

Ricerca sulle reti

INDICE

1	Modello OSI	3
2	Struttura di rete.....	4
2.1	Client e server.....	5
2.2	Schede di rete	5
2.3	i mezzi trasmissivi	5
2.4	I dispositivi di rete	7
2.5	Le tipologie di reti	8
3	Tecnologie di trasmissione	9
3.1	Lan ethernet.....	10
3.2	Accesso remoto e wan	10
3.3	VPN: l'alternativa alla wan privata	11
3.4	linee analogiche	12
3.5	Linee ISDN	12
3.6	Linee dedicate	13
3.7	Linee DSL	13
4	Sistemi di sicurezza.....	14
4.1	Il firewall.....	14
4.2	VPN ed Extranet.....	15
4.3	La crittografia.....	16
5	I protocolli di rete.....	16
5.1	Protocolli di 1° e 2° livello.....	16
5.2	Protocolli di 3° e 4° livello.....	17
5.3	Protocolli di 5°, 6° e 7° livello	18

1 Modello OSI

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

7 - Livello APPLICAZIONE
6 - Livello PRESENTAZIONE
5 - Livello SESSIONE
4 - Livello TRASPORTO
3 - Livello RETE
2 - Livello COLLEGAMENTO DATI
1 - Livello FISICO

🚧 Il livello fisico

Il livello fisico si occupa della trasmissione dei singoli bit da un estremo all'altro dei vari mezzi di comunicazione. Perché si possa avere una connessione tra PC è necessario dunque, ma non indispensabile, un supporto fisico, composto solitamente da un cavo e da interfacce di comunicazione. La connessione tipica di una rete locale utilizza sistemi Ethernet. I cavi e le schede Ethernet appartengono a questo primo livello. Protocollo standard è il protocollo Ethernet.

🚧 Il livello dati

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

🚧 Il livello di rete

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

🚧 Il livello trasporto

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

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

Il livello sezione

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

Il livello presentazione

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

Il livello applicazione

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

2 Struttura di rete

Ogni sistema di rete comprende:

almeno **due computer**;

un'interfaccia di rete su ogni computer, generalmente chiamata **scheda di rete (NIC - Network Interface Card)** o adattatore;

un **mezzo di collegamento**, generalmente un filo (doppino telefonico) o un cavo di rete (RJ45) o le fibre ottiche. Esiste inoltre la possibilità di far comunicare i computer e le periferiche collegati in rete senza tali strumenti, in questo caso si parla di comunicazione "wireless";

un **sistema operativo di rete** quale Windows 95/98/2000 o Windows NT Microsoft, Novell NetWare, Appleshare, Artisoft LANtastic.

un **dispositivo di connessione** (router o modem).

La maggior parte delle reti, persino quelle con solo due computer, comprende anche un hub o uno switch che fungono da punto di connessione tra i computer. Altri elementi aggiuntivi sono il router e i sistemi di sicurezza.



2.1 Client e server

Quando la rete si ingrandisce e si aggiungono altri computer, uno di essi diventa il cosiddetto **server**, cioè un punto centrale per l'archiviazione dei file o dei programmi applicativi in rete.

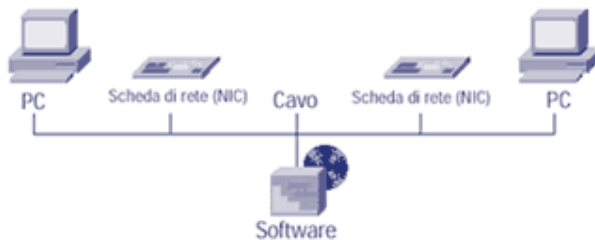
Dal server partono anche le connessioni verso le risorse comuni come le stampanti o i fax.

Trasformare un computer in un server dedicato consente di risparmiare sia sui costi aggiuntivi di nuove infrastrutture di rete, sia sui costi di gestione delle stesse. I computer collegati al server vengono chiamati **client**. Non è comunque necessario disporre di un server dedicato nella propria rete. Tuttavia, se alla rete si aggiungono sempre più utenti, un server dedicato può fungere da centrale per i compiti amministrativi come il backup dei file e gli upgrade dei programmi.



2.2 Schede di rete

Le schede di rete o adattatori, vengono generalmente installate all'interno dell'alloggiamento del computer. Per i portatili e i notebook sono disponibili in formato PCMCIA e occupano un solo slot. Anche per la scelta delle schede è necessario pianificare il futuro. Le schede Ethernet supportano solo i collegamenti Ethernet mentre le schede 10/100, che hanno ormai prezzi simili, possono supportare anche i collegamenti Fast Ethernet di prestazioni superiori. Inoltre, è necessario assicurarsi che le schede scelte siano compatibili con il cablaggio utilizzato, doppino telefonico (denominato anche 10BaseT), cavo coassiale (denominato anche 10Base2) o un'alternanza di entrambi.



2.3 i mezzi trasmissivi

Cablaggio

Una delle caratteristiche fondamentali di una rete è rappresentata dal mezzo trasmissivo impiegato per il trasferimento dei dati. La scelta del cavo è correlata di solito alla topologia, al protocollo e all'estensione della rete. I mezzi trasmissivi più utilizzati nella cablatura di una rete locale LAN sono:

- 🔧 **il cavo coassiale**, che assomiglia ai cavi per la televisione;
- 🔧 **il doppino telefonico**, che viene usato di norma nelle nuove installazioni ed è conforme a diversi standard quali, ad esempio, il doppino non schermato (UTP, Unshielded Twisted Pair) di Categoria 3, utilizzato spesso nelle linee telefoniche, e quello di Categoria 5, usato nelle reti;
- 🔧 **le fibre ottiche**, che generalmente vengono riservate ai collegamenti tra le apparecchiature di "dorsale" (backbone) delle grandi reti. In ambienti particolari, tuttavia, si utilizzano cavi a fibra ottica ad alta resistenza. Il cavo a fibre ottiche è il sistema di cablaggio più affidabile ma è anche il più costoso;
- 🔧 **i segnali radio o i raggi di luce infrarossa** (wireless LAN).



Il cavo coassiale

Il cavo coassiale ha al suo interno un filo conduttore di rame. Il cavo che ricopre il filo è di plastica e serve a garantire l'isolamento tra il filo di rame ed uno schermo di metallo intrecciato. Tale schermo serve a bloccare qualsiasi interferenza esterna. Il cavo coassiale è molto simile al cavo della TV. L'unica differenza è che trasporta dati digitali anziché analogici. I dati digitali sono molto più sensibili al rumore e alle interferenze del segnale, per cui le reti che utilizzano come mezzo trasmissivo il cavo coassiale possono essere cablate solo per distanze limitate a meno che non vengano impiegati dei ripetitori. Per molto tempo il cavo coassiale è stata l'unica possibilità per la cablatura di reti locali ad alta velocità, nonostante il grosso svantaggio dei costi (il cavo è difficile e costoso da fabbricare, non si può piegare facilmente e ed è soggetto a frequenti rotture meccaniche ai connettori).

Il doppino telefonico

Il doppino telefonico (o twisted pair) può essere di categoria 3 o di categoria 5. Il doppino di categoria 3, utilizzato in passato, non è più adatto per le nuove tecnologie: ora esiste il doppino TP di categoria 5, testato fino a 100 Mhz, che garantisce velocità dell'ordine dei 100 Mbps. Il twisted pair può essere schermato (STP - Shielded Twisted Pair) o non schermato (UTP - Unshielded Twisted Pair). Mentre il cavo coassiale permette cablaggi a catena con il TP sono possibili solo situazioni punto a punto (peer-to-peer); infatti la topologia di rete che utilizza come mezzo trasmissivo il TP è la topologia a stella. L'UTP è oggi il tipo di cablatura più usata nelle reti LAN. Viene infatti utilizzato nella maggioranza delle reti Ethernet come pure nelle Token Ring.

Le fibre ottiche

Il cavo in fibra ottica utilizza i segnali luminosi per trasferire i dati e li trasmette attraverso una sottile fibra in vetro. E' generalmente composto da una parte centrale in vetro circondata da parecchi strati di materiali protettivi. Il fatto di trasmettere impulsi luminosi anziché segnali elettrici consente di eliminare il problema delle interferenze elettriche. Per questo motivo è il mezzo trasmissivo ideale per quegli ambienti che hanno parecchie interferenze elettriche. I dati che viaggiano sulle fibre ottiche vengono trasferiti a velocità altissime e su distanze maggiori rispetto al cavo coassiale e al twisted pair. Le fibre ottiche vengono spesso utilizzate per le dorsali (backbone).

Wireless LAN

Le LAN di tipo wireless usano, per far comunicare i computer tra loro, segnali radio ad alta frequenza o raggi di luce infrarossa, anziché utilizzare i tradizionali cavi per i collegamenti. Ogni computer, ovviamente, deve avere un dispositivo che permette di spedire e ricevere i dati. Le reti wireless sono molto utili negli edifici dove può essere difficoltoso effettuare il cablaggio o crearlo in brevissimo tempo.

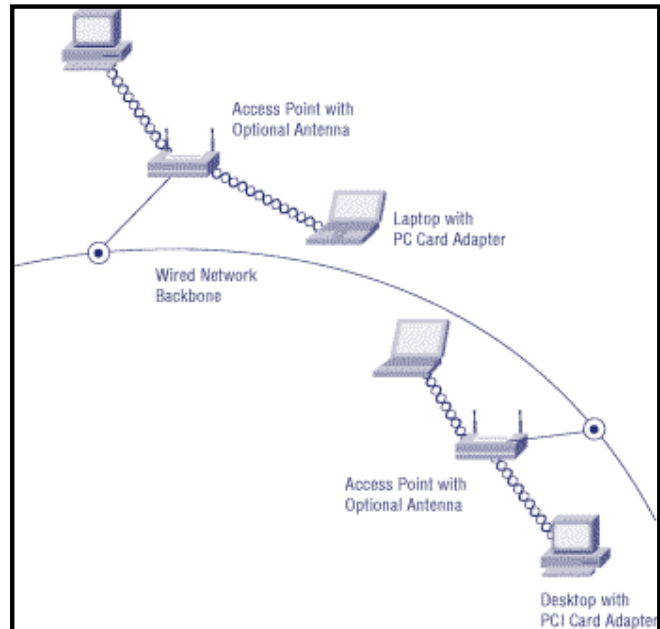
Il mercato del wireless è ampio: si va dalle applicazioni in ambito ospedaliero al mondo dell'alta finanza, dai magazzini alle aree aeroportuali, dalle vecchie strutture scolastiche in cemento armato agli antichi palazzi dei centri storici adibiti a uffici, fino all'utilizzo domestico, dove la tecnologia wireless permette una gestione centralizzata dell'abitazione, senza per questo dover effettuare costosi cablaggi. Pensate ad esempio ad un deposito di grandi dimensioni, dove si deve controllare il livello delle scorte ed effettuare eventuali rettifiche nel database aziendale. Se le operazioni vengono svolte utilizzando un'applicazione con un terminale portatile senza fili, le informazioni risultano accessibili a tutti i dipendenti e sono sempre aggiornate.

Grazie alla tecnologia wireless si possono stabilire sia collegamenti interni all'edificio (in-building), tramite access point o diretti tra PC (peer-to-peer), sia collegamenti esterni all'edificio (building-to-building), tramite bridge. Le WLAN permettono anche di stabilire linee di comunicazione temporanee o permanenti con fornitori per la gestione del magazzino: la sicurezza di un collegamento wireless è tale che il trasferimento di dati di magazzino fra un vendor e un cliente avviene in tempo quasi reale.

Le wireless LAN utilizzano un sistema a microcelle, simile al sistema cellulare telefonico. Ogni microcella ha dimensione limitata e un preciso raggio d'azione, ed è controllata da un Access Point (AP), la cui funzione principale è quella di coordinare le comunicazioni tra le varie stazioni wireless. Gli AP, a loro volta, sono collegati ad una dorsale (backbone), di solito un segmento della LAN aziendale.

A livello fisico si opera su una banda di frequenza che va da 2,4 GHz a 2,483 GHz, utilizzando modalità di trasmissione basate sulla tecnologia Spread Spectrum (a banda larga). A livello di configurazione, una WLAN (Wireless Local Area Network) offre tutti i vantaggi di una LAN tradizionale, come Ethernet e Token Ring, senza i limiti tecnologici di una rete wired.

Struttura di rete



2.4 I dispositivi di rete

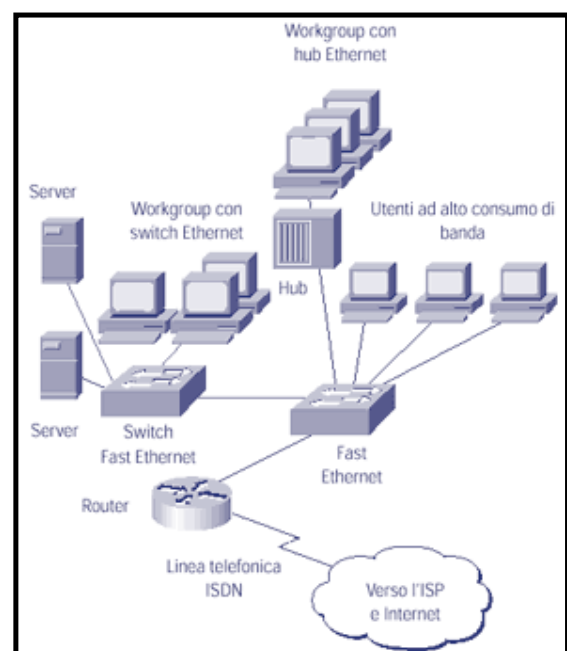
Oltre agli elementi base necessari per creare una rete esistono anche altri dispositivi aggiuntivi che possono facilitare, migliorare e proteggere l'intero sistema di networking.

Hub

Gli hub, o ripetitori, sono semplici apparecchiature che collegano fra loro gruppi di utenti. Ogni pacchetto di dati proveniente da un qualsiasi PC viene ricevuto dall'hub su una porta e trasmesso a tutte le altre. Tutti i PC possono essere collegati a un hub o a una serie ("stack") di hub che si trovano nello stesso "segmento" e che condividono la stessa larghezza di banda. Se il numero di utenti su un segmento aumenta, essi si devono dividere la larghezza di banda assegnata a quel determinato segmento.

Switch

Gli switch sono più intelligenti degli hub e offrono una



larghezza di banda dedicata più grande. Uno switch invia i pacchetti di dati alle porte specifiche dei destinatari, sulla base delle informazioni contenute nell'header di ogni pacchetto. Per isolare la trasmissione dalle altre porte, lo switch stabilisce una connessione temporanea tra la sorgente e il punto di destinazione, chiudendola al termine del collegamento.

Router

Ancora più intelligenti di hub e switch, i router utilizzano un "indirizzo" di pacchetto più completo per determinare il router o il PC che deve ricevere il pacchetto. Basandosi su una mappa di rete denominata "tabella di routing", i router possono fare in modo che i pacchetti raggiungano le loro destinazioni attraverso i percorsi più idonei. Se cade la connessione tra due router, per non bloccare il traffico, il router sorgente può creare un percorso alternativo. I router definiscono anche i collegamenti tra reti che utilizzano linguaggi diversi o, in termini tecnici, "**protocolli**" diversi. Tra i protocolli utilizzati vi sono IP (Internet Protocol), IPX (Internet Packet Exchange) e AppleTalk. Infine, gestiscono anche i trasferimenti "mobili", come lo spostamento continuo di un PC portatile.

2.5 Le tipologie di reti

Approfondimenti tecnici - Struttura di rete

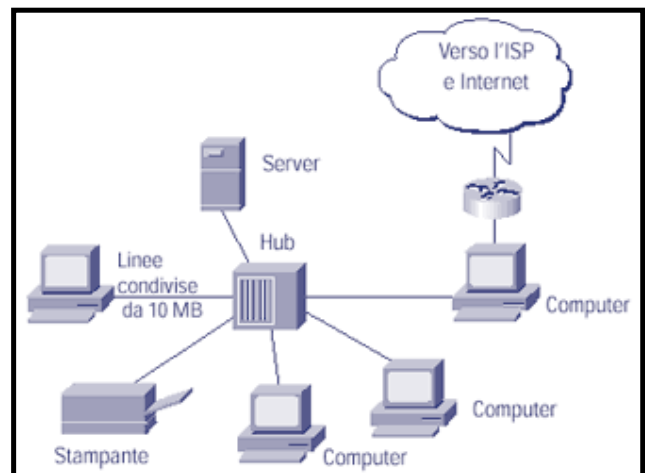
Le topologie di rete

Il termine topologia indica il modo in cui sono collegati i vari PC in rete. I PC identificano i nodi che compongono la rete. In genere i nodi di una rete non sono direttamente connessi l'uno all'altro (topologia "a maglia") poiché costerebbe troppo farlo, sono invece utilizzati dei nodi di connessione (hub o switch) che hanno la capacità di instradare messaggi, creare collegamenti logici ed eliminare così la necessità di connessioni fisiche dirette.

L'impiego di questi nodi di commutazione non è generalmente adottato nelle piccole reti locali, in quanto non strettamente necessari.

Le topologie più comuni per le LAN sono: a

bus, ad **albero**, a **stella** e ad **anello**.



Topologia a bus

Nella topologia a bus tutti i PC sono connessi tra loro in modo lineare, per così dire in sequenza "a catena". Le estremità di un bus non sono collegate tra loro, ma devono sempre essere terminate, altrimenti i segnali che raggiungono la fine del cavo possono fare un eco indietro, disturbando la trasmissione.

Nelle reti con topologia a bus, come in quelle con topologia ad anello, viene di solito utilizzata la trasmissione a "commutazione di pacchetto". Una stazione che vuole trasmettere delle informazioni divide il suo messaggio in tanti piccoli pacchetti e li invia uno alla volta. La topologia a bus è usata spesso con la cablatura in cavo coassiale. Un grosso limite è



dato dal fatto che un'interruzione del cavo interrompe la trasmissione in ogni direzione. Poiché tutti i computer connessi tramite topologia a bus condividono lo stesso mezzo trasmissivo, essi utilizzano dei protocolli che garantiscono che in ogni istante una sola stazione stia trasmettendo. Questi protocolli sono denominati protocolli d'accesso al mezzo MAC (Medium Access Control, protocol). La **topologia ad albero** è una generalizzazione della topologia a bus, infatti una rete ad albero viene realizzata collegando insieme più reti a bus.

Topologia a stella

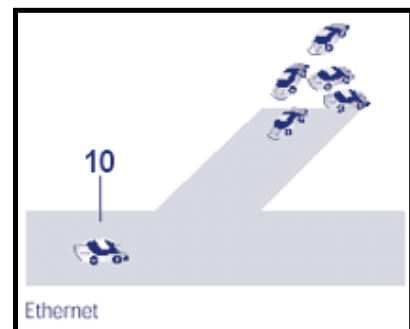
La topologia a stella è oggi la topologia più utilizzata. In essa tutti i computer sono connessi ad un nodo centrale che può essere un semplice ripetitore (hub) o anche un dispositivo intelligente (switch o router). Nelle reti con topologia a stella i pacchetti che vengono inviati da un PC ad un altro sono ripetuti su tutte le porte dell'hub. Questo permette a tutti i PC di vedere qualsiasi pacchetto inviato sulla rete, ma solo il PC a cui il pacchetto è indirizzato lo copierà sul proprio hard disk. Uno dei vantaggi è dato dal fatto che se vi è un'interruzione su una delle connessioni della rete solo il computer attaccato a quel segmento ne risentirà, mentre tutti gli altri PC continueranno ad operare normalmente. Uno svantaggio è il costo aggiuntivo imposto dall'acquisto di uno o più hub. Di solito, però, questa spesa è compensata dalla più facile installazione e dal costo più economico del cablaggio in twisted pair rispetto al cavo coassiale.

Topologia ad anello

Una topologia ad anello è in pratica una topologia a bus dove le due estremità sono unite tra loro a formare un anello. In questa topologia le informazioni viaggiano in una sola direzione. I dati, organizzati in pacchetti ognuno dei quali contiene l'indirizzo di destinazione, girano all'interno di questo anello fino a raggiungere il PC di destinazione. La topologia ad anello può essere utilizzata con la cablatura in twisted pair, in cavo coassiale o in fibra ottica. Il protocollo più importante attualmente utilizzato su reti locali con topologia ad anello è il protocollo Token Ring.

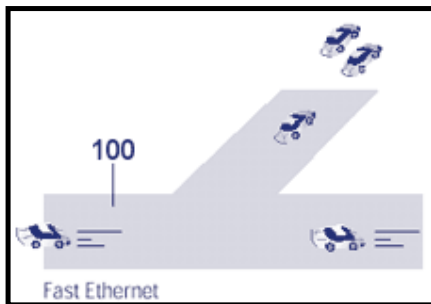
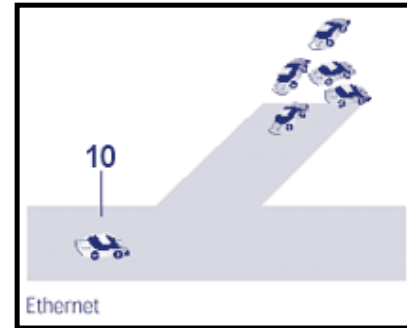
3 Tecnologie di trasmissione

Le tecnologie di trasmissione più utilizzate nelle reti locali (LAN) sono le tecnologie Ethernet, Fast Ethernet e Gigabit Ethernet. Per gli accessi remoti alle reti geografiche (WAN) vengono invece impiegate sia linee analogiche che digitali, ad esempio linee di tipo ISDN o DSL, mentre le VPN (Virtual Private Network), ossia le reti private virtuali, garantiscono connessioni sicure ed affidabili a basso costo.



3.1 Lan ethernet

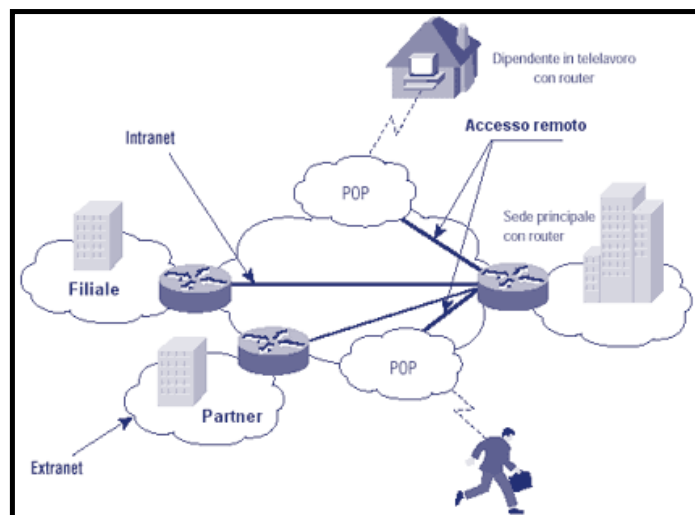
La tecnologia Ethernet è apparsa nel 1970 e da allora è quella più utilizzata per le reti locali (LAN). Ethernet si basa sullo standard CSMA/CD (Carrier Sense Multiple Access with Collision Detection). In pratica, una Ethernet può inviare i pacchetti di dati solo quando nessun altro pacchetto sta viaggiando sulla rete. In caso contrario, aspetta a trasmettere.



Se le stazioni multiple percepiscono un'apertura e iniziano ad inviare i dati nello stesso momento, può verificarsi una "collisione". Ogni stazione, allora, attende per un certo periodo e poi prova a inviare nuovamente il pacchetto di dati. Se gli utenti della rete aumentano, cresce rapidamente anche il numero di collisioni. La larghezza di banda (broadband) o la capacità di trasmissione dei dati (throughput) di Ethernet è di 10 Mbps. Fast Ethernet opera nello stesso modo (con l'identificazione delle collisioni) ma ad una velocità di 100 Mbps. Oggi esiste anche la tecnologia Gigabit Ethernet che trasmette a 1000 Mbps.

3.2 Accesso remoto e wan

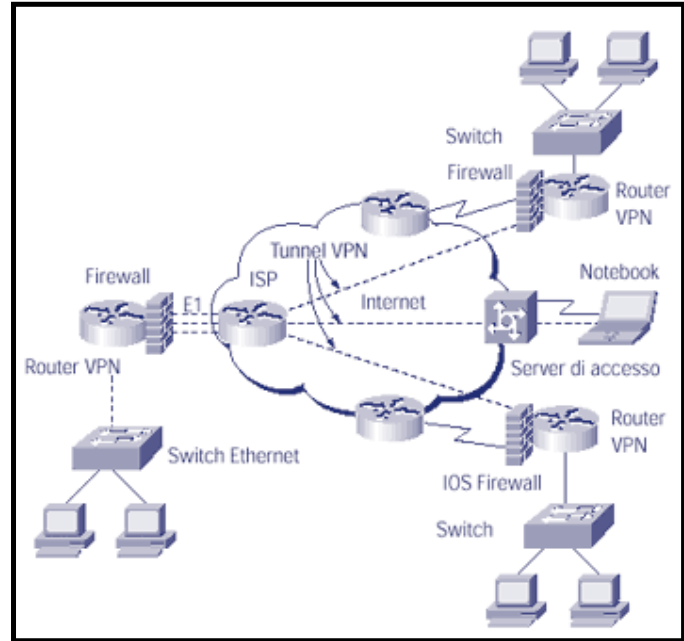
Le LAN collegano gli utenti locali all'interno di un edificio o in edifici adiacenti (i cosiddetti "campus"), le WAN, invece, collegano gli utenti e le LAN situati in qualsiasi parte del mondo. Per "accesso remoto" s'intende un semplice collegamento, generalmente attivato mediante linee telefoniche, tra un singolo utente e la rete centrale. Un'azienda può connettersi a Internet mediante vari tipi di collegamenti remoti. L'utente singolo può chiamare l'Internet Service Provider (ISP) attraverso un modem o un router, che a sua volta collega l'utente a Internet. In generale, le velocità delle LAN sono decisamente superiori a quelle delle WAN



e degli accessi remoti. Per esempio, una connessione singola Ethernet viaggia a 10 Mbps (milioni di bit al secondo). I modem analogici più veloci, attualmente disponibili, riescono a raggiungere 56 Kbps (migliaia di bit al secondo), quindi meno del 10 percento della velocità di una rete Ethernet. Anche le reti WAN, come le linee T1, non reggono il confronto (con una larghezza di banda di 1,5 Mbps, una T1 ha solo il 15 % della capacità di una singola connessione Ethernet).

3.3 VPN: l'alternativa alla wan privata

Con l'evolversi dell'attività, per condividere via Internet le informazioni e le risorse, le aziende devono collegare alla propria rete centrale un numero sempre maggiore di uffici e utenti remoti. In passato ciò era possibile mediante la creazione di una WAN privata, che utilizzava linee dedicate verso gli uffici connessi e server dial-access per il supporto degli utenti residenti e di quelli in telelavoro. Per un'azienda di medie e piccole dimensioni, una WAN privata tradizionale può essere molto costosa da creare e gestire. Per la connessione di siti e utenti remoti alla rete principale dell'azienda oggi è disponibile un'alternativa, la rete privata virtuale (VPN - Virtual Private Network). La VPN opera in assoluta sicurezza e permette l'accesso completo ai dati di una WAN privata sfruttando tutte le caratteristiche di Internet.



I vantaggi della VPN

✚ Maggiore convenienza

Gli utenti remoti possono collegarsi alle risorse di rete centralizzate attraverso un link locale verso un ISP, al prezzo di una chiamata locale.

✚ Maggiore flessibilità

I nuovi utenti vengono aggiunti con facilità senza nuove apparecchiature o linee dedicate. Le VPN semplificano anche la creazione di una extranet, che offre l'accesso a clienti o fornitori, protetti da password, a una parte della rete private (per esempio, per ordinare prodotti, verificare lo stato delle forniture, inviare fatture).

✚ Maggiore affidabilità

Le VPN sfruttano i mezzi delle vaste infrastrutture della rete pubblica e l'esperienza delle aziende che le controllano.

✚ Maggiore sicurezza

Le VPN utilizzano il "tunneling" e i sistemi di cifratura per proteggere il traffico privato. Il tunneling crea una connessione peer-to-peer temporanea tra l'utente remoto e quello centrale, bloccando l'accesso a chiunque si trovi all'esterno.

✚ Cosa serve per creare una VPN

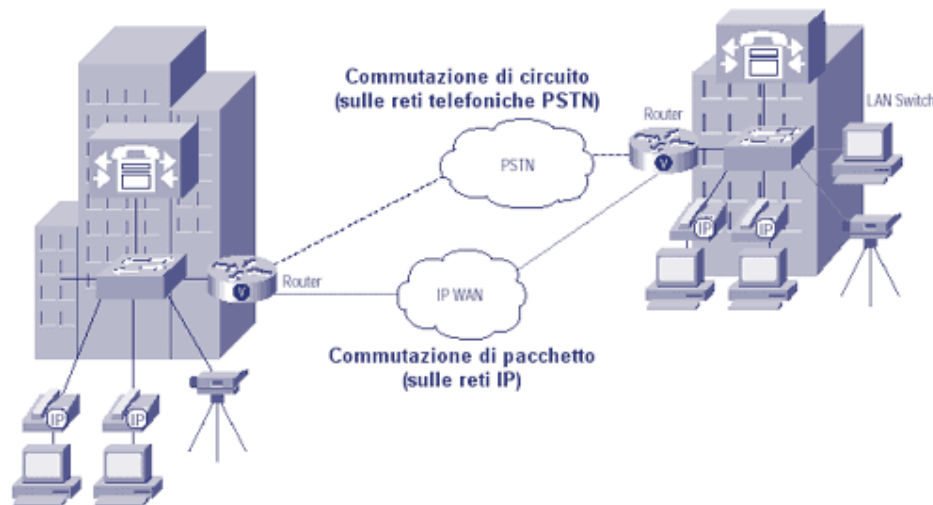
Una azienda di medie e piccole dimensioni può creare e gestire una propria VPN, ma è sicuramente più semplice affidarsi a un Internet Service Provider. In tal caso ci si deve semplicemente collegare al provider utilizzando un **router** o un **modem**. Le VPN esistenti sono generalmente di due tipi: dial e dedicate. Le prime permettono di sfruttare i bassi costi dei servizi dial-up normali mentre le altre possono utilizzare i servizi frame relay o le linee dedicate, soprattutto quando è necessario un collegamento remoto ad alta velocità e capacità.

3.4 linee analogiche

La soluzione più comune per collegarsi ad altre reti o a Internet, o per permettere agli utenti remoti di collegarsi alla propria rete centrale, è la linea analogica. La maggior parte delle linee telefoniche tradizionali è infatti di questo tipo. Basta quindi collegare un modem al computer e alla presa del telefono per essere in linea. La connessione costa come una telefonata normale, in base alla durata effettiva della comunicazione, espressa in secondi, più un importo iniziale. Le tariffe sono diversificate anche per fascia oraria e distanza.

Attualmente, i modem analogici più veloci per il trasferimento di dati operano a 56 Kbps. Anche se i modem rappresentano una soluzione semplice per le connessioni dial-up ad altre LAN e a Internet, essi non sono in grado di supportare una rete in continua espansione. Ogni modem può infatti supportare solo una "conversazione" remota alla volta e ogni apparecchiatura che vuole collegarsi con l'esterno deve disporre di un proprio modem.

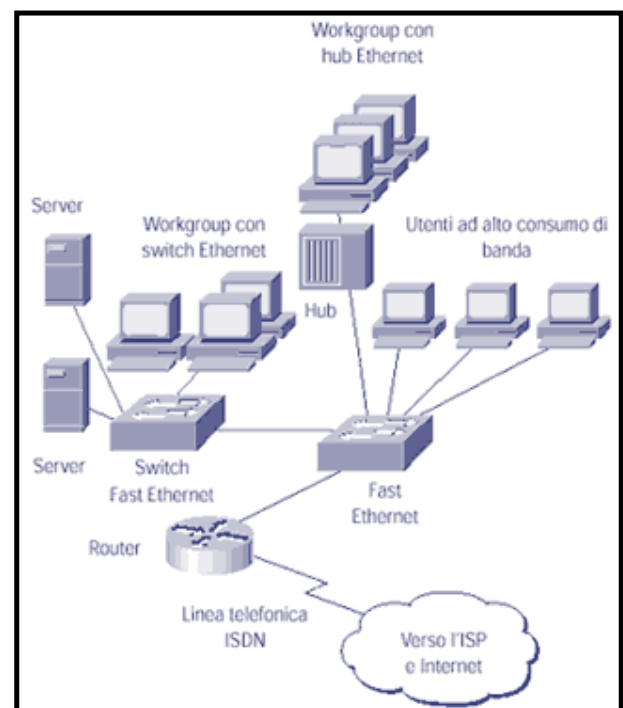
Una soluzione di compromesso tra il metodo dial-up e il routing vero e proprio è rappresentata dal routing "dial-on-demand". In questo caso il router stabilisce una connessione solo quando è necessario. La soluzione ideale sarebbe utilizzare un router collegato ad un modem o a una linea ISDN, che effettua la chiamata quando il router la richiede.



3.5 Linee ISDN

La linea telefonica ISDN opera a 128 Kbps e viene fornita dalle compagnie telefoniche pubbliche. L'ISDN comprende due canali da 64 Kbps che operano separatamente più un canale (chiamato D-Channel, a 16 Kbps) di servizio per i segnali di controllo. Talvolta se si dispone di un hardware compatibile è possibile effettuare il "bonding" (unione) dei due canali in un unico canale da 128 Kbps. Inoltre, essendo un servizio digitale, l'ISDN non presenta la cosiddetta "interferenza di linea", che rallenta le connessioni analogiche, e garantisce prestazioni molto elevate.

I collegamenti ISDN possono essere effettuati mediante un router predisposto per ISDN o un

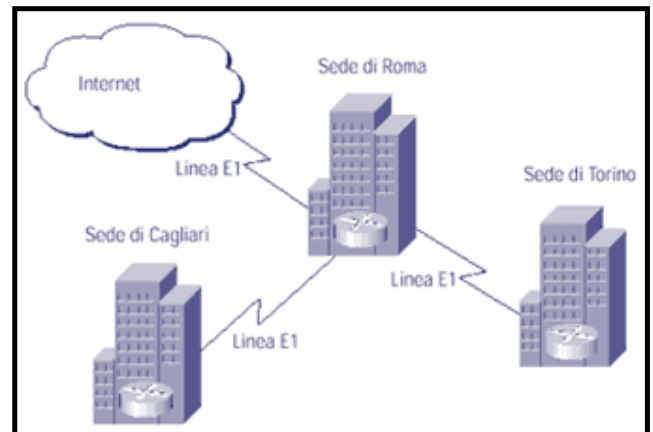


modem ISDN e una porta seriale sul router. I router, i modem o gli adattatori terminali ISDN possono avere porte analogiche che permettono di collegare telefoni, fax, modem o altri telefoni analogici. Per esempio, un router ISDN con presa telefonica analogica ci permette di effettuare telefonate e inviare fax e di collegarci contemporaneamente a un altro canale ISDN.

3.6 Linee dedicate

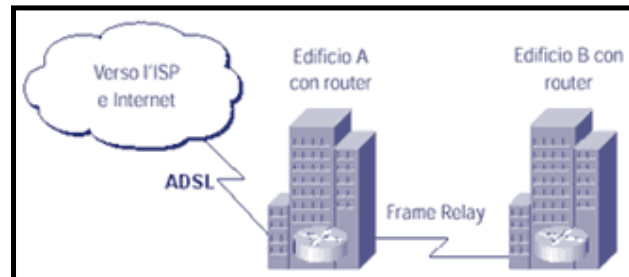
Le compagnie telefoniche offrono numerosi servizi con linee dedicate che non sono altro che percorsi di comunicazione peer-to-peer digitali, "aperti" 24 ore al giorno, sette giorni su sette. Invece di pagare un costo per ogni connessione, si paga una cifra fissa mensile senza limiti d'uso. Le linee dedicate migliori per le medie e piccole aziende hanno velocità variabili da 56 Kbps a 45 Mbps (un servizio T3). Considerando che le linee affittate operano tutte allo stesso modo, una scelta in tal senso dovrebbe quindi dipendere dal numero di utenti e dal volume di traffico della rete (e dalla larghezza di banda disponibile). Le aziende con un uso intensivo della WAN, generalmente, scelgono una linea E1 con larghezza di banda di 1,5 Mbps.

Per "peer-to-peer" significa che la linea dedicata utilizza una connessione fisica diretta tra l'azienda o la filiale e la centrale di commutazione della compagnia telefonica e gli altri uffici dell'azienda. Spesso, l'azienda che fornisce il servizio dati o telefonico deve installare un cablaggio nuovo.



3.7 Linee DSL

La tecnologia DSL (Digital Subscriber Line) è un servizio ad alta velocità che, come l'ISDN, opera attraverso il tradizionale doppino telefonico. La DSL è spesso più costosa dell'ISDN, utilizza modem speciali ed apparecchiature dedicate, ma garantisce una trasmissione dei dati più rapida rispetto ai modem analogici o al servizio ISDN. La DSL inoltre riserva un canale separato al servizio vocale, le chiamate telefoniche non vengono influenzate dalla trasmissione dei dati. Esistono vari tipi di DSL. L'ADSL, ad esempio, utilizza velocità di trasferimento dei dati asimmetriche (per esempio, i dati si muovono più rapidamente verso il PC che non verso Internet) mentre le altre tecnologie DSL trasferiscono i dati in modo simmetrico (stessa velocità da e verso il PC).



4 Sistemi di sicurezza

La sicurezza è la principale preoccupazione di chi utilizza una rete, sia essa una rete Internet, Intranet od Extranet. Un numero sempre più alto di utenti utilizza servizi Internet come la posta elettronica (E-mail), il File Transfer Protocol (FTP), i Newsgroup, ecc.

In più, molte aziende hanno un proprio sito web (website) a cui tutti possono accedere. Un'organizzazione ha bisogno di una politica di sicurezza adeguata per impedire agli utenti non autorizzati di accedere a risorse private. Ma qual è la strategia migliore da seguire?

Innanzitutto bisogna conoscere alla perfezione le infrastrutture hardware e software che si vogliono proteggere, oltre ai potenziali pericoli a cui esse possono essere sottoposte (accessi non autorizzati, sottrazione di informazioni riservate). Poi bisogna creare una lista di utenti che potenzialmente potrebbero avere bisogno di accedere a tali

risorse, tra cui gli "utenti remoti", persone che lavorano in luoghi lontani o che viaggiano spesso.

Infine si definiscono le policy di sicurezza dell'azienda, si stabilisce cioè quale tipo di uso è accettato o non accettato e quale è soggetto a restrizioni e una volta identificati gli accessi alle risorse, si determina quale tipo di dati può essere immagazzinato in uno specifico sistema.

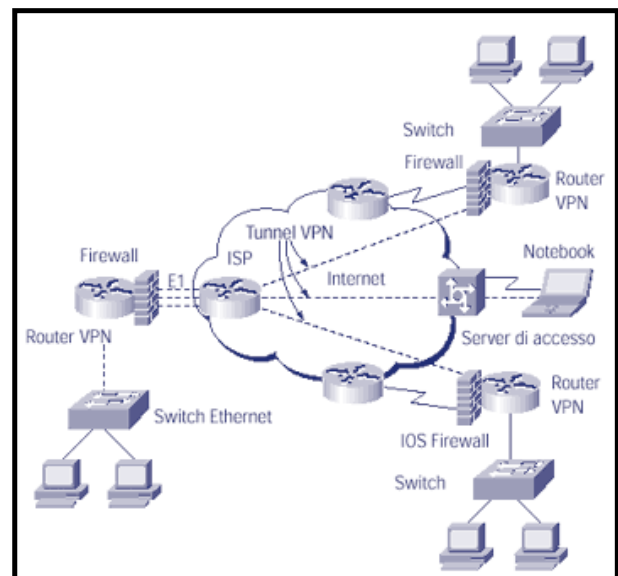
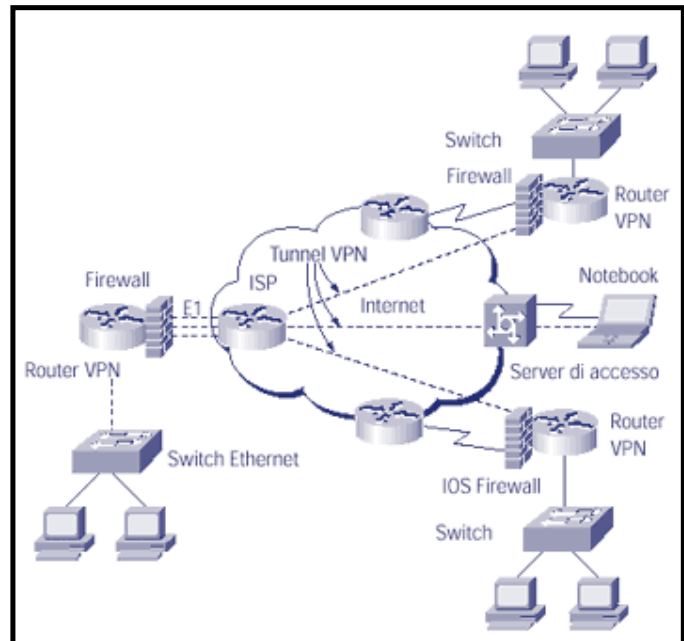
Molti tentativi di violazione di una rete vengono fatti con l'intento di sottrarre informazioni riservate. Accedere ai file di un'azienda non è semplice, ma se si riesce nell'impresa il danno che ne deriva è enorme, soprattutto per quelle aziende che producono beni e servizi che richiedono tempi di ricerca e sviluppo molto lunghi. Non va sottovalutata neppure la "vendetta" di un ex dipendente, deluso nelle sue aspettative. Il **firewall** è sicuramente un ottimo sistema di protezione, ma nei confronti di virus e applicazioni conosciute col nome di "cavalli di Troia" i firewall spesso hanno la peggio. Ad ogni modo, tutte le volte che la sicurezza verrà violata, questa dovrà essere necessariamente modificata, poiché è ovvio che se vi è stata una infrazione, a questa ne seguiranno altre.

4.1 Il firewall

Il firewall è in grado di controllare l'accesso alle reti intercettando tutti i messaggi in entrata e in uscita.

Il firewall, a seconda della configurazione e della tipologia, permette infatti il passaggio solamente di determinati tipi di dati, da determinati PC e da determinati utenti. Il firewall separa e protegge la rete interna, definendo e rafforzando le policy di rete.

I computer esterni alla rete devono attenersi a una specifica procedura per ottenere l'accesso alle risorse, agli host e a tutte le altre informazioni. Se l'accesso viene autorizzato l'utente può passare, a



patto che si attenga alla procedura definita dal firewall.

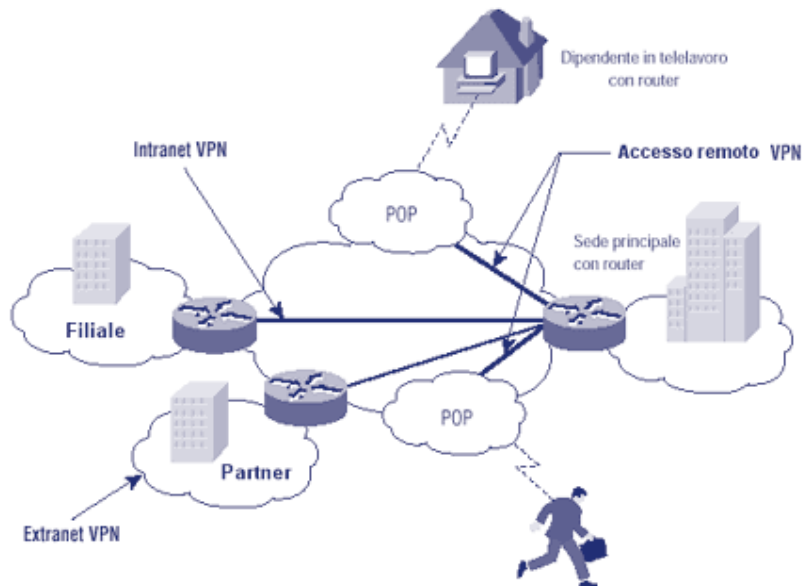
Di solito sono configurati per proteggere la rete contro i login non autenticati dall'esterno.

I firewall sono importanti anche perché possono provvedere alla sicurezza di singoli segmenti di rete laddove il controllo si renda assolutamente necessario. Può capitare che un'azienda, per esempio, desideri che le informazioni di tipo amministrativo (gestione paghe e contributi) vengano isolate dalla rete a cui accedono i dipendenti, oppure un'università potrebbe volere separare la rete degli studenti da quella dove sono memorizzate le loro votazioni. Sia che gestisca il traffico tra segmenti diversi della rete, sia che lo gestisca tra due reti differenti, un firewall deve trovarsi comunque in un ambiente operativo sicuro.

4.2 VPN ed Extranet

Molti firewall attualmente in commercio offrono anche funzionalità come, ad esempio, la gestione della posta elettronica e il supporto di **VPN (Virtual Private Network)** per lo scambio di informazioni cifrate.

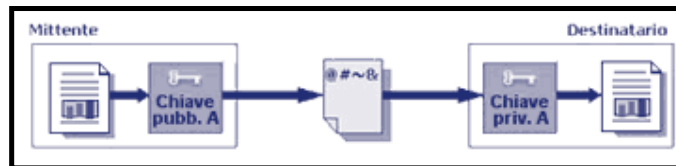
Per prevenire attacchi dai server di posta, una delle soluzioni potrebbe essere quella di predisporre un gateway sulla rete privata. La posta in partenza viene inviata al gateway, che a sua volta individua quella destinata a Internet e la trasmette al programma di gestione delle e-mail che si trova sul firewall. La posta in arrivo da Internet, prima di arrivare al gateway, passa attraverso il firewall. La presenza di un firewall che gestisce le operazioni di controllo della posta in entrata e in uscita da una rete privata offre il vantaggio di poter reagire, nel caso si verificassero tentativi di accessi indesiderati, oltre a controllare l'eventuale presenza di virus o programmi ritenuti pericolosi. Molte aziende hanno adottato solo recentemente nuove soluzioni che prevedono una rete Extranet e una VPN oltre alla Intranet aziendale. Nel caso di una **Extranet**, i firewall devono essere modificati per consentire agli utenti un accesso a determinate informazioni, mantenendone altre riservate e quindi non accessibili.



4.3 La crittografia

La crittografia, o cifratura (encryption), è una tecnica in continua evoluzione. Oggi viene utilizzata soprattutto per assicurare la riservatezza, l'autenticazione delle informazioni archiviate o inviate attraverso la rete.

La crittografia è anche la tecnica fondamentale per la generazione della firma digitale. Con la crittografia, un messaggio o, più in generale, un qualunque file di dati (testo, immagini, musica, ecc.) viene trasformato in un insieme di segni e simboli assolutamente privi di significato per chi non conosca la "**chiave**" giusta per decifrarli. Esistono sistemi a chiavi uniche e sistemi a "doppia chiave", una pubblica e una privata. Il problema principale comunque della crittografia è sempre stato la gestione della chiave. Anche il sistema di cifratura più sofisticato non serve a nulla se non si riesce a garantire la segretezza della chiave.



5 I protocolli di rete

Quando vogliamo trasmettere dei dati via Internet, la procedura di spedizione passa sempre attraverso i 7 livelli OSI che abbiamo appena visto. Tutti questi livelli sono governati da regole precise chiamate "**protocolli**" che gestiscono anche il rapporto con i livelli vicini. Ogni livello dunque rielabora il messaggio iniziale aggiungendo un header contenente informazioni per il livello successivo corrispondente del ricevente. Un messaggio può essere diviso in pacchetti sempre più piccoli, che vengono poi riassemblati dal destinatario.

Il modello standard di protocollo per il 1° livello e parte del 2° livello è il Protocollo **ETHERNET**, di cui fanno parte il **CSMA/CD** IEEE Standard 802.3 e il **Token Ring** Network IEEE Standard 802.5. Per il 3° livello è il protocollo **IP**, per il 4° livello sono i protocolli **TCP** e **UDP**. Per i livelli 5°, 6° e 7° i protocolli **FTP**, **SMTP**, **HTTP**, ecc.

5.1 Protocolli di 1° e 2° livello

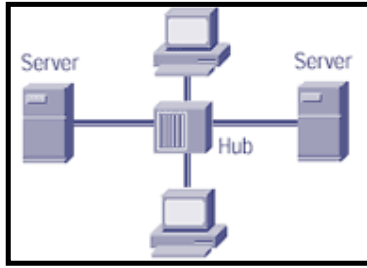
Ethernet: la topologia è quella a bus, su cavo coassiale con una velocità trasmissiva di 10 Mbps.

Fast Ethernet: la topologia è quella a bus, su cavo coassiale con una velocità trasmissiva di 100 Mbps.

Il protocollo più usato nelle reti con topologia a bus è il

CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Questo protocollo funziona nel seguente modo: quando una stazione vuole trasmettere "ascolta" il cavo. Se il mezzo è occupato la stazione aspetta finché non sarà libero, altrimenti trasmette immediatamente. Se due o più stazioni iniziano a trasmettere contemporaneamente avverrà una collisione che distruggerà i dati trasmessi. In tal caso tutte le stazioni che stavano trasmettendo smetteranno di farlo, e dopo un intervallo di tempo casuale cercheranno di trasmettere di nuovo. Quasi tutte le reti locali con topologia a bus utilizzano il protocollo Ethernet che si basa proprio sul CSMA/CD. Le reti Ethernet utilizzano sia il twisted pair schermato (STP), sia quello non schermato (UTP), il cavo coassiale e la fibra ottica.





Token Ring: la topologia è quella a stella (o con più hub collegati ad anello), su cavo coassiale intrecciato con una velocità di 14 Mbps. Così come Ethernet, anche il protocollo Token Ring fornisce servizi per i primi due livelli dell'OSI, cioè il livello Fisico e il livello Collegamento Dati. I protocolli per i livelli 1 e 2 dell'OSI si distinguono in funzione del mezzo trasmissivo usato e del modo in cui il segnale è applicato al mezzo.

Nelle reti Token Ring il metodo d'accesso al mezzo si basa sul passaggio di un token. Un "token" è una specie di "gettone" che circola sull'anello quando questo è libero. Quando una stazione

vuole trasmettere un pacchetto deve aspettare il gettone e rimuoverlo dall'anello prima di trasmettere il proprio pacchetto. Quest'ultimo viaggerà in una sola direzione lungo l'anello, passando da un PC all'altro. Come nel caso di reti Ethernet, il pacchetto è di solito indirizzato ad una singola stazione, e quando passerà da quella stazione il pacchetto verrà copiato. Poi continuerà a viaggiare lungo l'anello finché non ritornerà alla stazione di partenza, che provvederà a rimuoverlo dalla rete e ad inviare il gettone alla stazione successiva che si trova sull'anello.

- ✚ **LLC:** il protocollo Logical Link Control (IEEE802.2), è utilizzato per qualsiasi infrastruttura e ha il compito di fornire al livello rete un'interfaccia comune indipendente dal tipo di sotto livello MAC esistente, e quindi indipendente dalla topologia di rete e dalla tecnica di accesso al mezzo.
- ✚ **FDDI:** la topologia è quella a doppio anello di circolazione, utilizza fibre ottiche multimodali e modulazione a led con una velocità di trasmissione pari a 100 Mbps.
- ✚ **ATM:** ha una topologia libera (maglia, stella, albero) che opera a velocità tra i 25 Mbps ai 2.5 Gbps ed utilizza un metodo di condivisione delle risorse trasmissive con definizione delle priorità di traffico, tale per cui è possibile garantire a priori una capacità trasmissiva ben definita alle varie utenze e fornire quindi un supporto valido e comune a voce, audio e dati.

5.2 Protocolli di 3° e 4° livello

PROTOCOLLI DI 3° livello

- ✚ **IP (Internet Protocol):** è il protocollo che gestisce lo scambio dei dati tra i computer host di Internet.

PROTOCOLLI DI 4° livello

- ✚ **TCP (Transmission Control Protocol):** è il protocollo che trasferisce i dati tra le applicazioni di Internet (e-mail, ftp, www, ...). Frammenta il flusso di dati in arrivo dal livello superiore in messaggi separati che vengono passati al livello Internet. In arrivo, i pacchetti vengono riassemblati in un flusso di output per il livello superiore.
- ✚ **UDP (User Datagram Protocol):** è un protocollo non connesso e non affidabile, i pacchetti possono arrivare in ordine diverso o non arrivare affatto. Nato agli albori del networking è un protocollo molto semplice che si limita ad aggiungere ai dati un header, ovvero una

ulteriore porzione di byte contenenti le informazioni relative alle porte di origine e di destinazione.

- ✚ **ICMP (Internet Control Message Protocol):** trasporta i messaggi di errore e di controllo della rete. NETBEUI (NETBios Extended User Interface): è talvolta utilizzato per riferirsi al protocollo che supporta i servizi NetBIOS e/o i componenti software usati per implementarlo. NetBEUI era il nome di uno dei componenti software sviluppati in principio da IBM e Microsoft per supportare i servizi NetBIOS dei primi PC.
- ✚ **X25:** è un protocollo che integra nella rete telefonica pubblica il trasferimento dei dati e opera su rete a "commutazione di circuito", è utilizzato soprattutto su WAN, reti pubbliche telefoniche e poste elettroniche europee.

5.3 *Protocolli di 5°, 6° e 7° livello*

- ✚ **Telnet:** è il protocollo che permette ad un utente di collegarsi in maniera interattiva ad una stazione remota; è un'applicazione client/server usata per interrogazioni di database o per usufruire di servizi specifici di alcuni server.
- ✚ **SMTP (Simple Mail Transfer Protocol):** è il protocollo che gestisce la posta elettronica.
- ✚ **FTP (File Transfer Protocol):** è il protocollo comunemente utilizzato per il trasferimento di file da e verso un computer connesso in rete.
- ✚ **HTTP (Hyper Text Transfer Protocol):** è il protocollo su cui si basa il WWW (World Wide Web). L'attività principale svolta da un server HTTP è quella di inviare file, siano essi documenti testuali, documenti in formato HTML, immagini, suoni, sulla base delle richieste pervenuti dai client degli utenti Internet tramite browser.
- ✚ **DNS (Domain Name System):** non è un vero e proprio protocollo Internet ma piuttosto un servizio offerto agli utenti per chiamare altri computer. Il DNS può richiamare un sistema tramite un nome mnemonico (ad esempio www.nasa.org), anziché un numero del tipo 192.168.2.1 o uno simile.