP/IP, ma non prevede il supporto per la traduzione dei documenti. *Remote Procedure Call* (RCP) consente ai programmi di chiamare le sotto routine che vengono eseguite sull'host remoto.

12.10 PROBLEMI DI SICUREZZA SU INTERNET

La crescita di Internet ha portato al presentarsi di numerosi problemi di sicurezza. Di seguito ne vengono analizzati alcuni tra i più gravi.

6. Autenticazione. Internet richiede due tipi di autenticazione. Innansitutto, ciascun utente deve essere autenticato per accedere a un'applicazione TCP/IP, come TELNET o FTP. Le applicazioni TCP/IP richiedono all'utente di immettere un ID e una password, in modo che possa essere autenticato. A meno che non sia protetto in altro modo, un tipico codice client/server TELNET scambia ID e password come testo in chiaro. In secondo luogo, molti messaggi, transazioni e messaggi di posta elettronica su Internet possono richiedere l'autenticazione dell'origine. Ad esempio, un memeo dal presidente di un''azienda deve autenticare la propria origine prima che i dipendenti possano agire in accordo con esso.
7. Riservatezza. Internet richiede che qualsiasi informazione segreta o privata venga codificata. La codifica è necessaria per proteggere informazioni importanti che si possono trovare nei messaggi di posta elettronica, in FTP e nel commercio elettronico su Internet.
8. Integrità dei dati. Per certi tipi di dati, gli utenti Internet possono richiedere l'assicurazione che i dati stessi non siano stati modificati durante la trasmissione. L'integrità dei dati può essere necessaria per proteggere file FTP o messaggi di posta elettronica per la trasmissione su Internet.
9. Non ricusazione. La non ricusazione dà una prova sicura dell'origine dei dati o del loro invio. Serve per evitare che un mittente possa negare di avere inviato dei dati, se invece li ha inviati, e che il ricevente possa affermare di non averli ricevuti, se invece non li ha ricevuti. È un requisito fondamentale per poter effettuare transazioni commerciali sicure su Internet.

10. Accesso a Internet. Per collegarsi a Internet, le reti aziendali private possono richiedere un gateway che serva a intercettare ed esaminare i messaggi provenienti da Internet e diretti verso di esso. Un gateway Internet intercetta ogni messaggio proveniente da Internet e ne autentica l'origine; inoltre, questi gateway filtrano i pacchetti basandosi sull'indirizzamento IP e sui numeri di porta. Questi gateway Internet prendono il nome di firewall.

12.11 SERVIZI DI SICUREZZA PER LE APPLICAZIONI TCP/IP

Per soddisfare i requisiti sopra esposti, un'applicazione TCP/IP può essere considerata alla stregua di un'applicazione che debba accedere ai servizi di sicurezza di una rete. I protocolli TCP/IP, come TELNET o FTP, possono autenticare i client, trasmettere le password in maniera protetta e offrire i servizi di codifica e di integrità dei dati. I servizi di sicurezza possono essere forniti da GSSAPI, descritto in precedenza; questo metodo viene visualizzato nella Figura 6.5.
Si consideri come esempio un utente che richieda l'accesso al protocollo TELNET. Si dia per assunto che l'implementazione della rete comprenda GSSAPI per accedere ai servizi di sicurezza insieme con Kerberos come sistema di sicurezza sottostante.

11. L'utente presso l'host A accede al server di sicurezza e ottiene le credenziali da Kerberos. La password non viene trasmessa sulla rete. Questo è l'unico accesso utente richiesto per accedere alle varie applicazioni, compreso TELNET. Per garantire l'accesso singolo, ciascuna applicazione TCP/IP deve implementare le chiamate GSSAPI, in modo che possa accedere ai servizi di sicurezza.
12. L'utente desidera stabilire una sessione TELNET con un server presso l'host S; l'utente digita il comando TELNET insieme al nome dell'host S.
13. Il codice client di sicurezza sottostante invia le credenziali dell'utente all'host S.
14. Assumendo che il server che risiede sull'host S sia già stato autenticato al server di sicurezza, il server accetta le credenziali dell'utente e la sessione TELNET viene stabilita tra il client e il server TELNET.

13. Sicurezza della posta elettronica

13.1 POSTA ELETTRONICA

La posta elettronica (e-mail, dall'inglese Electronic Mail) è una delle applicazioni più comuni su Internet e viene utilizzata principalmente per scambiarsi messaggi.
Esiste un formato standard per la posta elettronica su Internet. Un messaggio di posta elettronica consiste di due parti, un'intestazione di messaggio (*message header*) e i dati del messaggio (*message data*), separati da una riga vuota. La riga *To:* indica l'indirizzo di posta elettronica del destinatario; la riga *From:* indica invece l'indirizzo di posta elettronica del mittente. La riga *Reply-To*: , se presente, contiene l'indirizzo di posta elettronica a cui inviare le risposte; se invece non è presente, l'indirizzo di ritorno è quello presente nella riga *From:.* L'eventuale rica *cc:* viene utilizzata per specificare l'indirizzo di posta elettronica dei destinatari secondari del messaggio.
L'indirizzo di posta elettronica consiste di due componenti: porta locale e nome di dominio. La porta locale è l'indirizzo di una casella di posta elettronica, il nome di dominio è il nome del dominio sul quale si trova la casella postale. Le due componenti sono separate dal simbolo at (@). Ad esempio, un possibile indirizzo di posta elettronica è:

avalli @ ediventi.it

Il name server locale del dominio del mittente deve aver accesso al name server appropriato che sia in grado di determinare l'indirizzo IP del destinatario del messaggio di posta elettronica.

13.2 SICUREZZA DELLA POSTA ELETTRONICA

La sicurezza della posta elettronica richiede tutti gli elementi analizzati in precedenza: autenticazione, riservatezza, integrità dei dati e non ricusazione. Inoltre, la sicurezza della posta

elettronica richiede anche l'anonimato. Questo requisito offre la possibilità di inviare un messaggio in modo tale che chi lo riceve non possa identificare l'identità del mittente.

13.3 PRIVACY-ENHANCED MAIL (PEM)

PEM venne sviluppato dalla comunità Internet per garantire la sicurezza ai messaggi di testo. Iniziò come progetto di Internet Architecture Board nel 1985; i documenti finali vennero pubblicati nel 1993.
PEM offre riservatezza, autenticazione dell'origine dei dati, integrità dei messaggi, non ricusazione dell'origine e gestione delle chiavi. Ogni messaggio PEM include automaticamente autenticazione, integrita dei dati e non ricusazione; l'integrità dei dati e l'autenticazione dell'origine vengono garantiti attraverso firme digitali codificate. La risevatezza dei messaggi è facoltativa.
PEM viene descritto in quattro RFC Internet. L'RFC 1421 (Linn 1993a) descrive la codifica dei messaggi e le procedure di autenticazione. L'RCF 1422 tratta della gestione delle chiavi basata sui certificati. Questo documento presenta l'architettura e l'infrastruttua di gestione delle chiavi, con un sistema di certificati a chiave pubblica. L'RFC 1423 descrive gli algoritmi di codifica e di integrità dei messaggi, compresa la gestione delle chiavi. Infine, l'RFC 1424 descrive tre tipi di servizi che servono a supportare PEM: certificazione delle chiavi, memorizzazione degli elenchi di revoca dei certificati (CRL, Certificate-Revocation List) e recupero dei CRL.
PEM consente di utilizzare diversi algoritmi per la codifica dei dati, la gestione delle chiavi e l'integrità dei dati. La gestione delle chiavi serve a codificare le chiavi di codifica e i valori di controllo per l'integrità dei messaggi. PEM non richiede l'utilizzo di un algoritmo specifico; per ciascuna di queste funzioni, nell'RFC 1423 sono specificati diversi algoritmi possibili.

13.4 ALGORITMI DI CODIFICA

Algoritmi di codifica supportati da PEM:

- DES in modalità CBC (Cipher Block Chaining Mode, modalità con concatenazione di blocchi cifrati).

Algoritmi di gestione delle chiavi supportati da PEM:

- DES in modalità ECB (Electronic Codebook Mode, modalità codice crittografico elettronico).
- DES in modalità EDE (Encrypt-Decrypt-Encrypt, codifica-decodifica-codifica) Triple-DES.
- RSA

Algoritmi per il controllo di integrità dei messaggi (MIC, Message Integrity Check):

- RSA ed MD2
- RSA ed MD5

PEM utilizza chiavi a 56 bit per la codifica DES; per Triple-DES PEM utilizza due chiavi DES, per una lunghezza totale di 112 bit. La dimensione delle chiavi RSA non viene specificata. Per la gestione delle chiavi, PEM consente di utilizzare DES o RSA; comunque, normalmente si utilizza DES per la codifica dei dati, mentre è consigliabile utilizzare RSA per codificare le chiavi DES per la trasmissione.

13.5 TIPI DI MESSAGGIO

Un messaggio PEM è sempre firmato, ma la codifica è facoltativa. PEM specifica tre tipi di messaggio:

- MIC-CLEAR
- MIC-ONLY
- ENCRYPTED

I messaggi di tipo MIC-CLEAR e MIC-ONLY servono per garantire l'integrità dei dati e l'autenticazione, ma non per la codifica. Un messaggio di tipo MIC-CLEAR offre invece integrità dei dati e autenticazione; un messaggio MIC-ONLY ha gli stessi attributi di un MIC-CLEAR, ma prevede anche un passaggio di codifica; perchè possa essere letto, un messaggio di tipo MIC-ONLY deve

essere dapprima trasformato con il software PEM. Un messaggio di tipo ENCRYPTED ha tutte le caratteristiche di un messaggio MIC-CLEAR, più la codifica.

13.6 TRASMISSIONE DI MESSAGGI

Per inviare un messaggio PEM occorre seguire quattro passaggi.

15. Canonizzazione
16. Integrità del messaggio e firma digitale
17. Codifica (facoltativo)
18. Codifica della trasmissione (facoltativo)

Un messaggio di tipo MIC-CLEAR segue i passaggi 1 e 2; un messaggio MIC-ONLY segue i passaggi 1, 2 e 4; infine, un messaggio di tipo ENCRYPT segue tutti i passaggi da 1 a 4.
La *canonizzazione* (standardizzazione) trasforma il testo del messaggio in formato standard. Molti elaboratori di testi e sistemi operativi sono in grado di generare messaggi testuali con formati e rappresentazioni diverse. Ad esempio, la rappresentazione delle nuove righe è diversa nei vari sistemi operativi. In MS-DOS, è composta da un carattere di un ritorno a capo pià uno di nuova riga, mentre in Macintosh si utilizza soltanto il carattere di nuova riga. Un'ulteriore considerazione da fare è che, nel caso di PEM, il formato di un messaggio non può essere modificato dopo che è stato codificato, perche un messaggio non può essere modificato dopo che è stato codificato, perché un messaggio codificato non verrebbe decodificato correttamente all'altro capo della trasmissione. PEM converte quindi tutti i messaggi in formato standard prima di applicare gli algoritmi per l'integrità dei dati.
Per l'integrità dei messaggi e la firma digitale, PEM consente di utilizzare tutti gli algoritmi sopra riportati. Per evitare attacchi spoofing (nei quali qualcuno può modificare il messaggio in transito e ricalcolare il MIC), il MIC viene firmato dal mittente. Per consentire al ricevente di verificare il valore del MIC e l'identità del mittente, al messaggio viene accodato un certificato X.509. I messaggi PEM sono sempre firmati.
Se poi l'utente ha deciso di codificare i dati (il tipo di messaggio è ENCRYPTED), il testo del messaggio viene codificato.
Infine, i messaggio PEM viene codificato per la trasmissione, se si tratta di un tipo MIC-ONLY o ENCRYPTED. PEM supporta la trasformazione del messaggio da una codificazione a 8 bit a una a 16 bit.
Nel momento in cui riceve il messaggio PEM, il ricevente ne verifica innanzitutto il tipo. Se è di tipo MIC-ONLY o ENCRYPTED, viene decodificato, invertendo la codifica da 16 a 8 bit. Il passaggio successivo serve a decodificare il messaggio, se è di tipo ENCRYPTE. Infine, il formato canonico del messaggio viene convertito in un formato adatto per il ricevente.

13.7 GERARCHIA DI CERTIFICAZIONE

PEM ha una gerarchia di certificazione ben definita. Alla radice dell'albero gerarchico di trova l'Internet Policy Registration Authority (IPRA, autorità di registrazione dei criteri Internet), che stabilisce fini e criteri per l'attività di generazione di tutti i certificati sotto questa gerarchia. Sotto l'IPRA si trovano le Policy Certification Authority (PCA, autorità di certificazione dei criteri), ciascuna delle quali pubblica i propri criteri di registrazione degli utenti e delle società; i documenti vengono pubblicati sotto forma di un RFC. Ciascuna PCA deve essere registrata presso l'IPRA. Al di sotto della PCA si trovano le Certification Authority (CA, autorità di certificazione), che certificano gli utenti e le società subordinate.

13.8 UTILIZZO DEI CERTIFICATI

PEM utilizza i certificati X.509. Il MIC viene codificato dal mittente con la propria chiave privata; il mittente, inoltre, accoda il proprio certificato X.509, il quale a sua volta è firmato da un'autorità di certificazione (CA). Il ricevente, per prima cosa, decodifica il certificato utilizzando la chiave

pubblica dell'autorità di certificazione (che può essere ottenuta a partire dall'IPRA che si trova in cima alla gerarchia di certificazione).
In questo modo, il ricevente ha la certezza che il certificato è stato concesso da un'autorità di certificazione valida e che non si tratti di un falso. A questo punto, il ricevente verifica se il certificato è stato revocato, supponendo che sia valido, il ricevente può ricavare la chiave pubblica del mittente direttamente dal certificato, dopodiché utilizza questa chiave pubblica per decodificare il MIC. Se il MIC viene verificato con successo, l'origine del messaggio è autenticata correttamente ed è garantito che il messaggio non è stato modificato durante la trasmissione

13.9 PRETTY GOOD PRIVACY (PGP)

PGP è un altro sistema di sicurezza per la posta elettronica. È facile da usare, liberamente distribuito su Internet e funziona su molti diversi sistemi operativi. PGP utilizza uno schema di crittografia a chiave pubblica.
PGP versione 1 fu progettato e sviluppato da Philip Zimmerman nel 1991. PGP versione 2.0 fu sviluppato da diverse persone al di fuori degli Stati Uniti, per evitare questioni legali relative all'esportazione. PGP versioni 2.5 e 2.6, sono stati rilasciati dal Massachusetts Institute of Technology, che ne possiede il breveto. Con il rilascio della versione 2.6, il MIT ha dichiarato che la versione era rilasciata con la collaborazione di RSA Data Security Inc.; ciò significa che la versione 2.6 può essere utilizzata liberamente e legalmente per uso personale e non commerciale. La versione 2.6 può essere utilizzata liberamente e legalmente per uso personale e non commerciale. La versione 2.6 è l'attuale versione gratuita di PGP. ViaCrypt commercializza PGP versione 2.7 per usi commerciali.
PGP è in grado di garantire riservatezza, autenticazione dell'origine dei dati, integrità di messaggi e non ricusazione dell'origine. PGP è progettato per fornire automaticamente autenticazione, integrità dei dati e riservatezza per tutti i messaggi; però possibile inviare un messaggio non riservato. PGP consente inoltre l'invio di un messaggio senza autenticazione né integrità. L'autenticazione e l'integrità sono strettamente legate ed entrambe possono essere ottenute eseguendo una funzione hash non invertibile sul messaggio, codificando i risultati prima della trasmissione.

13.10 ALGORITMI DI CODIFICA

PGP versione 2 utilizza i seguenti algoritmi:

- Algoritmo di codifica dei dati: IDEA in modalità CBC
- Algoritmo di gestione delle chiavi: RSA
- Algoritmi per il controllo dell'integrità dei messaggi e per la firma digitale: MD5 ed RSA

Le chiavi RSA di PGP possono essere di tre lunghezze distinte: grado casual (384 bit), grado commerciale (512 bit) e grado militare (1024 bit). Le chiavi di 384 bit dovrebbero essere utilizzate soltanto per la prova e per la codifica del testo del messaggio. Per la gestione delle chiavi e le firme digitali, si raccomandano le chiavi a 1024 bit. Le chiavi a 512 bit dovrebbero essere utilizzate esclusivamente se la sicurezza non è fondamentale.

13.11 TRASMISSIONE DEI MESSAGGI

Esistono quattro passaggi che devono essere seguiti per inviare un messaggio PGP: la firma (facoltativo), la compressione, la codifica (facoltativo) e la codifica di trasmissione (facoltativo).
La firma PGP consente al ricevente di autenticare l'origine e di verificare che il messaggio non è stato modificato durante la trasmissione. PGP esegue innanzitutto l'algoritmo MD5 per calcolare la funzione hash non invertibile del messaggio; il valore hash risultante viene codificato utilizzando la chiave privata del mittente. La firma digitale, compreso il valore hash, può essere inviata insieme con il messaggio; in alternativa, è possibile memorizzare e inviare separatamente la firma digitale del messaggio. Un vantaggio importante di staccare la firma dal messaggio consiste nel fatto che il mittente (o il ricevente) può mantenere un file di registrazione separato di tutte le firme che ha inviato (o ricevuto).
A questo punto, PGP applica al messaggio l'algoritmo di compressione. La compressione serve a ridurre le dimensioni del messaggio e a eliminarne tutte le ridondanze. La codifica è facoltativa con

PGP. L'algoritmo utilizzato per la codifica del testo del messaggio è IDEA. Come si è visto IDEA fornisce una compressione con chiave segreta di 128 bit. Per trasmettere la chiave di codifica di 128 bit, essa viene codificata utilizzando l'algoritmo RSA e la chiave pubblica del ricevente. Se il messaggio è destinato a più di un destinatario, PGP codifica una copia della chiave segreta con la chiave pubblica di ognuno.
PGP supporta inoltre la conversione da un flusso di testo cifrato a 8 bit in caratteri ASCII stampabili, utilizzando il medesimo algoritmo utilizzato in PEM; questa conversione è necessaria perché molti sistemi di posta elettronica non consentono l'utilizzo di caratteri che non appartengano al set ASCII.
Il ricevente inizia a elaborare il messaggio controllando innanzitutto se è stato codificato per la trasmissione. Un messaggio codificato viene decodificato in testo con caratteri di 8 bit. A questo punto, PGP determina se il messaggio è stato cifrato; se si, il ricevente decifra la chiave segreta utilizzando la propria chiave privata, dopodiché la chiave segreta viene utilizzata per decifrare il testo cifrato. Infine, PGP verifica se il messaggio è firmato. Se si, per prima cosa viene decodificato il valore hash utilizzando la chiave pubblica del mittente, dopodiché viene verificata l'integrità dei dati e ne viene autenticata l'origine.

13.12 UTILIZZO DEI CERTIFICATI

Per l'origine e l'accettazione dei messaggi, PGP utilizza un metodo del tutto diverso da quello utilizzato da PEM; questa è probabilmente la differenza maggiore tra i due sistemi.
PEM utilizza una struttura gerarchica per ottenere l'autorizzazione dei certificati mentre la certificazione delle chiavi di PGP è basata sulla nozione che la fiducia è un concetto sociale. Isa riceve la propria chiave firmata da una persona che conosce, Ale accetta la chiave di Isa se è firmata da qualcuno di cui Ale si fida. Ale e Isa possono quindi accettare le chiavi l'uno dell'altro, se sono firmate da un amico comune.
Per molte comunicazioni, potrebbe anche non essere necessario stabilire l'assoluta autenticità dell'altra parte. Si supponga che Ale inizi una discussione su Internet con qualcuno che non conosce. La persona all'altro capo utilizza un soprannome: a seconda del tipo di discussione che si è instaurata, i due possono comunicare l'uno con l'altro senza dover per forza autenticarsi l'uno all'altro. Lo stesso varrebbe se Ale incontrasse una persona sulla metropolitana e facesse quattro chiacchiere.
Con il metodo PGP, un dato utente di PGP non può verificare la validità di tutti gli altri utenti. Con PEM esiste una singola gerarchia di certificazione che rende molto semplice la verifica dei certificati altrui.

14. Sicurezza sul World Wide Web

14.1 WORLD WIDE WEB

Per un lungo periodo Internet è stata carente in due aree: la facilità d'uso e la sicurezza. Il World Wide Web ha iniziato a risolvere il problema della facilità d'uso. I client (o browser) Web e i server Web offrono anche alcuni servizi di sicurezza, come autenticazione, riservatezza, integrità dei dati e non ricusazione.
Il Web è un segmento di Internet in rapida espansione. Secondo Dunlap (1995) esistono dai dieci ai quindici milioni di utenti Web e più di 100000 siti Web. Si stima che ogni giorno entrino in linea dai 50 ai 100 nuovi siti, secondo HWANG (1995).
IL World Wide Web è noto anche come W3, WWW o Web. Il Web è il servizio più user-friendly esistente attualmente su Internet. Si tratta di un servizio ipermediale distribuito; nessuno controlla il Web, così come nessuno controlla Internet. Il Web è stato inventato presso il CERN (centro di ricerca per l'energia nucleare), un centro di ricerca europea sulla fisica delle alte energie, con sede in Svizzera. I ricercatori intuirono la necessita di un protocollo semplice ad assenza di stato tra client e server; il protocollo doveva essere leggero, in modo da riuscire ad accedere con facilità agli oggetti multimediali presenti su Internet. Il CERN sviluppò allo scopo il cosiddetto H*yperText Transfer Protocol* (HTTP, protocollo di trasferimento ipertestuale). HTTP è il linguaggio comune

utilizzato tra i client e server Web su Internet. il National Center for super computing Applications (NCSA) collaborò fattivamente alla ricerca di un client adatto, arrivando alla pubblicazione di Mosaic, un browser Web, ossia la porzione client del sistema client/server del Web. Mosaic gratuito e funziona sotto Windows, Macintosh e alcuni sistemi Unix. Diversi produttori hanno a catalogo dei browser Web, che sono diventati molto popolari perché propongono un'interfaccia grafica intuitiva e facile da usare per accedere con semplicità alle risorse di Internet.
Il Web può essere visto come un insieme di server HTTP su Internet. Viene utilizzato dalle imprese per fornire informazioni sui propri prodotti e servizi; le informazioni sono memorizzate sotto forma di una cosiddetta home page su un server Web. Quando si accede alla home page, questa viene mostrata al client Web, il quale può inoltre presentare diverse opzioni per ottenere ulteriori informazioni sugli argomenti interessanti.

14.2 HYPERTEXT TRANSFER PROTOCOL (HTTP)

Si consideri uno scambio di dati che inizia da parte dell'utente, il quale apre un browser Web. L'utente immette un *Uniform Resource Locator* (URL, indirizzo di un file che si trova su un host ed è accessibile attraverso Internet) e fa clic per procedere con la connessione.
In effetti, al client Web viene indicato di accedere a un file (chiamato home page che si trova su un server Web. Per prima cosa, il client stabilisce una connessione TCP/IP con il nome di host specificato nell'indirizzo URL. Quando la connessione è realizzata, il client invia una richiesta, insieme con l'oggetto della richiesta. La richiesta viene inviata al server sotto forma di comando HTTP. Un comando tipico, ad esempio, è GET, che serve a recuperare l'home page del server, insieme con l'Uri (Universal Resource Identifier), che è in pratica l'URL privata del nome dell'host. Il server risponde con i dati richiesti e chiude la connessione. Sia il client sia il server possono fornire ulteriori informazioni durante questo scambio.
Le home page del Web vengono create scrivendo il testo in linguaggio chiamato Hyper Text Markup Language (HTML). In un file HTML possono trovare posto grafica, video, suono e collegamenti a file. Un documento HTML può essere collegato con estrema facilità ad altri documenti HTML; un semplice esempio di pagina HTML viene dato di seguito. La pagina HTML inizia con il tag <HTML> e termina con il tag </HTML>, mentre il testo normale non richiede altri tag; le lettere in grassetto iniziano con <B> e terminano con </B>.

```
        <HTML>
Questo libro tratta dei problemi di sicurezza sulle reti, compresa la sicurezza su Internet.
    <B>Il presente capitolo tratta della sicurezza su Internet. </B>
    </HTML>
```

14.3 REQUISITI DI SICUREZZA DEL WEB

I requisiti di sicurezza del Web prevedono l'utilizzo di un canale sicuro e autenticato tra il client e il server Web. In modo simile a quanto accade per la posta elettronica, il Web richiede agli utenti di autenticare l'origine dei dati, di codificarli e di assicurare l'integrità dei dati tra client e server.
Poco dopo l'introduzione di client e server Web, alcuni produttori e forum di Internet iniziarono a studiare i problemi di sicurezza sul Web. Esistono due prodotti appositamente creati, Secure Socket Layer e Secure HyperText Transfer Protocol.

14.4 SECURE SOCKET LAYER

Netscape ha sviluppato un protocollo di sicurezza per la comunicazione tra browser e server Web. Secure Socket Layer (SSL) serve a garantire la privacy su Internet. La descrizione di SSL si può trovare in Hickman (1995), documento Internet datato giugno 1995.
SSL offre autenticazione, codifica e integrità dei dati; è pensato per autenticare il server e , facoltativamente, il client. SSL utilizza, come protocollo di trasporto, il TCP, ottenendo una trasmissione di dati affidabile. Poiché SSL risiede al livello del socket, è indipendente dalle applicazioni di alto livello e può quindi offrire servizi di sicurezza a protocolli di livello più elevato, come TELNET, FTP e HTTP.
SSL consiste di due protocolli, SSL Record Protocol e SSL Handshake Protocol. SSL Record Protocol è descritto più avanti; SSL Handshake Protocol viene utilizzato per negoziare i parametri di sicurezza per una connessione SSL. La descrizione di SSL riportata in questo libro si basa su Wayner (1996) e Hickman (1995).

14.5 SSL HANDSHAKE PROTOCOL

In SSL Handshake Protocol, il clent e il server si scambiano una serie di messaggi che servono alla negoziazione dei parametri di sicurezza: SSL Handshake Protocol consiste di sei fasi, descritte di seguito.
La prima fase è la cosiddetta fase di Hello e viene utilizzata per mettere d'accordo client e server su un insieme di algoritmi che verranno utilizzati per garantire privacy e autenticazione. Oltre a ciò in questa fase viene rilevato qualsiasi ID di sessione proveniente da una sessione precedente. Il client inizia inviando il messaggio CLIENT-HELLO al server; questo messaggio comprende tre tipi di informazioni, ossia il tipo di tecnica di codifica che il client è in grado di gestire, l'ID di sessione lasciato da sessioni precedenti interrotte (se ne esistono) e un dato casuale che serve come richiesta al srver. Se il server riconosce l'ID della sessione precedente, la sessione viene riavviata; se invece si tratta di una nuova sessione, il server invia un certificato X.509 al client. Questo certificato comprende la chiave pubblica del server, firmata con la chiave privata di un'autorità di certificazione per decifrare la chiave pubblica del server. La chiave pubblica del server viene a sua volta utilizzata per leggere il certificato del server. In questa fase vengono scambiati i seguenti messaggi:

CLIENT-HELLO
SERVER-HELLO

La secondo fase è quella di scambio delle chiavi. In questa fase, tra il client e il server vengono scambiate le informazioni riguardanti le chiavi; al termine di questa fase, entrambi i capi della connessione hanno una chiave principale condivisa. SSL versione 3 supporta tre algoritmi per lo scambio di chiavi: RSA, Diffie-Hellman e Fortezza-KEA. La chiave viene inviata come testo cifrato utilizzando la chiave pubblica del server. Per le versioni destinate all'esportazione, soltanto una parte della chiave viene inviata come testo cifrato. In questa fase vengono scambiati i seguenti messaggi:

CLIENT-MASTER-KEY
CLIENT-DH-KEY

La terza fase è quella di produzione di una chiave di sessione e serve a scambiare la chiave che verrà effettivamente utilizzata per comunicare durante la sessione corrente. In questa fase viene scambiato il seguente messaggio, inviato dal client:

CLIENT-SESSION-KEY

La quarta fase è la fase di verifica del server e viene utilizzata solamente quando si utilizza l'algoritmo di scambio delle chiavi RSA. In questa fase viene verificata la chiave principale e le chiavi di sessione successive ricevute dal server. Quando il server riceve la chiave principale e le chiavi successive dal client una conferma rispondendo alla richiesta casuale inviata dal client nel messaggio CLIENT-HELLO. Il client decodifica la risposta alla richiesta casuale e, se esiste corrispondenza, si stabilisce una connessione a cui si concede fiducia tra client e server. Durante questa fase viene scambiato questo messaggio:

SERVER-VERIFY

La quinta fase è quella di autenticazione del client. Se si richiede l'autenticazione del client, il servr richiede al client un certificato; a questa richiesta il client risponde con un messaggio CLIENT-CERTIFICATE. Finora SSL supporta solamente i certificati X.509. Durante questa fase vengono scambiati i seguenti messaggi:

REQUEST-CERTIFICATE
CLIENT-CERTIFICATE

La sesta e ultima fase è la fase finale, durante la quale sia il client sia server si scambiano i messaggi finiti. Il client indica il completamento dell'autenticazione inviando l'ID di sessione sotto forma di testo cifrato; il server invia un messaggio SERVER-FINISHED, che comprende l'ID di sessione codificato con la chiave principale. A questo punto, si è stabilita una connessione a cui si concede fiducia tra il client e il server. Durante questa fase vengono scambiati i seguenti messaggi:

CLIENT-FINISHED
SERVER-FINISHED

14.6 SSL RECORD PROTOCOL

SSL Record Protocol specifica l'incapsulamento di tutti i dati in ricezione e in trasmissione. La parte dei dati di un record SSL ha tre componenti:

- MAC-DATA
- ACTUAL-DATA
- PADDING-DATA

MAC-DATA è il codice di autenticazione del messaggio (MAC, Message Authentication Code). Per MD2 ed MD5 questo campo è lungo 128 bit. ACTUAL-DATA sono i dati che devono essere aggiunti, quando necessario, se si utilizza un algoritmo di codifica a blocchi. Quando si invia un record SSL come testo in chiaro, i campi MAC-DATA e PADDING-DATA non vengono inclusi. MAC-DATA viene calcolato applicando la funzione hash su:

MAC-DATA=HASH(SECRET, ACTUAL-DATA, PADDING-DATA, SEQUENCE-NUMBER)

Il contenuto del campo SECRET dipende da chi ha inviato il messaggio e dal tipo di codifica adottata. SEQUENCE-NUMBER è invece un contatore, mantenuto e aggiornato dal client e dal server. Per ciascuna direzione di trasmissione, vengono mantenuti due contatori, uno da parte del mittente e l'altro del destinatario. Il contatore viene incrementato di 1 ogniqualvolta il mittente invia un messaggio; i contatori sono senza segno a 32 bit.

14.7 ALGORITMI DI CODIFICA

Come parte della negoziazione tra client e server, il mittente può identificare l'algoritmo di codifica supportato. SSL versione 2 e versione 3 supportano:

- RC4 128 bit ed MD5
- RC4 128 bit (40 bit per l'estero) ed MD5
- RC2 128 bit CBC e MD5
- RC2 128 bit (40 bit per l'estero) ed MD5
- IDEA 128 bit CBC ed MD5
- DES 64 bit CBC ed MD5
- DES 192 bit EDE3 CBC ed MD5

MD5 viene utilizzato come funzione hash per calcolare il MAC.

Esistono delle limitazioni sulla dimensione della chiave di codifica per i prodotti da esportazione. Le regole sull'esportazione consentono una chiave di dimensioni non superiori ai 40 bit, sebbene ci possano essere eccezioni. SSL raccomanda l'utilizzo di chiavi di almeno 128 bit con RC2 ed RC4 per l'utilizzo all'interno degli Stati Uniti. Per l'esportazione soltanto 40 bit della chiave sono mantenuti segreti, gli altri 88 bit sono inviati in chiaro.

14.8 SECURE HYPERTEXT TRANSFER PROTOCOL

Secure HyperText Transfer Protocol (S-HTTP) è stato sviluppato da Enterprise Integration Technologies (EIT); la descrizione che se ne fa in questo libro è basata su Internet Draft (Rescorla

1995). S-HTTP offre servizi di sicurezza flessibili per le transazioni HTTP; i client S-HTTP possono comunicare con server che non lo utilizzano e viceversa, benché queste transazioni, ovviamente, non utilizzino le caratteristiche di sicurezza di S-HTTP.
Attraverso un insieme di negoziazioni tra il client e il server, si ottengono notevoli miglioramenti sulle caratteristiche di sicurezza e sugli algoritmi associati. Ad esempio, l'utente può scegliere se la richiesta e la risposta sono firmate, codificate o tutt'e due. Qualsiasi messaggio può essere firmato, autenticato, codificato o qualsiasi combinazione di queste cose. I meccanismi di gestione delle chiavi comprendono segreti condivisi manualmente, come le password, lo scambio di chiavi pubbliche e la distribuzione di ticket Kerberos. Se si è scelto di utilizzare il supporto della firma, è necessario accodare il certificato adatto; S-HTTP supporta i certificati X.509 e le gerarchie di certificati come quelle utilizzate in PEM.
Le negoziazioni tra client e server vengono eseguite scambiandosi dati formattati, che comprendono varie opzioni di sicurezza che possono essere accettate dall'origine. Le righe dei dati devono conformarsi alle regole seguenti:

*<Riga>:=<Campo>':'<Valore_chiave>(';'<Valore_chiave>)**
*<Valore_chiave>:=<Chiave>'='<Valore>(','<Valore>)**
<Chiave>:=<Modalità> ','<Azione>
<Modalità>:='orig'|'recv'
<Azione>:='optional'|'required'|'refused'

Il valore *<Modalità>* indica se l'azione è riferita a un messaggio originato dall'agente o a un messaggio ricevuto da questo agente; l'agente è l'origine dei dati formattati.
Il parametro *<Azione>* specifica l'azione che deve essere eseguita. Il valore *recv-required* indica che il ricevente non processerà i messaggi privi della caratteristica specificata; il valore *recv-refused* indica invece che il ricevente non processerà messaggi con questa caratteristica di sicurezza. Oltre a ciò ù, per le informazioni che vengono originate da questo agente è possibile specificare valori di azioni corrispondenti. Ad esempio, *orig-required* indica che l'agente genera sempre la caratteristica di sicurezza.
Le intestazioni di negoziazione comprendono una serie di azioni corrispondenti. Ad esempio, *orig-required* indica che l'agente genera sempre la caratteristica di sicurezza.
Le intestazioni di negoziazione comprendono una seri di opzioni che servono a scegliere tra diversi algoritmi per ciascuna riga dell'intestazione; per ciascuno degli oggetti sotto riportati è presente una riga di intestazione.

14.8.1 SHTTP-Privacy-Domains

Questa intestazione specifica la classe degli algoritmi di codifica e il packaging dei dati; i due valori definibili per questa intestazione sono PEM e PKCS-7.
PKCS-7 un formato di incapsulamento crittografico dei messaggi simile a quello del PEM. PKCS-7 è definito da RSA e utilizza Abstract Syntax Notation di OSI.
Ad esempio:

SHTTP-Privacy-Domains: orig-required=pem
recv-optional=pem, pkcs-7

comporta che l'agente generi sempre messaggi di tipo PEM, ma possa leggere messaggi PEM o PKCS-7.

14.8.2 *SHTTP-Certificate-Types*

Questa intestazione specifica il formato accettabile del certificato; attualmente, S-HTTP consente soltanto il valore X.509 per i certificati X.509.

14.8.3 SHTTP-Key-Exchange-Algorithms

Questa riga indica gli algoritmi che devono essere utilizzati per lo scambio delle chiavi; i valori consentiti sono RSA, Outband, Inband e Krb. Il valore RSA viene utilizzato se si utilizza il meccanismo RSA; Outband indica che ci sarà qualche modifica esterna. Inband e Krb vengono utilizzati quando le ciavi sono specificate direttamente tra il client e il server.

14.8.4 SHTTP-Signature-Algorithms

Specifica l'algoritmo per la firma digitale; i due algoritmi supportati sono RSA e NIST-DSS.

14.8.5 SHTTP-Message-Digest-Algorithms

Questa riga identifica l'algoritmo utilizzato per garantire l'integrità dei dati attraverso una funzione hash. Gli algoritmi supportati sono RSA-MD2, RSA-MD5 e NIST-SHS.

14.8.6 SHTTP-Symmetric-Content-Algorithms

Questa riga specifica l'algoritmo a blocchi con chiave simmetrica utilizzato per codificare i dati. Gli algoritmi di codifica simmetrica per S-HTTP sono elencati di seguito.

- DES-CBC
- DES-EDE-CBC
- DES-EDE3-CBC
- DESX-CBC
- IDEA-CFB
- RC2-CBC
- RC4
- CDMF

14.8.7 SHTTP-Symmetric-Header-Algorithms

Questa riga contiene un elenco delle possibili codifiche con chiave simmetrica utilizzate per codificare le intestazioni.

- DES-ECB
- DES-EDE-ECB
- DES-EDE3-ECB
- DESX-ECB
- IDEA-ECB
- RC2-ECB
- CDMF-ECB

14.8.8 SHTTP-Privacy-Enhancement

Questa riga di intestazione specifica le caratteristiche di sicurezza associate con il messaggio; i valori possibili sono sign, encrypt e auth. Questi valori vengono utilizzati per indicare se il messaggio è rispettivamente firmato, codificato o autenticato.
Esistono altre righe di intestazione relative alla specifica delle varie chiavi e dei loro nomi simbolici.

14.9 S-HTTP ED SSL

S-HTTP ed SSL utilizzano sistemi diversi per offrire servizi di sicurezza agli utenti Web. SSL esegue un protocollo di negoziazione per stabilire una connessione sicura a livello di socket. I servizi di sicurezza sono trasparenti all'utente e all'applicazione.
I protocolli S-HTTP sono integrati in HTTP. I servizi di sicurezza vengono negoziati attraverso le intestazioni e gli attributi accodati alla pagina. I servizi S-HTTP sono disponibili soltanto per le connessioni di tipo http e l'applicazione (HTTP) è in grado di riconoscere il protocollo.
Dato che S-HTTP si trova al livello applicazioni ed SSL al livello di socket, è abbastanza facile concepire un sistema combinato tra S-HTTP ed SSL.

15. Commercio sicuro

Nel luglio del 1995, il Congresso degli Stati Uniti venne informato che il commercio elettronico stava diventando una realtà. Secondo Maddox (1995), l'Holiday Inn Worldwide di Atranta fu la prima azienda a proporre prenotazioni in linea su Internet, nel giugno del 1995. Il suo sito Web riceve circa

7000visitatori alla settimana, tre quarti dei quali verificano se esistono stanze disponibili. Il numero di siti Web sta aumentando rapidamente, così come il commercio su Internet. Secondo un rapporto di Forrester Research citato in Press (1994), il totale delle vendite al dettaglio negli Stati Uniti raggiungeva il valore di 1,5 trilioni di dollari, dei quali 200 milioni era dato dalle vendite su Internet, CompuServe e altri servizi in linea. Nel 1998, si prevede che le vendite in linea cresceranno fin quasi a 5 miliardi di dollari.
Il commercio su Internet sta diventando sempre più comune in varie forme. Va dall'ammissione di studenti presso le università, fino al rintracciamento in linea dei pacchi postali. In questo paragrafo viene presentata una panoramica del commercio elettronico su Internet e dei problemi di sicurezza correlati.

15.1 COMMERCIO SU INTERNET

Per le transazioni commerciali su Internet, esistono opportunità uniche, ma esistono anche problemi di sicurezza che vanno affrontati e risolti. Innanzitutto, occorre dare una breve spiegazione di alcune particolarità rispetto ai normali canali commerciali.

- Il commercio su Internet ha la facoltà di aggiornare prontamente la pubblicità dei prodotti sulle home page. Ad esempio, i negozi possono aggiornare quasi istantaneamente i propri cataloghi con i nuovi prodotti, specie se in confronto al ciclo di stampa e distribuzione dei cataloghi cartacei.
- È facile presentare offerte speciali per gestire eventi o servizi a breve e brevissimo termine. Ad esempio, una compagnia aerea può offrire uno sconto speciale per un particolare volo, in un particolare giorno, da Londra a New York poiché ci sono state delle cancellazioni dell'ultimo minuto. Un hotel può offrire sconti speciali se le camere sono libere un giorno molto prossimo.
- È possibile tracciare gli eventi in tempo reale. Ad esempio, è possibile seguire e compravendere azioni in tutto il mondo; altri esempi possono essere la determinazione di arrivi, partenze e ritardi di linee aeree, treni e bus.
- Si può accedere a servizi commerciali in linea. Esempi di servizi in linea comprendono l'home banking, le assicurazioni e i viaggi, nonché la pubblicità su Internet.

Nonostante tutti questi benefici, il percorso per arrivare alla diffusione del commercio su Internet non è così semplice come sembra.

19. Il commercio su Internet deve emulare da vicino la maniera con cui si conducono normalmente gli affari. Il commercio, al giorno d'oggi, consiste in acquisti, pubblicità, trattative, ordini e fatturazioni, pagamenti, gestione di conti correnti e via dicendo.

20. Il commercio su Internet dovrebbe essere sufficientemente flessibile per gestire gli errori, risolvere le dispute e offrire una documentazione legale accettabile per tutti gli aspetti delle transazioni commerciali.

21. Il commercio su Internet deve offrire una facilità d'uso sufficiente e sistemi di sicurezza adatti a guadagnarsi la fiducia e il rispetto dei clienti attuali. Il Web sta in parte risolvendo i problemi nella facilità d'uso; quelli di sicurezza vengono presentati più avanti in questo paragrafo.

22. Il commercio su Internet deve offrire un'integrazione perfetta con i sistemi commerciali attuali. Ad esempio, non dovrebbe esistere alcun impatto con gli attuali sistemi di processo degli ordini, di pagamento o di gestione dell'inventario.

Chiaramente, questi problemi possono risultare potenzialmente in una migrazione più lenta al commercio su Internet. Ci si deve aspettare che, prima o poi, le aziende si rivolgeranno a Internet come nuovo canale pubblicitario, al che seguiranno negozi e punti vendita per transazioni commerciali su Internet.

15.2 REQUISITI DI SICUREZZA

Garantire la sicurezza è fondamentale perché il commercio su Internet possa essere un successo, e un successo rapido. Clienti, aziende, banche e compagnie di carte di credito: chiunque richiede

una sicurezza impenetrabile per poter effettuare con tranquillità acquisti o trasmettere pagamenti su Internet.
Alcuni dei problemi più importanti relativi alla sicurezza del commercio elettronico vengono riportati di seguito.

23. Deve esistere un meccanismo che garantisca il trasferimento sicuro delle informazioni per i pagamenti. Il meccanismo di pagamento sicuro dovrebbe essere in grado di gestire differenti modalità di pagamento: carte di credito, assegni elettronici, carte di debito e denaro digitale. Oltre a ciò, il meccanismo di pagamento sicuro deve offrire una distribuzione dei dati privati in tre sensi. Si consideri un esempio, in cui Pietro ordina un televisore attraverso la home page di un negozio su Internet. A Pietro viene richiesto di immettere il numero di carta di credito, con la data di scadenza. Mentre il negozio deve essere certo che Pietro abbia una carta di credito valida e coperta, si può considerare che sia inutile mostrare al negoziante le informazioni sulla carta di credito di Pietro. La banca che fornisce la carta di credito deve quindi prendere queste informazioni, convalidarle e approvare l'acquisto del televisore. Questo esempio dimostra come sia necessario lo scambio a tre vie di dati sicuri per garantire la sicurezza nei pagamenti su Internet.

24. Deve esistere un meccanismo per garantire la non ricusazione sulle transazioni commerciali. Ad esempio, deve esistere un modo per provare che il mittente ha davvero inviato un ordine e che il destinatario l'ha veramente ricevuto. Questo problema viene parzialmente risolto autenticando l'origine di ciascun messaggio.

25. Deve esistere un meccanismo per assicurare l'integrità dei dati su Internet; questo è necessario per garantire la privacy delle transazioni. Se Anna ordina un servizio da tè particolare, può richiedere che nel proprio ordine o nell'offerta non vengano apportate modifiche durante la trasmissione dei dati su Internet. oltre a ciò, per ragioni di privacy, Anna potrebbe richiedere che nessun altro se non il negozio possa conoscere ciò che è scritto nell'ordine.

26. Deve esistere un'infrastruttura che possa stabilire la fiducia tra diverse parti. Ad esempio, chiunque può iniziare una transazione, facendosi passare per Gianni. Deve esistere un modo per Gianni di provare la propria identità al negozio; questa necessità risolta se Gianni invia al rivenditore il proprio certificato X.509. Probabilmente dovrà esistere più di un tipo di certificato, esattamente come esistono diversi tipi di carta di credito.

16. Modello di commercio sicuro

Basandosi sulle necessità e sui requisiti sopra riportati, in questo paragrafo si prova a proporre un modello per supportare il commercio sicuro su Internet, per mezzo delle carte di credito. Ci sono tre parti coinvolte in una transazione commerciale di questo tipo: un browser Web, un server Web e un gaeway. Il browser Web comprende un'applicazione per il pagamento sicuro, che serve a gestire il pagamento. Il server Web fornisce le funzioni necessarie al rivenditore ed è collegato ai sistemi di gestione degli ordini di questi. Infine, esiste un gateway alla rete finanziaria che collega il server del rivenditore alla banca che ha fornito la carta di credito.
Isa desidera acquistare una videocamera su Internet; fornisce perciò il proprio numero di carta di credito, insieme con la data di scadenza e il prezzo di acquisto. L'ordine di acquisto elettronico viene creato sul browser Web, il server Web va a recuperare i dettagli della videocamera e inoltra le relative informazioni al sistema di processo degli ordini del rivenditore. Le informazioni sulla carta di credito, insieme con l'entità dell'acquisto, vengono inoltrate al gateway.
Si considerino infine le tecnologie di sicurezza richieste per supportare questo ipotetico modello. Supponendo che ciascuna parte abbia una coppia di chiavi pubbliche e private, le informazioni sul pagamento possono essere codificate utilizzando la chiave privata di Isa. Il messaggio può poi essere firmato utilizzando la chiave privata; inoltre Isa deve inviare il proprio certificato X.509 per provare di essere veramente lei stessa. Il certificato deve quindi essere fornito da qualcuno che la banca conosca come autorità di certificazione approvata; inoltre, è necessario un protocollo a tre vie, per poter garantire una distribuzione sicura delle informazioni necessarie ai tre partecipanti.

Infine, si possono anche rendere protette e sicure le informazioni sull'ordine, oltre a quelle sul pagamento, utilizzando un protocollo di sicurezza Web, come SSL o S-HTTP, che sono stati appena spiegati.

17. FIREWALL INTERNET

Internet si sta rapidamente trasformando; da sistema di ricerca accademica, sta diventando un servizio a disposizione di tutti, per accedere alle informazioni e svolgere attività commerciali. Ogni giorno, sempre più reti si connettono a Internet; man mano che la dimensione di Internet cresce, crescono anche i rischi corsi dalle reti private connesse a Internet. Per proteggere le reti private da eventuali intrusioni e altri attacchi provenienti da Internet, è necessaria una barriera adeguata; questa barriera chiamata *filewall* (letteralmente: muro antincendio) dovrebbe intercettare tutto il traffico che passa tra una data rete privata e Internet. Un firewall non deve soltanto proteggere le risorse aziendali dagli attacchi degli hacker, ma intercettare anche qualsiasi trasmissione di informazioni aziendari importanti proveniente dalla rete privata e diretta su Internet.
Per prima cosa, verrano rivisti concetti e funzioni del firewall, dopodi ché tutti i componenti di un firewall saranno descritti componente per componente; in particolare, si parlerà di filtri, server proxy, Domain Name Service (DNS, servizi di denominazione dei domini) e gestione della posta. Il capitolo si conclude con una spiegazione di alcuni servizi di sicurezza più comuni forniti dai firewall, come la riservatezza dei dati.

17.1 CONCETTI FONDAMENTALI

17.1.1 Firewall

Un firewall serve a controllare l'accesso tra le reti private e Internet; il firewall intercetta tutti i messaggi trasmessi tra i due sistemi. Secondo la configurazione, il firewall è in grado di determinare se un pacchetto di dati o la richiesta di una connessione possono passare attraverso il firewall, oppure essere scartati. Durante la descrizione, si farà riferimento a due tipi di host: innanzitutto, esistono sistemi host sulle reti sicure, private e protette; questi sitemi host possono accedere a Internet solamente attraverso un firewall. gli altri sistemi host risiedono su Internet; a essi si può accedere soltanto attraverso Internet, al quale non si può concedere fiducia.

17.1.2 Necessità di un firewall

Una posta elettronica sicura protegge le comunicazioni tra due utenti Internet; un Web sicuro protegge le transazioni e gli scambi di dati tra due utenti Web; nessuno di questi sistemi protegge però le altre risorse di una rete privata. L'utilizzo di un firewall è un po' come chiudere la porta di casa, o assumere un portinaio: l'obiettivo è assicurarsi che soltanto la gente con un appropriato permesso possa entrare in casa e che nessuno che si trova in casa possa andarsene con gli ori di famiglia.
Quando una rete privata si trova connessa a Internet, ci sono tre aree di rischio.

27. Le informazioni. È infatti possibile sottrarre o distruggere le informazioni che si trovano sulla rete privata.
28. Le risorse. È possibile che qualcuno riesca a danneggiare o utilizzare a proprio scopo i sistemi informatici della rete privata.
29. La reputazione. Si può anche danneggiare la reputazione di un'azienda dimostrandone la vulnerabilità.

Oltre a ciò, la necessità di un firewall si fa sentire anche per un altro motivo: un'azienda potrebbe desiderare l'isolamento delle reti di differenti divisioni. Un'università potrebbe richiedere che la rete amministrativa (dove sono memorizzate, tra le altre cose, anche tutte le votazioni degli studenti) sia isolata dalla rete dedicata agli studenti; gli ospedali potrebbero desiderare di mantenere le schede dei pazienti separate dalla rete amministrativa, sia per questioni legali sia per questioni inerenti la

privacy dei pazienti stessi. La protezione all'interno di una stessa azienda può essere raggiunta con l'installazione di un firewall. E' possibile utilizzare uno o più firewall per isolare e controllare l'accesso tra le diverse parti di un'azienda.
Un firewall, in pratica, è un software che controlla l'accesso tra una rete privata e Internet, oppure tra diverse parti di una stessa rete privata. Un firewall deve soddisfare i requisiti di seguito riportati.

30. Qualsiasi pacchetto che non sia esplicitamente permesso riceve, per impostazione predefinita, un rifiuto. Il requisito implica che l'amministratore deve specificare esplicitamente qual è il traffico legittimo al quale è consentito di passare attraverso il firewall; tutto l'altro traffico di rete deve essere impedito per impostazione predefinita.
31. Appena possibile, il firewall deve tenere gli utenti esterni al di fuori della rete privata. L'accesso alla rete privata da parte di utenti esterni deve essere vietato; se proprio alcuni utenti Internet devono poter accedere liberamente ad alcuni file (come quelli pubblici dell'azienda), questi file dovrebbero essere installati al di fuori del firewall sul lato Internet.
32. Il firewall deve utilizzare file di registrazione, controllo e allarmi. Ciò significa che il firewall deve essere in grado di effettuare una continua registrazione degli eventi e del traffico che gli passa attraverso. Il firewall deve essere inoltre in grado di generare allarmi se si sospetta che qualcuno stia tentando di sfondarlo.

17.1.3 Progettazione di un firewall

La progettazione di un firewall comprende svariati componenti; questi componenti sono suddivisi in tre gruppi, ossia un sistema operativo sicuro, filtri gateway, servizi di denominazione dei domini e gestione della posta (messaggistica). I componenti vengono analizzati immediatamente, mentre i dettagli sono presentati più avanti nel capitolo.
Innanzitutto, il firewall stesso deve trovarsi in un ambiente sicuro: ciò significa che deve risiedere al di sopra di un sistema operativo sicuro che possa proteggere il codice del firewall e i file dall'attacco portato dagli hacker. Spesso su un dato sistema host l'unica applicazione che può essere eseguita è proprio il firewall; l'assenza di altre applicazioni sul sistema del firewall riduce infatti la possibilità di tentativi non autorizzati di oltrepassare il firewall stesso.
La comunità di Internet utilizza spesso il termine *bastione* per indicare un host dedicato a un fire wall; un host bastione è un computer con un livello di sicurezza molto elevao, poicé è completamente esposto all'attacco diretto degli hacker che girano su Internet.
Di seguito viene presentato il concetto di *filtri.* Lo scopo principale di un firewall è intercettare i pacchetti e consentire esclusivamente il traffico autorizzato. Il firewall intercetta perciò tutti i pacchetti che vengono trasmessi tra la rete privata e Internet; il filtro tiene conto di un insieme di regole definite dell'amministratore del firewall durante la fase di configurazione. Le regole sono basate su diversi parametri, che comprendono gli indirizzi IP, i numeri di porta e il tipo di applicazione. Il problema principale con la tecnica dei filtri è che si tratta di un sistema basato sugli indirizzi IP, che non sono sicuri di per sé; il risultato è che un dato host può farsi passare per un altro modificando l'indirizzo IP all'origine.
Un *gateway di applicazione* intercetta il traffico e autentica gli utenti al livello delle applicazioni TCP/IP. La funzione di gateway di applicazione viene spesso ottenuta implementando un cosiddetto *server proxy*, o più semplicemente *proxy*. Un utente sulla rete privata può accedere a un proxy, il quale autentica l'utente; dopo l'autenticazione, l'utente accede al server remoto che si trova su Internet. In modo simile, tutte le comunicazioni da Internet verso la rete privata vengono ricevute dai proxy, poi analizzate e inoltrate secondo la necessità. Poiché un server proxy funziona a livello di applicazione, può essere necessario un server proxy separato per ciascun tipo di applicazione. Il proxy autentica ogni utente, sia proveniente dall'interno della rete privata, sia proveniente da Internet. Per evitare agli utenti non autorizzati di poter entrare nella rete privata o di uscirne è necessario un sistema di autenticazione assolutamente sicuro.
Anche il server *SOCKS* serve per fornire un supporto gateway attraverso un firewall. La differenza principale tra un server proxy e un server SOCKS consiste nel fatto che con un proxy è necessario cambiare il modo con il quale un utente accede al server Internet, senza apportare modifiche al

software client; un SOCKS, invece, richiede la modifica del software client, ma le procedure dell'utente non vengono cambiate in alcun modo.
I firewall possono altresì comprendere un DNS e un servizio di messaggistica. Il DNS (Domain Name Service, servizio di denominazione di dominio) isola di servizio di denominazione della rete privata da quello di Internet; il risultato è che gli indirizzi IP interni degli host della rete privata non sono disponibili agli utenti Internet. I servizi di messaggistica assicurano invece che qualsiasi scambio di posta elettronica tra la rete privata e Internet venga elaborato e passato attraverso il firewall.

17.1.4 Gradi di sicurezza dei firewall

E' possibile individuare diversi gradi di sicurezza di un firewall, secondo i componenti che sono stati installati. Se si consente un accesso totale e aperto da Internet sulla rete privata, non si garantisce alcun tipo di sicurezza. È poi possibile aggiungere dei filtri ai tipici prodotti router, in modo da garantire un livello minimo di intercettazione di traffico non autorizzato. Il firewall può quindi comprendere filtri e gateway di applicazione. Continuando, di possono aggiungere dei proxy, in combinazione con diverse tecniche di autenticazione. È anche possibile migliorare la sicurezza della rete privata aggiungendo al firewall servizi di messaggistica e funzioni di denominazione di dominio. Il firewall può quindi risiedere al di sopra di un sistema operativo sicuro, migliorando anche la sicurezza del firewall stessa. Il firewall può inoltre garantire la riservatezza e l'integrità dei dati, come si descriverà più avanti in questo capitolo. Infine come misura di sicurezza definitiva, l'azienda può anche decidere di negare qualsiasi tipo di accesso a Internet. Anche se potrebbe apparire soltanto una soluzione teorica, per certi tipi di ambiente che necessitano di assoluta sicurezza questa può rivelarsi l'unica scelta accettabile.

17.1.5 Rischi irrisolti

Ci sono diversi tipi di rischi per la sicurezza che un firewall non è in grado di risolvere. Alcuni di questi rischi vengono riassunti di seguito.

- Intrusione dall'interno. Il firewall non è in grado di proteggere le risorse da un attacco proveniente da un utente interno alla rete privata. Il firewall è semplicemente un gateway che intercetta il traffico tra una rete privata e Internet; inoltre, un firewall interno all'azienda può intercettare il traffico tra diversi dipartimenti dell'azienda. In ogni caso, un utente interno potrebbe sottrarre dati critici o informazioni riservate dell'azienda, oppure danneggiarne le risorse senza essere intercettato dal firewall. Questo rischio quò essere affrontato solamente implementando sistemi di autenticazione e controllo d'accesso adeguati.
- Traffico Internet diretto. Un firewall può servire solamente se tutto il trafffico di Internet viene gestito dal firewall stesso. Esso non è infatti in grado di proteggere le risorse della rete privata dal traffico che avviene direttamente con Internet, oltrepassando la barriera posta dal firewall. Ad esempio, se un utente della rete privata scambia dati attraverso un accesso diretto (una normale connessione telefonica, per fare un esempio) con Internet, il fire zall non è in grado di intercettare, e di conseguenza nemmeno di esminare, i dati. Ciò significa che è fondamentale, per la rete privata, assicurare che tutto il traffico da e verso Internet venga ritrasmesso attraverso il firewall.
- Virus. Normalmente un firewall non è in grado di proteggere una rete privata da virus provenienti dall'esterno. Un virus può essere trasferito sulla rete privata con un'operazione di FTP (File Transfer Protocol, protocollo di trasferimento file) o con altri mezzi. Per realizzare la protezione dai virus, il firewall deve aver il software adatto.

17.2 FILTRAGGIO DI PACCHETTI

Esistono attualmente sul mercato diversi prodotti router che instradano i pacchetti IP basandosi sull'indirizzo di destinazione riportato nell'intestazione IP. Se il router sa come inviare il pacchetto all'indirizzo di destinazione, lo fa senza ulteriori problemi; se invece il router non sa come inviare il

pacchetto all'indirizzo di destinazione specificato, lo restituisce all'indirizzo di origine unitamente a un messaggio ICMP di "destinatario irraggiungibile".
I router utilizzati nei firewall vengono chiamati screening router o filtri. Nel momento in cui ricevono un pacchetto, il filtro determina se questo deve essere scartato oppure inoltrato all'indirizzo di destinazione; la decisione dipende dalle regole del filtro, regole che vengono specificate dall'amministratore del firewall.

17.2.1 Regole dei filtri

le regole dei filtri vengono spesso definite durante la fase di installazione del firewall, anche se possono essere modificate, aggiunte o eliminate in una fase posteriore. Ciascuna regola consiste di due parti: il campo dell'azione e i criteri di selezione. Il campo dell'azione specifica l'azione da intraprendere se il pacchetto viene selezionato da questa regola. Sono possibili due tipi di azione.

- BLOCK (o DENY, rispettivamente blocco o negazione): questa azione implica che il pacchetto selezionato deve essere rifiutato.
- PERMIT (o ALLOW, consenso): questa azione specifica che il pacchetto selezionato può essere inoltrato.

I criteri di selezione possono basarsi su parecchi tipi diversi di parametri. Alcuni dei parametri più comuni sono riportati di seguito.

- Indirizzi di origine e di destinazione. La regola del filtro comprende una maschera di indirizzo che serve a selezionare un pacchetto secondo l'indirizzo di origine o quello di destinazione.

La scelta dell'indirizzo viene realizzata specificando due indirizzi numerici; il primo è quello desiderato, mentre il secondo è la maschera che serve a selezionare i bit del campo di indirizzo. Si supponga ad esempio che si desideri selezionare qualsiasi pacchetto il cui indirizzo di origine inizi con 157.4.5. L'indirizzo di origine del pacchetto è 157.4.5.0, mentre la maschera di indirizzo per la selezione del pacchetto è 255.255.255.0; per questa maschera di indirizzo, i primi tre byte selezionano tutti e 24 i bit dei primi tre byte dell'indirizzo di origine del pacchetto. I 25 bit selezionati vengono quindi confrontati con il valore 157.4.5; se esiste corrispondenza, il pacchetto viene selezionato. Un procedimento simile può essere utilizzato anche per il pacchetto di destinazione.

- Porta di origine e di destinazione. La regola del filtro può anche essere applicata a un numero di porta specifico, sia dell'host di origine sia di quello di destinazione.
- Protocollo. È possibile selezionare un pacchetto basancosi sul livello del protocollo. Ad esempio, un pacchetto può essere selezionato se utilizza i protocolli TCP, UDP o ICMP.
- Direzione. Infine, è anche possibile selezionare un pacchetto basandosi sulla direzione della trasmissione rispetto al firewall. Ad esempio, un pacchetto indirizzato all'interno (inbound packet) proviene da Internet ed è indirizzato alla rete privata, mentre un pacchetto indirizzato all'esterno (outbound packet) proviene dalla rete privata ed è indirizzato su un indirizzo Internet.

Un tipico firewall può consentire fino ad un massimo di 255 regole di filtro; l'ultima specifica di scartare (azioni BLOCK o DENY) tutti i pacchetti, come verrà descritto più avanti.
Il componente filtro di un firewall funziona come segue. Quando un pacchetto arriva al componente filtro, viene verificato, confrontandolo con la prima regole del filtro. Se la regola vale per il pacchetto, viene eseguita l'azione specificata per la regola, ossia il pacchetto viene rifiutato oppure inoltrato. Se invece la regola non vale per il pacchetto, si verifica la seconda regola e così via fin all'ultima. Per ciascuna regola, se il pacchetto soddisfa i criteri di selezione viene eseguita l'azione specificata. Si supponga poi che il pacchetto non venga selezionato da alcuna regola, fino ad arrivare all'ultima. L'ultima regola specifica però di scartare tutti i pacchetti, per cui il pacchetto viene scartato. In breve l'azione predefinita per il filtraggio dei pacchetti è di scartare il pacchetto, a meno che non venga selezionato altrimenti da una delle regole di filtro. Questa è una regola fondamentale della politica di sicurezza, intesa a evitare che pacchetti non autorizzati possano passare sulla rete privata.

17.2.2 Configurazione dei filtri

Un problema riguardante il filtraggio dei pacchetti è la complessità di configurare le regole dei filtri. Le regole sono infatti molto complesse e possono richiedere una conoscenza approfondita del sistema di indirizzamento del TCP/IP. L'amministratore del firewall può quindi commettere degli errori durante la definizione delle rigole di filtro. Per questo motivo i produttori si stanno indirizzando verso prodotti che semplifichino la specificazione delle regole anche senza un'approfondita conoscenza del TCP/IP. Inoltre esistono sul mercato programmi di utilità che possono essere d'aiuto nel controllo della sintassi delle regole.

17.2.3 Attacco spoofing

Il 22 gennaio 1995 lo Stanford Linear Accelerator Computing Center (SLAC) rilevò che qualcuno stava controllando l'host che si trovava dietro il firewall. Si scoprì che il programma intruso si era nascosto nel sistema operativo e si stava appropriando degli ID e delle password di tutti gli account. Il giorno successivo, il sistema informatico dello SLAC venne arrestato e tutti gli accessi esterni della rete furono tagliati. L'attaccante aveva utilizzato il cosiddetto *attacco spoofing* (letteralmente: attacco imbroglio).
In questo caso, l'host attaccante invia all'host obiettivo una richiesta, riproducendo l'indirizzo di origine dell'host attaccato. L'host obiettivo invia quindi una risposta positiva alla richiesta di connessione. L'host attaccante deve evitare che l'host obiettivo riesca a rilevare la risposta e ad annullare la connessione, dal momento che si tratta di una connessione simulata. Per raggiungere questo scopo, l'host attaccante invia numerose richieste di connessione all'host attaccato, il che porta a riempire il vero host di richieste di connessione; nel frattempo, l'host attaccato si perde la risposta della connessione simulata. A questo punto, l'host attaccante deve rispondere alla risposta di connessione inviata dall'host obiettivo; la risposta deve inoltre contenere un numero di sequenza. La maggior parte delle installazioni utilizza però l'implementazione Berkeley del TPC, per la quale i numeri di sequenza si riescono a indovinare con una certa facilità. L'host attaccante predice quindi il numero di sequenza e invia all'host obittivo una risposta corretta, il risultato è una connessione regolare, tale che l'host attaccante può inviare diversi comandi all'host obiettivo.
Questo tipo di attacco può essere evitato configurando appropriatamente il firewall, come descritto di seguito.

17.3 REGOLE RACCOMANDATE

1. Come si è spiegato nel paragrafo precedente, uno dei problemi più grandi presentati dal sistema dei filtri consiste nel fatto che l'indirizzo di origine di un'intestazione IP non è sicuro; ciò significa che un host può essere in grado di modificare il proprio indirizzo di origine in modo che appaia come se provenisse da un altro host. Per evitare un attacco di questo tipo, leregole di filtro devono scartare qualsiasi pacchetto proveniente da Internet che contenga l'indirizzo di origine di un host all'interno della rete privata. La ragione di questo comportamento sta nel fatto che un pacchetto proveniente da Internet che presenti l'indirizzo origine di un host all'interno della rete privata indica che il pacchetto è un tentativo di penetrare nel sistema. Le regole di filtro devono quindi specificamente rifiutare il pacchetto.
2. Se si sa che un host su Internet invia normalmente pacchetti falsificati, è necessario bloccare qualsiasi tipo di traffico proveniente da quell'host e anche diretto verso l'host. È sufficiente aggiungere una nuova regola di filtro, all'inizio di tutte le regole esistenti, che rifiuti tutti i pacchetti con un indirizzo di origine uguale a quello dell'host attaccante.

17.4 SERVER PROXY

I server proxy intercettano ed esaminano il traffico al livello applicazioni del TCP/IP. L'utente della rete privata deve innanzitutttto accedere al server proxy prima di poter accedere a un server di applicazioni su Internet. La maggior parte dei proxy dei firewall prevedono le funzioni di TELNET ed FTP; poiché si tratta di servizi al livello applicazioni, per ciascun tipo di applicazione è necessario un proxy separato. Il client proxy può essere invece implementato in molti modi, descritti di seguito.

Scopo di un server proxy è intercettare l'accesso utente verso un'appliczione Internet, autenticare l'utente, assicurarsi che sia autorizzato ad accedere all'applicazione e donsentirgli quindi di accedere al server su Internet. Anche per un utente su Internet che desideri accedere al sistema informatico dell'azienda è previsto un servizio simile. Quando l'utente sul client TELNET viene autenticato dal server proxy, questo verifica se l'utente può accedere al seervizio di TELNET presente su Internet; se sì, l'utente può inviare una richiesta TELNET su Internet. Di seguito viene descritta una procedura per utilizzare il server proxy.

1. Il client A sulla rete privata invia una richiesta TELNET al firewall; si tratta di una procedura nuova per l'utente, che non richiede però alcuna modifica al software client.
2. Il server proxy sul firewall richiede all'utente di immettere ID e password.
3. L'utente immette ID e password; il server proxy autentica l'utente verificandone l'ID e confrontandolo con la password a esso corrispondente. Se l'autenticazione dell'utente non va a buon fine, la sua richiesta viene rifiutata, mentre se va a buon fine si passa al punto 4.
4. L'utente invia la richiesta TELNET al server TELNET B che si trova sull'host di Internet.
5. Il server B autentica l'utente; se l'operazione va buon fine si passa al punto 6, altrimenti la richiesta viene rifiutata.
6. Qualsiasi sia il traffico dal client A verso il server B, il codice del firewall lo intercetta e sostituisce l'indirizzo origine del pacchetto IP con quello del firewall stesso. In questo modo, gli indirizzi interni della rete privata non vengono mai inviati su Internet.

Possono poi esistere file, come dei documenti standard, che devono essere resi disponibili tramite FTP anonimo. In effetti, gli utenti Internet possono accedere direttamente a questi file, senza alcun tipo di autenticazione. Per supportare questo tipo di trasferimento, alcune reti private mettono a disposizione un apposito server al di fuori del firewall. Questa soluzione limita gli utenti Internet ad accedere solamente alle risorse locali che risiedono su questo server; chiaramente, la connessione tra il server esterno e la rete privata deve assolutamente essere effettuata soltanto attraverso il fierwall.

17.5 REALIZZAZIONE DI SERVER PROXY

Come si è detto, un sistema proxy consiste di un server proxy situato sul firewall, mentre dal lato client esistono almeno tre sistemi per implementare il proxy.

1. **Personalizzazione della procedura utente.** Con questo sistema, le procedure utente vengono modificate in modo da implementare il sistema proxy; si tratta del sistema spiegato in precedenza. Vantaggio fondamentale di questo metodo consiste nel fatto che il software client non viene toccato. Dato che su una rete esiste probabilmente moltissimo installato, questo sistema è sicuramente molto conveniente. Esiste però anche uno svantaggio ossia che l'utente deve essere istruito sulle nuove procedure necessarie per l'accesso al server proxy. Per siti particolarmente grandi, dove le applicazioni TCP/IP vengono utilizzate da molto tempo, il costo dell'istruzione può essere molto elevato.
2. **Personalizzazione del software client.** Questo sistema richiede di dover modificare il software client, mantenendosi totalmente trasparente all'utente per quanto riguarda l'accesso a Internet. Il software client intercetta e redireziona infatti tutto il traffico. Un'implementazione molto comune di questo metodo è SOCKS, già citato in precedenza e descritto nel dettaglio più avanti.
3. **Mantenere sul firewall tutte le modifiche.** In questo caso, non occorre modificare né il software client né le procedure di accesso dell'utente. Questo metodo richiede comunque che tutti i messaggi provenienti da e diretti verso Internet passino attraverso il firewall. La situazione tipo vede l'utente inviare una richiesta di connessione per un server Internet, alla quale, in maniera del tutto trasparente all'utente, il firewall risponde intercettando la richiesta, autenticando l'utente, verificando la richiesta e procedendo con la connessione.

17.6 SOCKS

SOCKS serve per fornire un sistema proxy attraverso la personalizzazione del software client. Per effetturare l'intercettazione presso il firewall tra l'utente della rete privata e il server di Internet, SOCKS richiede di apportare modifiche al software client. SOCKS viene solitamente utilizzato per accedere d ahost su una rete privata su server Internet.
Il protocollo SOCKS è stato pubblicato da David Koblas e Michelle R. Koblas (Koblas 1992). La versione 4 del prodotto è descritta in Leech (1994), oltre che in alcuni testi sulla sicurezza come Chapman (1995) e IBMFW (1995).
Il prodotto richiede modifiche ai client TCP/IP tali da supportare l'interazione con il server SOCKS. Il client modificato effettua chiamate a SOCKS in modo totalmente trasparente all'utente. Il server SOCKS risiede sul firewall e interagisce con i client modificati; il server su Internet non necessita invece di alcuna modifica.
SOCKS versione 4 (Leech 1994) funziona come segue. Lo scopo di SOCKS è offrire uno schema generico per le applicazioni TCP7IP, entro il quale sia possibile tilizzare in tutta sicurezza i servizi di un firewall. Il protocollo è indipendente dall'applicazione TCP/IP supportata. Quando un client TCP/IP richiede di accedere a un server, il codice del client deve innanzitutto aprire una connessione TCP/IP verso il server SOCKS: il numero di porta convenzionale del servizio SOCKS è 1080. se la richiesta di connessione viene accettata, il client invia una richiesta al server SOCKS, che comprende una serie di informazioni sotto riportate.

- Porta di destinazione desiderata.
- Indirizzo di destinazione desiderato.
- Informazioni di autenticazione.

Il server SOCKS valuta le informazioni contenute nella richiesta, accetando la richiesta stessa e stabilendo la connessione con il server Internet, oppure rifiutando la richiesta. La valutazione dipende dai dati di configurazione del server SOCKS; in qualsiasi caso, il server SOCKS invia al client una risposta, che contiene le informazioni che indicano se la richiesta è stata accettata oppure no.
Un chiaro vantaggio del protocollo SOCKS è che è totalmente trasparente all'utente: questi può accedere a Internet senza nemmeno accorgersi della presenza di un firewall. Non è quindi necessario istruire gli utenti quando si installa un firewall sulla rete privata. D'altro canto, questo metodo richiede una serie di modifiche al software client, per cui è necessario aggiornare tutte le stazioni di lavoro degli utenti. L'aggiornamento necessario può essere effettuato a livello di applicazioni oppure di codice TCP/IP sottostante. Nel primo caso, ciascuna applicazione client, come TELNET ed FTP, deve essere modificata in modo da supportare SOCKS; nel secondo caso, il protocollo SOCKS viene implementato nello stack del TCP/IP in modo che sia trasparente anche alle applicazioni che sul TCP/IP si basano. In questo modo, ogni applicazione TCP/IP può fare un uso trasparente dei servizi del protocollo SOCKS.
Infine, è opportuno sottolineare il fatto che qualsiasi approccio che faccia uso di un gateway si basa pesantemente sul sistema di autenticazione sottostante; uno schema di autenticazione poco affidabile o sicuro può facilmente vanificare tutti gli sforzi fatti per l'installazione di un firewall.

17.7 AUTENTICAZIONE

Una tipica applicazione TCP/IP come TELNET richiede l'immissione di un ID e di una password; almeno però che non sia protetta in altro modo, la password viene trasmessa su Internet in chiaro. Il primo problema, in questo caso, consiste nell'autenticazione dell'utente al firewall; altro problema è poi l'autenticazione dell'amministratore del firewall al firewall.

17.8 RETE PRIVATA SU INTERNET

Si considerino per un momento i sue scenari dell'autenticazione degli utenti: nel primo scenario, il client inizia inviando al firewall il proprio ID e la propria password; questo scambio di dati avviene sulla rete privata (sicura). Il rischio di furto della password è, abbastanza chiaramente, inferiore in questo scenario, in confronto a quello di una password trasmessa su Internet. Il secondo scenario vede l'utente accedere all'host su Internet inviando l'ID e la password attraverso Internet; la trasmissione di password su Internet viene esaminata di seguito.

17.9 INTERNET SU RETE PRIVATA

Nel secondo scenario, l'utente accede da Internet a un server sulla rete privata; per prima cosa, l'utente invia il proprio ID e la propria password al firewall, il che può condurre a un attacco, nel quale l'attaccante immette la password codificata e ottiene l'accesso al firewall, dopodiché alla rete privata. Per evitare questo tipo di attacco, è consigliabile utilizzare password monouso. Esistono diversi tipi di token card che possono generare password casuali da utilizzare una sola volta. In questo caso, anche se la password viene sottratta, non è di alcuna utilità all'intruso, poiché una password monouso non viene più utilizzata dopo essere stata usata una prima volta.

17.10 AUTENTICAZIONE DELL'AMMINISTRATORE

Si consideri ora l'accesso di un utente al firewall, in qualità di amministratore. Alla fine del 1994, pare che un intruso sia riuscito a penetrare in un firewall, con la qualifica di amministratore, partendo da Internet. l'intruso aveva provato diverse password su Internet e, alla fine, era riuscito a indovinare quella corretta. Supponendo che il firewall risieda su un sistema Unix, ci sono due precauzioni che si possono prendere per evitare questo genere di attacchi.

1. L'amministratore dovrebbe sempre utilizzare una password monouso per accedere al firewall da una postazione remota.
2. L'accesso al firewall come amministratore non dovrebbe essere convalidato per chiunque riesca a penetrare da lato Internet. In effetti, l'accesso al firewall come amministratore dovrebbe essere consentito esclusivamente dalla rete privata; questa precauzione può ridurre in maniera sostanziale le possibilità per un hacker di ottenere un accesso come amministratore al firewall partendo da Internet.

In ultimo, i file dove vengono memorizzate le password sono notoriamente un bersaglio principe degli hacker.

17.11 DOMAIN NAME SERVICE

Un firewall può offrire una funzione di name service per gli utenti che si trovano sulla rete privata, o al suo esterno. Il firewall non dovrebbe però divulgare gli indirizzi IP degli host all'interno della rete privata; ciò significa che, per le richieste provenienti da Internet, il firewall dovrebbe risolvere tutti i nomi degli host all'interno della rete privata nell'indirizzo IP del firewall. Per le richieste provenienti dagli host all'interno della rete privata, invece, il firewall deve offrire nomi per la risoluzione degli indirizzi degli host di Internet.
Per prima cosa, un client della rete privata richiede la risoluzione di un indirizzo per un host che si trova su Internet; il server di denominazione della rete privata inoltra questa richiesta al firewall. Il DNS de firewall accede al server di denominazione su Internet, ottiene l'indirizzo IP di un host che si trova all'interno della rete privata; questo, infine, inoltra la risposta al client dal quale ha avuto origine la richiesta.
Si supponga ora che un client di Internet richieda l'indirizzo IP di un host che si trova all'interno della rete privata. La richiesta viene inviata a un server di denominazione su Internet, il quale inoltra la richiesta al firewall. Questo a sua volta risponde con il proprio indirizzo IP del firewall, invece di poter arrivare a conoscere quello degli host all'interno della rete privata.

17.12 MESSAGGISTICA

La posta elettronica è una delle ragioni principali per le quali una rete privata può pensare di connettersi a Internet. Viene utilizzata ampiamente dagli utenti di Internet per scambiarsi informazioni l'un con l'altro; solitamente, per la gestione della posta (o messaggistica) su Internet si utilizza il protocollo SMTP (Simple Mail Transfer Protocol, protocollo semplice per il trasferimento di posta), anche se sono stati sviluppati sistemi per la gestione sicura della posta.
La posta elettronica può anche dover essere intercettata e inoltrata appropriatamente. Il cosiddetto demone (daemon, programma in background in esecuzione su un server) della posta, SENDMAIL, è noto per avere diversi punti deboli e continua a essere oggetto di numerosi attacchi.
Per proteggere la rete privata, un sistema consiste nel fornire un gateway di posta sulla rete privata. La posta elettronica che parte dalla rete privata viene innanzitutto inviata al gateway della posta, il quale, a sua volta, seleziona la posta destinata a Internet e inoltra al programma di gestione della posta che si trova sul firewall. La posta in ricezione da Internet viene invece inviata dal firewall al gateway sulla rete privata. Per gli utenti Internet, il firewall è l'unico gateway di posta esposto agli attacchi. Questo sistema comporta diversi vantaggi.

1. Tutta la posta elettronica proveniente da Internet viene ricevuta da firewall e non dal gateway della posta della rete privata. Ciò è positivo, poiché il firewall è meglio equipaggiato per gestire eventuali tentativi di intrusione di quanto non lo sia un gateway della posta.
2. Esiste un unico punto di controllo della posta elettronica tra la rete privata e Internet; in questo modo, un sito può implementare una serie di controlli che servano a intercettare e verificare la presenza di possibili virus o altro software dannoso inviato alla rete privata. Il gateway della posta può anche verificare che soltanto gli utenti autorizzati possano inviare o ricevere posta su e verso Internet.

17.13 SICUREZZA IP

La comunità degli standard di Internet ha di recente sviluppato una serie di RFC (Request For Comments, richiesta di commento) che garantissero meccanismi di sicurezza per il protocollo IP.
L'RFC 1825 (Atkinson 1995a) è una panoramica del sistema di sicurezza di IP che sonsite di un'intestazione di autenticazione IP e di un trasporto di sicurezza per l'incapsulamento IP (ESP,IP Encaplùsulation Security Payload). L?RFC 1826 (Atkinson 1995b) tratta appunto del'ESP IP. L'RFC 1828 (Metzger 1995) descrive l'autenticazione IP che utilizza Keyed MD5 e l'RFC 1829 (Karn 1995) tratta invece della trasformazione ESP DES-CBC. Si inizia ora rivedendo alcuni dei concetti fondamentali, seguiti da alcuni potenziali utilizzi nei firewall.

17.14 INTESTAZIONE DI AUTENTICAZIONE IP

L'intestazione di autenticazione IP serve a offrire i servizi di autenticazione e integrità tra due entità che supportino questo tipo di intestazione. L'intestazione può essere utilizzata tra host o gateway. Poiché cono richiede la riservatezza, è liberamente esportabile.
L'intestazione ESP IP comprende un indice dei parametri di sicurezza (SPI, Security Parameter Index). La combinazione tra SPI e indirizzo di destinazione identifica in maniera univoca *un'associazione di sicurezza*. Un'associazione di sicurezza comprende diversi parametri che identificano i servizi di crittografia applicabili al datagramma; esempi di questi parametri possono essere gli algoritmi di autenticazione e di codifica, le modalità degli algoritmi, le chiavi utilizzate per essi e la durata delle chiavi. Il sistema di sicurezza IP utilizza moltissimo le associazioni di sicurezza.
L'intestazione di sicurezza IP consiste delle informazioni di autenticazione per il datagramma IP; queste informazioni vengono calcolate applicando una funzione di autenticazione crittografica sul datagramma IP; la funzione viene a sua volta calcolata utilizzando una chiave segreta. Secondo Metzger (1995), è necessario l'utilizzo dell'algoritmo MD5 per garantire il supporto dell'intestazione di autenticazione IP; essa dovrebbe essere utilizzata quando gli utenti richiedono autenticazione e integrità dei dati, ma non riservatezza.

17.15 IP ENCAPSULATION SECURITY PAYLOAD (ESP)

Questo trasporto è inteso a offrire integrità dei dati e riservatezza per i datagrammi IP. ESP codifica i dati da proteggere, dopodiché li posiziona come parte ESP del datagramma. ESP funziona in due modalità, la modalità tunnel e la modalità trasporto.
In modalità tunnel, il mittente incapsula il datagramma originale in ESP, ottiene la chiave di codifica (utilizzando l'associazione di sicurezza) e applica la trasformata di codifica. L'ESP codificato viene posizionato all'interno di un datagramma IP che comprende intestazioni IP in chiaro, che servono per instradare il pacchetto attraverso la rete IP. Il destinatario elimina l'intestazione in chiaro, ottiene la chiave di sessione utilizzando l'associazione di sicurezza e decodifica infine l'ESP utilizzando la chiave di sessione.
In modalità trasporto, soltanto il frame del livello di trasporto (TCP o UDP) viene incapsulato nell'ESP; questa modalità risparmia larghezza di banda, poiché le intestazioni IP non vengono codificate.

17.16 SICUREZZA IP PER I FIREWALL

Un firewall può includere componenti che offrano riservatezza e integrità. Una rete aziendale può consistere di due o più reti private, interconnesse attraverso Internet: l'azienda può perciò richiedere che esistano riservatezza integrità dei dati durante lo scambio tra le reti. Un altro esempio si ha quando un dirigente d'azienda è in viaggio e deve comunicare in maniera sicura dalla stanza d'albergo con l'azienda. Anche in questo caso, è necessario che il traffico dei dati tra stanza d'albergo e l'azienda sia codificato.
Le necessità sopra riportate possono essere risolte utilizzando i meccanismi di sicurezza IP. Utilizzando la modalità tunnel di ESP, il traffico dei dati tra i due firewall può essere codificato; in questo modo, si può assicurare la riservatezza dei dati tra le due reti private. Si noti che la funzione è trasparente agli utenti finali e ai sistemi host delle due reti private; inoltre, non sono necessarie, modifiche né cambiamenti al software degli host.
Si consideri poi la necessità dell'utente che deve comunicare in maniera sicura con l'azienda dalla propria stanza d'albergo, utilizzando Internet. Per offrire la riservatezza dei dati, il computer portatile dell'utente (nella stanza d'albergo) e il firewall aziendale devono supportare la modalità tunnel di ESP, oppure la modalità trasporto. Questo sistema dà per scontato che presso l'albergo non esista un firewall, il che è abbastanza probabile.
Infine, si può richiedere anche la riservatezza tra i capi della comunicazione, tra un host sulla rete privata e un altro host su Internet. Questa necessità può essere affrontata implementando la modalità tunnel su ciascuno dei sistemi host.

18. GESTIONE DEL SISTEMA DI SICUREZZA

Per *gestione del sistema di sicurezza* si intende sia la definizione delle politiche di sicurezza di un'intera azienda, sia la loro applicazione. La gestione di un sistema di sicurezza può essere suddivisa in due compiti principali: il primo riguarda la *gestione dei dati del sistema di sicurezza*, il secondo la *protezione dei dati specifici delle procedure di gestione.* La gestione dei dati del sistema di sicurezza consiste nella memorizzazione, nel reperimento e nell'aggiornamento di informazioni come gli ID degli utenti le password e le chiavi di codifica. La protezione dei dati di gestione consiste invece nella protezione di questi dati sia quando si trovano memorizzati sul sistema, sia quando vengono trasmessi sulla rete. Prima di trattare questi argomenti è però necessario parlare delle politiche di sicurezza da adottare a livello di impresa.
In questo capitolo verranno quindi trattati tre argomenti principali: la definizione e la realizzazione delle politiche di sicurezza, la gestione dei dati del sistema di sicurezza e la protezione dei dati di gestione.

18.1 POLITICHE DI SICUREZZA

Il principale obiettivo di una *politica di sicurezza* è proteggere le risorse dell'azienda, senza però trascurare l'effetto dell'applicazione di un sistema di sicurezza sulla produttività degli utenti. La definizione di una politica di sicurezza, che deve essere applicata in modo uniforme in tutta l'azienda, si articola principalmente in tre fasi.
Durante la prima fase vengono definiti i vari aspetti della politica stessa. La seconda fase è dedicata alla realizzazione delle procedure e alla loro effettiva introduzione. La terza fase riguarda l'implementazione della politica appena creata, ad esempio per mezzo degli schemi di sicurezza descritti nei capitoli precedenti. In questo paragrafo verranno pertanto descritte le prime due fasi.

19. Definizione della politica di sicurezza

La politica di sicurezza deve tenere conto di tutti i problemi connessi alla protezione delle risorse. Di seguito sono elencati i più importanti.

1. **Politica di gestione.** Questo aspetto riguarda la scelta del tipo di autenticazione, le regole per l'utilizzo delle password e la definizione delle responsabilità dei singoli nei confronti delle risorse a loro disposizione. La politica di gestione definisce quindi le regole del sistema di sicurezza e le responsabilità dell'amministratore della sicurezza dei dirigenti e dei dipendenti.
2. **Politica del controllo d'accesso.** Questo aspetto della politica riguarda i dati necessari per controllare gli accessi, l'utilizzo del controllo d'accesso DAC o MAC e l'attribuzione del livello di riservatezza ai dipendenti.
3. **Politica della riservatezza dei dati.** Questo aspetto della politica riguarda la definizione del tipo di codifica necessario per le varie risorse. Specifica quindi le tecniche di codifica da adottare, la lunghezza delle chiavi, gli algoritmi per la distribuzione delle chiavi e l'autorità di certificazione.
4. **Politica dell'integrità dei dati.** Questo aspetto della politica definisce le esigenze di integrità dati di ciascuna risorsa. Specifica quindi i protocolli e le tecnologie da adottare per ottenere il livello di integrità dati desiderato.
5. **Politica di gestione dei dati.** Questo aspetto della politica riguarda la gestione dei dati dell'azienda, ossia del sistema informativo aziendale. Specifica quindi i requisiti necessari per la memorizzazione, la trasmissione, il reperimento e l'aggiornamento dei dati. Il sistema informativo aziendale è composto dagli elementi elencati di seguito.
    - **Dati** amministrativi dell'azienda. Comprendono tutti i file e i database riguardanti l'attività dell'azienda. Ad esempio, i database dei clienti e dei fornitori, dei dati contabili, degli stipendi e degli ordini di acquisto.

- Dati di sicurezza. Comprendono gli ID degli utenti, le password, le chiavi di codifica, gli elenchi per il controllo d'accesso e tutte le altre informazioni necessarie per l'utilizzo e la realizzazione del sistema di sicurezza.
- Dati di gestione del sistema. Comprendono tutte le informazioni necessarie per il controllo e la registrazione delle operazioni effettuate sulla rete. Queste informazioni devono essere memorizzate e trasmesse in modo sicuro.

Procedure per la definizione della politica di sicurezza

Di seguito è descritta la procedura da utilizzare per definire la politica di sicurezza da adottare.

1. Identificare tutte le risorse principali dell'azienda, classificandole in base al loro valore effettivo.
2. Indicare gli obiettivi della protezione da applicare agli elementi classificati al punto 1.
3. Raccogliere tutti i possibili flussi di informazioni per le risorse selezionate.
4. Effettuare l'analisi dei rischi per ciascuna risorsa.
5. Definire le regole necessarie a proteggere le risorse dai rischi individuati.
6. Definire le procedure di sicurezza in base alle regole definite al punto 5.
7. Eseguire le procedure di sicurezza dopo averne informato i diretti interessati.

Molti di questi passaggi sono ovvi. Nel seguito, il problema della definizione di una politica di sicurezza verrà trattato in funzione del valore intrinseco delle risorse da proteggere.

Analisi dei costi

La realizzazione di un sistema di sicurezza di rete, che abbia lo scopo di proteggere tutte le risorse dell'azienda, comporta il sostenimento di vari costi. Naturalmente, è necessario valutare l'opportunità di sostenere tali costi in base al valore delle risorse da proteggere.
Se il valore di una risorsa è A e P è il costo da sostenere per introdursi nel sistema e compromettere la sicurezza o il funzionamento della risorsa, il *fattore di rischio* è dato da A/P. Il fattore di rischio è quindi il rapporto fra il valore della risorsa e il costo da sostenere per danneggiarla o violarne la riservatezza. Una rete può essere considerata sicura se il valore di P è superiore a quello di A: in questo caso, infatti, il costo da sostenere per danneggiare la risorsa supera il valore della risorsa stessa.
Inoltre, se N è il costo di realizzazione del sistema di sicurezza per una determinata risorsa (investimento), in una rete ben strutturata questo costo dovrebbe essere proporzionale al valore di A e, naturalmente, inferiore ad esso. Il rapporto K = N/A è detto *fattore di investimento*.
Per molte reti, il costo N, necessario per la realizzazione del sistema di sicurezza, e il costo P, necessario per violare il sistema di sicurezza, sono costanti per tutte le risorse. In questi casi, è necessario stimare il fattore di rischio per le risorse più importanti.
Per ulteriori informazioni sulle politiche di sicurezza, consultare i testi di Shaffer (1994), Amoroso (1994) e Russel (1991) e il manuale IBMSEC (1995). Nella parte restante del capitolo verranno trattati la gestione dei dati del sistema di sicurezza e la protezione dei dati di gestione.

19.1 GESTIONE DEI DATI DEL SISTEMA DI SICUREZZA

I *dati del sistema di sicurezza* comprendono gli ID degli utenti, la password, gli elenchi per il controllo d'accesso e le chiavi di codifica. Un tipico esempio di gestione di una chiave di codifica è costituito dalla memorizzazione sulla stazione di lavoro della chiave privata di un utente. Poiché la chiave di codifica è in genere una stringa da 512 a 2048 bit, gli utenti non sono in grado di ricordarla a memoria. Tuttavia, poiché è indispensabile per generare la firma digitale dell'utente, questa chiave deve essere memorizzata sul computer ma , come altre informazioni di questo tipo, deve essere protetta dagli attacchi di eventuali hacker o intrusi. Per proteggere queste informazioni, è ad esempio possibile dotare gli utenti di speciali schede, da inserire nel computer quando necessario. Oltre a consentire la memorizzazione dei dati, sulle schede è anche possibile memorizzare gli algoritmi di codifica.

In una stessa azienda, possono essere presenti dati di sicurezza riguardanti sistemi acquistati da diversi produttori. Tuttavia, ciascun sistema può disporre di un proprio database per i dati di sicurezza. Ad esempio su ogni sistema può essere presente un database, o registro di sicurezza per gli ID degli utenti e le password da utilizzare per accedere al sistema stesso.
La gestione di questi dati di sicurezza comporta però numerosi problemi. L'amministratore del sistema di sicurezza deve infatti gestire e aggiornare tutti i registri. Quando un dipendente viene licenziato o trasferito, tutti i registri corrispondenti devono essere aggiornati in brevissimo tempo. In un'azienda di grandi dimensioni, questo compito può richiedere molto tempo e, soprattutto, può essere fonte di errore.
Di recente sono stati proposti vari metodi per risolvere il problema della gestione di più registri di sicurezza. Nella situazione descritta sopra, infatti necessario ridurre al minimo il numero degli interventi dell'amministratore, necessari per la creazione e l'aggiornamento dei registri. L'amministratore dovrebbe infatti disporre di un registro di sicurezza unificato, o poter accedere a tutti i registri come se si trattasse di un unico registro. Ad esempio, l'amministratore deve poter aggiungere o eliminare con un unico comando tutte le voci corrispondenti a un determinato utente. Questa procedura può addirittura essere automatizzata in modo da non richiedere alcun intervento umano, delegando le operazioni di aggiornamento dei registri al software dell'amministratore, ma richiede l'utilizzo di programmi di grandi dimensioni per coordinare la gestione di tutti i registri.
Il registro del sistema OSF DCE contiene varie informazioni sul profilo dell'utente. Utilizzando un apposito programma di utilità, l'amministratore del sistema di sicurezza può modificare il registro DCE aggiungendo, eliminando o sostituendo informazioni nel database. Oltre a questi requisiti, DCE 1.1 consente di utilizzare anche gli *attributi estesi del registro* (ERA, Extended Registry Attributes). Questa caratteristica consente di effettuare accessi singoli grazie all'aggiunta di alcune informazioni al registro DCE (consultare il manuale OSFDCE11, 1995). Per ulteriori informazioni sul registro DCE, consultare il testo di Rosenberry (1992).

19.2 PROTEZIONE DEI DATI DI GESTIONE DEL SISTEMA DI SICUREZZA

La gestione di qualsiasi rete richiede l'utilizzo di determinati protocolli, per proteggere le informazioni scambiate tra l'host gestito e l'host di gestione. Ad esempio, è necessario impedire a chiunque l'invio di falsi allarmi, come segnalazioni di interruzione di attività in un impianto nucleare o richieste di sospensione dei servizi di rete in aeroporto.

19.3 SNMP

Per consentire il controllo delle reti TCP/IP, la comunità di Internet ha definito alcuni protocolli standard. Questi protocolli, noti come *SNMP (Simple Network Management Protocol)*, hanno lo scopo di gestire i componenti delle reti TCP/IP. Nel corso degli ultimi anni, l'intera comunità ha lavorato al miglioramento delle funzioni di sicurezza della prima versione di SNMP; molte delle funzioni di sicurezza di SNMP sono state infatti estese nella versione 2. In questo paragrafo verranno quindi descritte le funzioni di SNMP versioni 1 e 2.
Il protocollo SNMP definisce il formato da utilizzare per scambiare informazioni tra una stazione di gestione della rete e un agente di gestione. La stazione di gestione è in genere, ma non necessariamente, una stazione separata che costituisce l'interfaccia fra un essere umano, come l'amministratore di rete, e il sistema di gestione della rete. Sulla stazione di gestione vengono eseguite una o più applicazioni per la gestione della rete e il ripristino dalle situazioni di errore. La gestione di piattaforme come router, bridge e host viene invece effettuata creando un agente di gestione. Lo scambio di dati tra la stazione di gestione e l'agente di gestione è regolato da protocollo SNMP.
In questo protocollo, il termine *oggetto* viene utilizzato per indicare una qualsiasi delle risorse di rete. Ciascun oggetto della rete è rappresentato da una variabile di dati e l'insieme di tutte le variabili è chiamato *base di informazioni per la gestione (MIB*, Management Information base). Questo insieme di informazioni indica gli oggetti che devono essere gestiti dal nodo di gestione.
Di seguito sono elencate le funzioni del protocollo SNMP.

1. **GET.** Consente di trovare nel MIB di un agente di gestione le informazioni riguardanti un determinato oggetto.
2. **SET.** Consente alla stazione di gestione di modificare le variabili associate agli oggetti nel MIB di un agente di gestione.
3. **TRAP.** Consente all'agente di gestione di avvisare la stazione di gestione quando si verificano eventi di particolare importanza.

SNMP è progettato per operare sul protocollo UDP. Pertanto, ciascun agente di gestione deve implementare i protocolli SNMP, UDP e IP.

SNMP versione 2

La prima versione del protocollo SNMP presenta però alcune carenze, soprattutto per quanto riguarda la protezione delle informazioni durante il trasferimento. Di seguito sono descritti tutti i principali difetti di SNMP versione 1.

1. Il traffico tra la stazione e l'agente di gestione può essere intercettato da una terza parte.
2. Le funzioni GET e SET possono essere eseguite anche da host hacker in grado di sostituirsi alla stazione o all'agente di gestione. In questo modo, l'eventuale hacker ha la possibilità di leggere e modificare i dati del MIB.

Questi due problemi di sicurezza, che sono stati già visti in precedenza, possono essere risolti utilizzando le funzioni di riservatezza e richiedendo l'autenticazione dell'origine dei dati.
Nel 1993, su Internet sono stati diffusi vari RFC (Request For Comments , richieste di commenti) per descrivere la versione 2 di SNMP (SNMPv2). I protocolli di sicurezza di SNMPv2 sono descritti nel testo di Galvin, RFC 1446, del 1993.
In questo testo vengono descritti tre servizi di sicurezza: la protezione dell'integrità, l'autenticazione dell'origine e la protezione della riservatezza dei dati. La funzione di integrità dei dati è stata sviluppata utilizzando l'algoritmo MD5 per il calcolo del valore di controllo. Questo algoritmo viene infatti utilizzato per calcolare il valore di controllo di 128 bit corrispondente a ogni singola porzione dei messaggi SNMPv2.
L'autenticazione dell'origine dei dati viene invece effettuata come descritto di seguito. Prima di calcolare il valore di controllo, al messaggio viene aggiunto un valore segreto, noto solo al mittente e al destinatario del messaggio SNMPv2. In questo modo, l'autenticazione dell'origine del messaggio viene effettuata semplicemente verificando il valore di controllo MD5.
La protezione della riservatezza dei dati viene invece garantita dall'utilizzo di DES in modalità CBC (Cipher Block Chaining Mode, concatenazione di blocchi cifrati). La porzione di messaggio SNMPv2 da inviare viene infatti codificata e inviata insieme al messaggio originale.

20. IL NUOVO PORTALE INTERNET DEL MINISTERO DEL TESORO, DEL BILANCIO E DELLA PROGRAMMAZIONE ECONOMICA

Il portale del Ministero del Tesoro, del Bilancio e della Programmazione come strumento di erogazione di servizi economica è nato da un processo di revisione del sito www.tesoro.it, come concreto strumento interattivo di informazione e di servizio offerto al Paese, tenendo anche conto delle recenti esigenze sorte all'interno del processo di globalizzazione e, soprattutto, delle forti dinamiche in ambito europeo.

Con una direttiva emanata il 10 novembre 2000, il ministro Vincenzo Visco ha sancito la nascita del Portale del Tesoro, con la costituzione di un comitato di coordinamento, presieduto dal Portavoce del ministro e composto da un rappresentante per ciascuno dei quattro Dipartimenti e dal responsabile dell'area Internet della Consip S.p.A, la concessionaria per i servizi informatici del ministero.

La nuova iniziativa, sotto il profilo della presenza in Rete della Pubblica Amministrazione, parte da una posizione di indiscussa autorevolezza: 9.160 documenti, 25mila pagine web, 14.250 immagini, 15 banche dati, 10 negozi elettronici, oltre 20 milioni di contatti nel corso del 2000.

Fin dalla pagina di benvenuto, il nuovo portale rappresenta il superamento non soltanto grafico, ma anche concettuale, della tradizionale impostazione dei siti Internet – basati sul modello "vetrina" - per sfruttare fino in fondo le potenzialità interattive del nuovo media – che si rifanno invece all'analisi dei bisogni dell'utente. Dal punto di vista progettuale, ciò ha significato dover integrare le funzioni di gestione e di offerta archivistica dell'abbondante documentazione, con modalità innovative per la Pubblica Amministrazione, non più cioè soltanto di mera consultazione e mutuate anche dal mondo del marketing.

Con questa iniziativa, il ministero del Tesoro, del Bilancio e della Programmazione economica ha voluto allinearsi a quanto espresso dal piano di e-government del Governo ("le amministrazioni centrali dovranno erogare servizi a quelle locali e queste ultime saranno responsabili di rappresentare sul territorio lo sportello verso i cittadini e le imprese…") e il portale si configura come l'insieme strutturato degli ingressi telematici per l'accesso al sistema informativo del ministero, in uno spirito di collaborazione reciproca, - istituzioni/cittadini/istituzioni – e nell'ottica della trasparenza e della massima efficienza.

Naturalmente, questa nuova filosofia ha condizionato le scelte grafiche, dei colori, dei simboli, del linguaggio, nella direzione di un colloquio aperto, semplice, trasparente, elaborato per rispondere alle esigenze di ciascuna tipologia di utente. Né poteva essere dedicata meno attenzione a dotare il portale di un sistema di consultazione destinato anche alle persone disabili, utilizzando alcune raccomandazioni del WAI-Web Accessibility Iniziative, insieme di suggerimenti, concordati a livello internazionale e rivolti agli sviluppatori dei siti web, per la realizzazione di pagine consultabili anche da certe categorie di utenti portatori di handicap. Rispondendo con questo tempestivamente all'appello lanciato dalla Presidenza del Consiglio con la circolare del 13 marzo 2001, n. 3/2001, che fornisce le linee guida per l'organizzazione, l'usabilità e l'accessibilità dei siti web delle Pubbliche Amministrazioni.

20.1 HOME PAGE

La pagina di benvenuto è divisa in quattro "spicchi" fondamentali: in alto a sinistra gli ingressi alle quattro aree tematiche, i percorsi di navigazione suggeriti; in basso a sinistra l'angolo istituzionale del Ministero; in alto a destra "La Vetrina", le aree tematiche cioè che in quel momento sono ritenute di maggior rilevanza; al centro "In Primo Piano", dove di volta in volta viene evidenziato quale, di questi temi, prevale per attualità; infine "Ultimi Arrivi", dove scorrono gli ultimi tre inserimenti in ordine temporale nell'intero sito.

All'interno di ciascuna area – alla quale si accede attraverso una qualsiasi delle porte (tutte si rivelano al passaggio del mouse) presenti in home page – comincia il portale vero e proprio: tutte le pagine sono costruite secondo uno standard che consente in qualsiasi momento di cambiare percorso, gli argomenti e le tipologie di servizi offerti sono accorpati per semplificare la ricerca, come primo oggetto viene proposto un sommario dei contenuti che utilizza la tecnologia delle "ancore" per scorrere velocemente le pagine. Le funzioni interattive per la raccolta delle informazioni o l'accesso a servizi sono semplificate dall'uso di strumenti grafici come mappe (es.: carte dell'Italia attive al passaggio del puntatore) o icone-simbolo (es.: cassetta delle lettere in "area giornalisti" per prenotarsi la ricezione dei comunicati stampa direttamente nella casella di posta elettronica)

20.2 I QUATTRO SPORTELLI E GLI UTENTI

CITTADINO

Per il giovane che va a studiare all'estero; per l'anziano che aspetta la pensione; per chi cerca un lavoro o un lavoro migliore; per chi cerca un aiuto economico per avviare un'attività; per chi vuole investire in titoli di Stato; per chi vuole difendersi dall'usura; per chi è un dipendente pubblico o vuol partecipare a un concorso o fare uno stage di formazione; per tutti i curiosi che vogliono scoprire il Palazzo e come funziona

IMPRESA

Per le imprese e gli imprenditori; per chi vuole investire al Sud, nel Nordest, all'estero, utilizzando i finanziamenti che promuovono lo sviluppo; per chi l'azienda deve portarla nell'euro; per chi vuol diventare fornitore della Pubblica Amministrazione; per chi vuol conoscere le leggi, le agevolazioni, l'andamento dell'economia nazionale, comunitaria, globale

P. A.

Per la Pubblica Amministrazione, centrale o periferica; per ottenere informazioni e servizi direttamente dal ministero; per evitare gare e appalti e fare gli acquisti on-line; per formare e riqualificare il personale; per conoscere e utilizzare le iniziative che promuovono lo sviluppo territoriale; per accedere alla normativa e stampare la modulistica

STUDI&MEDIA

Per giornalisti e studiosi; per leggere e scaricare; per conoscere subito, per sapere cosa e dove cercare; per avere accesso alle banche dati, agli archivi dei documenti, alle biblioteche, alle pubblicazioni periodiche e agli arretrati del ministero; per leggere in anteprima i discorsi del ministro

20.3 LE AREE ISTITUZIONALI

IL MINISTRO	la biografia di Vincenzo Visco, i suoi più stretti collaboratori, i suoi discorsi più recenti e più significativi
L'ORGANIGRAMMA	tutta la struttura del ministero del Tesoro, del Bilancio e della Programmazione economica, ufficio per ufficio, responsabile per responsabile
I DIPARTIMENTI	le quattro grandi strutture in cui è divisa l'Amministrazione, compiti, ambiti di competenza
BIBLIOTECHE E DOCUMENTI	le biblioteche e le raccolte di riviste ospitate all'interno del Palazzo di via XX Settembre e l'archivio di tutta la documentazione
L'EDICOLA	le pubblicazioni periodiche prodotte all'interno del ministero
VISITA SCOLASTICA	viaggio virtuale all'interno del Palazzo delle Finanze, alla scoperta dei tesori della storia e dell'arte, e di chi ci lavora, come e perché
MAPPA E GUIDA	la struttura del sito e i consigli per navigarlo con profitto
CERCA E CHIEDI	i diversi motori di ricerca, per gli addetti ai lavori, per chi ha bisogno di aiuto, per mettersi in contatto con l'Amministrazione, tramite l'Ufficio per i Rapporti con il Pubblico
L'AGENDA DEL MINISTERO	le date e gli appuntamenti da non dimenticare

20.4 LA VETRINA

DEBITO PUBBLICO	le pagine web dedicate alla presenza dello Stato sul mercato, aggiornate in tempo reale
RELAZIONI INTERNAZIONALI	pagine, ancora in elaborazione, dedicate all'attività istituzionale in materia di relazioni finanziarie
G7 FINANZIARIO	il sito del G7 Finanziario, gestito dalla Presidenza italiana
CIPE	appuntamenti e delibere del Comitato Interministeriale Programmazione Economica
QCS	per conoscere da vicino uno dei più efficaci strumenti della politica per lo sviluppo
EURO	accesso in evidenza alle tematiche legate all'introduzione della moneta unica
ACQUISTI ON LINE	il sito per gli acquisti via Internet di beni e servizi della Pubblica Amministrazione
INTESE IST. DI PROGRAMMA	banca dati sulle varie tipologie negoziali in ambito regionale
CONTI PUBBL. TERRITORIALI	quadro dettagliato dei fabbisogni e delle risorse già impiegate nel processo di decentramento amministrativo
PARI OPPORTUNITÀ	le pagine gestite dal comitato interno al ministero
ALTRI	raccolta di link utili
THE ENGLISH CORNER	i documenti tradotti in lingua inglese

21. Portale Intranet del 1° Dipartimento

Il portale Intranet del Dipartimento del Tesoro, operativo da dicembre 2000 all'indirizzo http://prometeo/intranetdt, offre numerose funzionalità di interesse per il Dipartimento.

Attualmente, consente l'accesso ai seguenti servizi:

- Applicazioni
- Bacheca
- Banche Dati
- Formazione
- Link a siti di interesse
- Modulistica
- News
- Organigrammi
- Ricerca
- Rubrica (novità all'interno dei Numeri Utili)

Il servizio Applicazioni permette all'utente di accedere a tutte le applicazioni in modo organico ed all'interno dello stesso portale.
Le Applicazioni presenti attualmente sono quattro:

- BPE (Beni Perduti all'Estero)
- GFT (Gestione Flussi di Tesoreria)
- SIGI 2K (Sistema Informativo Gestione Infrazioni)
- GEPAD (Gestione Patrimonio Dati)

Il servizio di Bacheca permette la consultazione di documenti del Dipartimento che, nella fase di avvio, saranno organizzati per Direzioni di competenza e per aree tematiche sulla base delle attività istituzionali degli Uffici afferenti la Direzione stessa.

Il servizio Banche Dati prevede la fruizione da parte dell'utente di alcune banche dati di natura giuridica o economica che possono essere gratuite o a pagamento. In alcuni casi vengono accedute attraverso una utenza ed una password.

Il servizio Formazione permette all'utente la consultazione del piano formativo e di altri documenti inerenti la formazione (consuntivi, analisi del fabbisogno formativo, ecc.).

Nella Intranet il piano formativo viene aggiornato on line, inserendo eventuali modifiche/integrazioni ai corsi/seminari indicati nel progetto distribuito all'inizio dell'anno

Il servizio Link mette a disposizione dell'utente una serie di collegamenti internet a siti di interesse.

Il servizio di Modulistica permette all'utente la consultazione e la stampa di vari moduli prodotti dagli uffici del Dipartimento.

Anche i moduli sono organizzati e ripartiti per aree tematiche così da facilitarne la ricerca ed il reperimento.

A tal fine, è inoltre previsto un apposito motore di ricerca dei moduli pubblicati nel sito.

Il servizio si limita, al momento a semplificare la distribuzione della modulistica all'interno del Dipartimento del Tesoro. Non è prevista l'automazione del processo di invio dei moduli compilati, che continuerà comunque ad essere ricevuta dagli uffici interessati in formato cartaceo.

Il servizio News consente all'utente di essere aggiornato circa nuove funzioni implementate o novità inerenti funzioni già presenti nella intranet.

Il servizio Organigrammi permette la consultazione degli organigrammi del Dipartimento del Tesoro e della CON.S.I.P. e l'utilizzo di eventuali applicazioni di cui l'ufficio è responsabile e della parte di modulistica gestita dallo stesso.

All'interno di ciascuna Direzione è possibile accedere alle informazioni di dettaglio della relativa segreteria.

L'organigramma della CON.S.I.P. è anch'esso collegato alla rubrica attraverso la quale è possibile risalire alle informazioni dei dipendenti della società.

Il servizio di Ricerca si compone di due motori di ricerca, uno per il sito intranet ed uno per la rete esterna internet.

Il primo consente di effettuare la ricerca di documenti e pagine pubblicati all'interno del sito intranet.

Il secondo consente di effettuare ricerca nella rete intranet utilizzando i principali motori presenti attualmente sul mercato (AltaVista, Excite, Lycos, Yahoo, etc.)

Il servizio di Rubrica si compone di due funzionalità: Ricerca e Numeri utili. La prima permette all'utente di reperire informazioni quali: struttura di appartenenza, sede, telefono, fax, e-mail per i dipendenti del MTBPE e della CON.S.I.P:.

Per i dipendenti del MTBPE è possibile conoscere anche la qualifica e in un prossimo futuro le informazioni logistiche (piano, scala, lato, stanza).

E' prevista la possibilità di salvare i risultati di una ricerca (es. i dipendenti di un ufficio) in un foglio di lavoro Excel.

La seconda funzionalità consente la consultazione di una serie di numeri d'utilità che possono riguardare uffici, enti ed organizzazioni interni al MTBPE ed esterni ad esso.

Nella sezione Numeri Utili Interni è possibile reperire informazioni inerenti numeri di telefono, fax ed indirizzi e-mail. Le stesse informazioni possono essere anche reperite accedendo all'organigramma del Dipartimento del Tesoro.

Sempre nella sezione Numeri Utili Interni sono disponibili le principali informazioni riguardanti gli Uffici dirigenziali degli altri dipartimenti del MTBPE.

In ausilio agli utenti, per consentire un'agevole navigazione all'interno del portale Intranet DT, è disponibile una Guida in Linea che indica, per ogni servizio, le modalità operative e di utilizzo.

Tale Guida in linea (il cui link è attivo nella barra di menù verticale, in alto a sinistra nella Intranet) può essere consultata elettronicamente o stampata.

Infine, nella intranet, e' stata disposta una casella di posta elettronica per il Webmaster (wintranet@dt.tesoro.it), a cui si possono inoltrare richieste di chiarimenti, suggerimenti, segnalazioni inerenti i servizi offerti dal Portale, mentre, utilizzando l'indirizzo ufficio3.banchedati@dt.tesoro.it, e' possibile inoltrare richieste di abilitazioni per la sezione Banche Dati.