

eNet HowTo

versione 0.2

maggio 2005

a cura di

andrea guido sommaruga

viale tunisia, 25 - 20124 - milano

retro della copertina

inserito pensando alla gestione della stampa in fronte retro

Indice

1 Scopo del documento.....	2
2 Introduzione.....	2
3 Obiettivi.....	2
4 Altri documenti correlati.....	2
5 Cenni storici.....	3
6 Le reti di calcolatori.....	3
12 I Protocolli.....	6
13 Il protocollo TCP/IP.....	6
17 Interconnessioni tra reti.....	9
18 Modalità di connessione ad Internet o reti Remote.....	10
21 Connessioni Telefoniche.....	11
26 Connessione ad Internet mediante Modem.....	12
27 Connessione ad Internet mediante Router.....	13
28 Connessione ad Internet mediante Proxy Server.....	14
29 Sicurezza delle Reti.....	17
30 Firewall.....	17
32 IDS Intruder Detection System.....	20
33 Antivirus.....	21
34 Intranet.....	22
35 WEB server.....	22
36 FTP server.....	22
37 MAIL server.....	22
38 News server.....	23
39 Servizi basati su TCP/IP.....	24
40 HD virtuali su Internet.....	24
41 Gateway FAX via email.....	25
42 WebCam.....	26
43 Protezioni.....	27
44 Gruppo di continuità.....	27
45 Stabilizzatore di tensione.....	27
46 Protezione elettriche.....	27
47 Climatizzazione.....	28
48 Antincendio.....	28
49 Antifurto.....	28
50 Crediti, Ringraziamenti, Licenza.....	29
51 Crediti.....	29
52 Ringraziamenti.....	29
53 Licenza.....	29
54 Impaginazione di questo documento.....	30

1 Scopo del documento

Con questo documento ci proponiamo di illustrare la firma elettronica o firma digitale per consentire agli utenti di avvicinarsi a questa tecnologia con cui un domani dovremo interagire di frequente.

2 Introduzione

Questo documento nasce come una libera raccolta di idee e suggerimenti per la configurazione delle reti di calcolatori con particolare accento verso le piccole realtà e gli studi professionali.

Non è scritto pensando di sostituire i manuali di istruzione o i readme dei programmi relativi alla configurazione degli apparati di rete e relativi alla configurazione dei server. Questo manuale si pone l'obiettivo di spiegare “**cosa fare**” e non “**come fare**”. Per le istruzioni operative rimandiamo ai manuali forniti con i prodotti.

3 Obiettivi

L'obiettivo è fornire una guida per districarsi nel mondo delle reti e per capire quali servizi possono essere richiesti e quali sono veramente utili.

Le reti di calcolatori

La connessione ad internet

La protezione delle reti

4 Altri documenti correlati

Per approfondimenti in merito agli argomenti trattati in questo documento è possibile consultare anche gli altri documenti correlati:

- **eDocHowTo** note sui documenti in formato elettronico
- **eMailHowTo** note sulla firma digitale e sulla crittografia
- **Schede Software Libero** schede programmi

5 Cenni storici

6 Le reti di calcolatori

Una rete di calcolatori è definibile come un insieme di più calcolatori tra di loro interconnessi in qualche modo che riescono a scambiarsi informazioni mediante un insieme di protocolli in comune. A seconda dell'estensione delle rete possono prendere diversi nomi. Si parla quindi di:

- LAN, Local area network, rete locale
- MAN, Metropolitan area network, rete metropolitana
- WAN, Wide area network, rete geografica

Internet è un esempio di rete WAN. Nel caso delle reti locali, ovvero quelle reti composte da sole macchine site in uno stesso edificio e in vari edifici tra loro connessi, a seconda del tipo di cablaggio, si può parlare di:

- reti a stella
- reti a bus

Le reti locali sono in genere limitate alle macchine connesse all'interno di uno stesso edificio o al limite in edifici adiacenti. A seconda del protocollo usato si parla ad esempio di reti:

- ethernet
- token ring
- ATM
- ecc

I media trasmissivi, ovvero i cablaggi, possono essere di diversi tipi anche misti tra di loro.

- cavo coassiale Rg58
- cavo coassiale Rg59
- UTP-Classe 5
- UTP Classe 5a
- UTP-Classe 6
- Fibra ottica
- Wireless

Ovviamente i diversi tipi di cablaggio presentano caratteristiche diverse e quindi vanno scelti in base al campo di impiego. Il classico cavo coassiale Rg58 ad esempio presenta un costo relativamente basso, è di facile installazione, ha una buona immunità ai disturbi ed è particolarmente adatto per realizzare piccole reti locali cablate con topologia a bus

TABELLA 1 – CARATTERISTICHE DELLE SCHEDE ETHERNET

7 Cavo RG213

Il cavo coassiale RG213 è una vecchia tecnologia usata per le prime connessioni di rete. Offre una velocità fino a 10Mbit/sec con una distanza massima tra le macchine di 500mt.

Il limite di quel tipo di cavo era, oltre alla velocità, il tipo di connessione: si usavano dei connettori chiamati vampire tap, che perforavano letteralmente il cavo per prelevare il segnale. Il cavo si deteriorava facilmente.

8 Cavo RG58

Il cavo coassiale RG58 ha sostituito l'RG213. Anche questo tipo di cablaggio è andato in disuso. Offriva una velocità di 10Mbit/sec con una massima lunghezza tra le tratte inferiore a 200mt. Le singole macchine erano connesse mediante connettori a "T". La rete era molto fragile perché la rottura di un cavo fermava l'intera tratta.

9 Cavo UTP

Il cavo UTP (Unshielded Twisted Pair) è un cavo composto da 4 coppie non schermate. E' classificato in base alla sua categoria ed è oggi il sistema più diffuso per realizzare le reti locali.

Con il cavo UTP si realizzano reti a stella ovvero i singoli PC o apparati vengono connessi a degli HUB o degli SWITCH che possono essere a loro volta connessi ad altri HUB o SWITCH per realizzare reti locali anche molto estese.

Si deve considerare che i singoli cavi di connessione degli apparati agli HUB o SWITCH non devono superare la massima lunghezza ammissibile per i cavi che nel caso di rete ethernet via UTP si aggira a circa 150mt per le singole connessioni.

Attualmente le reti più diffuse sono a 100 Mb con cavo UTP di classe 5 anche se gli ultimi calcolatori iniziano ad essere dotati di schede di rete a 1Gb su rame. Per realizzare le reti ad 1Gb occorre comunque utilizzare i cavi UTP in classe 5e o classe 6.

Più si sale di velocità e più il cablaggio diventa critico. Un cablaggio mal realizzato può essere fonte di seri problemi a volte anche molto complessi da diagnosticare.

Con velocità dai 100Mb in su è essenziale avere la certificazione del cablaggio.

10 Rete in Fibra Ottica

Per quanto riguarda la fibra ottica oggi è usata prevalentemente per realizzare delle dorsali, ad esempio per collegare direttamente gli SWITCH ai diversi piano degli edifici o per collegare edifici adiacenti in un'unica LAN. Per la fibra sono ammesse distanze massime di un paio di km a seconda del tipo di fibra che si utilizza. La fibra consente di raggiungere velocità trasmissive dell'ordine del Gbit o superiori, presenta un'ottima insensibilità ai disturbi elettromagnetici e per contro ha un costo elevato ed un maggior

costo di posa in opera. La fibra è anche scarsamente usata per collegare direttamente i singoli calcolatori dato i maggiori costi delle apparecchiature. Un ottimo concorrente della fibre è il Gbit su rame con cui si raggiungono praticamente le stesse prestazioni in termini di velocità ma non di distanza tra gli apparati ad un costo più contenuto e soprattutto con un'installazione più semplice.

La fibra ottica ha il difetto di avere un costo elevato e di utilizzare dei cavi fragili.

11 Rete Wireless

Come ultima novità abbiamo le reti wireless ovvero le reti che si appoggiano all'etere come mezzo trasmissivo. In questo caso tutti gli apparati sono dotati di antenne o di dispositivi ad infrarossi e si connettono con delle stazioni base che consentono la connessione.

Queste reti presentano dei limiti tecnologici quindi non risultano particolarmente veloci ed affidabili. Sono idonee a realizzare delle reti caratterizzate da alta mobilità delle apparecchiature.

Sono particolarmente comode ad esempio per realizzare una rete di connessione tra calcolatori portatili in una sala corsi.

Si consiglia di impiegare le tecnologie wireless solo se veramente necessarie.

12 I Protocolli

I calcolatori connessi in rete sono in grado di comunicare mediante una serie di protocolli comuni. In questo modo è possibile fare parlare tra loro apparati diversi. Pensando ad Internet possiamo definirla una rete di reti composte da macchine IP interconnesse, ovvero collegate tra loro mediante il protocollo IP.

13 Il protocollo TCP/IP

In realtà definire il TCP/IP un protocollo non è molto corretto. Sarebbe meglio dire che è un insieme di protocolli che comprendono TCP, IP, UDP ed altri protocolli. Cerchiamo comunque di dare un'idea di che cosa è il TCP/IP.

La connessione tra apparati è possibile solo se si è in grado di implementare un meccanismo di indirizzamento per le informazioni da trasmettere. Ogni apparato deve quindi avere un suo indirizzo univoco che lo distingue dagli altri apparati connessi alla stessa rete. L'indirizzo prende il nome di indirizzo IP.

Vediamo di introdurre brevemente il meccanismo di funzionamento del TCP/IP. In realtà sono due distinti protocolli il TCP e l'IP.

Il protocollo IP (Internet Protocol) è il protocollo che consente la trasmissione di dati tra due calcolatori identificati univocamente mediante il loro indirizzo IP. La trasmissione dei dati mediante il protocollo IP segue uno schema semplicissimo, i dati da trasmettere sono suddivisi in pacchetti di una certa dimensione, ad ogni pacchetto è associato l'indirizzo del mittente e l'indirizzo del destinatario quindi il pacchetto viene regolarmente instradato dai router. Il protocollo IP non prevede alcun controllo sui dati trasmessi, non verifica che tutto ciò che si è trasmesso arrivi a destinazione e non verifica nemmeno che i pacchetti giungano a destinazione nell'ordine corretto con cui sono stati inviati. In realtà può capitare che un pacchetto trasmesso dopo arrivi prima di un altro a destinazione perché nella rete IP ha preso una strada più corta. Non è garantito che tutti i pacchetti prendano la stessa strada.

Il protocollo TCP lavora in coppia con l'IP, questo protocollo si preoccupa della correttezza delle trasmissioni, verifica che tutto ciò che è stato inviato sia arrivato effettivamente a destinazione ed eventualmente chiede la ritrasmissione dei dati andati persi. Verifica inoltre che la sequenza di ricezione sia la stessa della trasmissione, in caso contrario prevede un meccanismo per risistemare la corretta sequenza dell'informazione. Il TCP si basa sul protocollo IP per l'invio fisico dei dati.

14 L'indirizzo IP

Gli indirizzi IP sono dei numeri che identificano univocamente un certo dispositivo. A seconda dello standard a cui si riferiscono si parla di IPv4 o IPv6.

Questi indirizzi sono gestiti in modo centralizzato da un organismo delegato ad assegnare gli indirizzi la cui home page su internet è raggiungibile all'indirizzo: <http://www.iana.org/>

La struttura segue uno schema fortemente piramidale. IANA assegna lotti di indirizzi ad altre organizzazioni che si preoccupano della gestione del range di indirizzi a loro assegnato.

Le singole organizzazioni che necessitano di eventuali indirizzi IP statici verso internet devono richiederli ai loro Internet Service Provider che sono assegnatari di classi di indirizzi.

Non essendo ammissibili indirizzi duplicati si deve mantenere un rigido schema di assegnamento.

15 L'indirizzo IPv4

Gli indirizzi IP sono dei numeri nella forma xxx.xxx.xxx.xxx con xxx che varia da 0 a 255. Si tenga presente che ogni calcolatore collegato ad Internet deve assolutamente avere un suo indirizzo IP unico. Questo è essenziale per il funzionamento della rete, IP duplicati causano blocchi o malfunzionamenti nella rete.

Cercando di essere più precisi il singolo dispositivo viene configurato in realtà con un indirizzo IP ed una maschera di sotto rete. Un possibile esempio può quindi essere:

```
indirizzo IP           192.168.1.2
maschera sottorete:   255.255.255.0
```

La maschera di sottorete serve per suddividere in due parti l'indirizzo IP. Mediante un algoritmo matematico l'indirizzo è quindi suddiviso nelle sue due componenti:

```
indirizzo di rete      192.168.1
indirizzo dell'Host    .1
```

Per un'umano la cosa viene quindi interpretata come la macchina con indirizzo 1 sulla rete 192.168.1.

Che cosa vuole dire tutto questo? Cerchiamo di illustrarlo scrivendo gli indirizzi e la maschera di sottorete come li vedono i calcolatori, i calcolatori ragionano in BIT ed il nostro indirizzo è composto da 4Byte ovvero:

	Decimale	Binario
Indirizzo IP	192.168.001.002	11000000.10101000.00000001.00000010
Maschera	255.255.255.000	11111111.11111111.11111111.00000000
Indirizzo di rete	192.168.001	11000000.10101000.00000001
Indirizzo di macchina	002	00000010
Indirizzo di Broadcast	192.168.001.255	riservato
Indirizzo di Rete	192.168.001.000	riservato

In questo caso l'indirizzo IP assume un nuovo significato: la prima parte ovvero 192.168.001 è l'indirizzo delle rete e la seconda parte 002 è l'indirizzo del singolo PC o Host all'interno della rete.

A seconda del numero di byte riservati all'indirizzo di rete, le reti prendono il nome di reti di classe A, B o C. Per ogni tipologia di rete sono previsti degli intervalli di indirizzi riservati alle reti private ovvero indirizzi per macchine non connesse direttamente ad Internet.

Una rete di classe C ad esempio ha 256 possibili indirizzi a cui si devono togliere il primo e l'ultimo quindi una rete di classe C è in grado di indirizzare 254 Host.

da	a	n reti previste	maschera
000.000.000.000			
001.000.000.000	126.xxx.xxx.xxx	classe A	255.000.000.000
010.000.000.000	010.xxx.xxx.xxx	classe A private	255.000.000.000
127.000.000.000	127.xxx.xxx.xxx	rete loopbak	255.000.000.000
127.000.000.001		indirizzo localhost	
128.000.000.000	191.xx.xxx.xxx	classe B	255.255.000.000
172.016.000.000	172.31.xxx.xxx	classe B private	255.255.000.000
192.000.000.000	223.xxx.xxx.xxx	classe C	255.255.255.000
192.168.000.000	192.168.xxx.xxx	classe C private	255.255.255.000
224.000.000.000	239.xxx.xxx.xxx	classe D	
240.000.000.000	247.xxx.xxx.xxx	classe E	

Per la gestione delle reti private sono stati quindi riservati 3 gruppi di indirizzi

da	a	n reti previste	maschera
010.000.000.000	010.255.255.255	1 rete di classe A	255.000.000.000
172.016.000.000	172.031.255.255	31 reti di classe B	255.255.000.000
192.168.000.000	192.168.255.255	256 reti di classe C	255.255.255.000

Questi indirizzi sono disponibili per le reti private, se si deve realizzare una LAN con protocollo TCP/IP deve essere configurata utilizzando un range di indirizzi tra quelli riservati per le reti private. Gli indirizzi riservati alle reti private hanno la caratteristica di essere non instradabili ovvero non sono in grado di essere indirizzati dai router in Internet. Sono solo riservati alle LAN.

Un esempio di schema di indirizzamento per una rete locale in classe C composta da tre calcolatori, un server, una stampante di rete ed il router per internet può essere fatta secondo il seguente schema:

Indirizzo	Maschera	Calcolatore
192.168.001.001	255.255.255.0	Primo PC
192.168.001.002	255.255.255.0	Secondo PC
192.168.001.003	255.255.255.0	Terzo PC
192.168.001.100	255.255.255.0	Server
192.168.001.101	255.255.255.0	Stampante
192.168.001.254	255.255.255.0	Router

Tra questi indirizzi è evidenziato l'ultimo ovvero quello del Router perché deve essere utilizzato come indirizzo del gateway predefinito sui singoli dispositivi che devono accedere all'esterno della rete.

16 L'indirizzo IPv6

L'indirizzo IPv4 prima illustrato ha un limitato numero di reti e instradabile. Le nuove tecnologie telefoniche prevedono un'aumento esponenziale dei dispositivi IP. I futuri cellulari sono tutti destinati a diventare dei veri e propri dispositivi IP dotati quindi del loro indirizzo statico. Per potere realizzare questi nuovi servizi è necessario espandere il numero di indirizzi. E' quindi stato progettato il protocollo IPv6 che prevede uno spazio di indirizzamento superiore.

Il protocollo IPv6 è comunque stato progettato per potere coesistere con gli attuali dispositivi dotati di indirizzi IPv4.

17 Interconnessioni tra reti

Internet è stata più volte definita come la rete delle reti ovvero è una grossa rete composta dall'unione di tante piccole reti. L'elemento che consente di unire tra loro più reti è il “**router**”.

Il router funziona come ponte tra due reti e consente di instradare correttamente i pacchetti di dati. Il meccanismo di instradamento si basa sul meccanismo di mascheramento prima illustrato. Come all'interno di una rete locale non ci possono essere più dispositivi con lo stesso indirizzo IP così non ci possono essere due reti con lo stesso indirizzo di rete.

In realtà le cose sono poi leggermente diverse perchè, per quanto riguarda internet, gli indirizzi di rete privati illustrati in precedenza non sono routabili ovvero non si propagano dai router.

Le reti locali basate su indirizzi IP privati sono quindi mascherate dal mondo internet. Di quelle reti da internet sono solo visibili gli indirizzi IP pubblici assegnati alle interfacce esterne dei router. Le singole macchine delle reti interne non sono quindi raggiungibili dall'esterno.

Per configurare una rete tutta visibile dal mondo internet è necessario utilizzare degli indirizzi IP pubblici.

18 Modalità di connessione ad Internet o reti Remote

La connessione di un calcolatore ad Internet è semplicemente una connessione di un calcolatore o di una rete di calcolatori (LAN) ad un'altra rete di calcolatori. Questo è possibile grazie a due cose: un protocollo comune di trasmissione dati (TCP/IP) e dei dispositivi che connettono il calcolatore alla rete telefonica (Modem) o che connettono la LAN alla rete telefonica. A seconda del tipo di connessione telefonica si parla quindi di connessione PSTN o analogica, di connessione ISDN o digitale ed infine di connessione ADSL. In realtà ci sono anche dei sistemi ibridi di connessione ad Internet che impiegano ad esempio le tradizionali tecnologie tipo ISDN per inviare informazioni da un Calcolatore verso il Provider e per ricevere informazioni utilizzano un canale satellitare molto più veloce. Queste sono comunque ancora poco diffuse e destinate ad applicazioni decisamente di nicchia.

Oggi si iniziano anche ad avere le prime offerte di connessione ad Internet con reti dedicate in fibra Ottica. A Milano ad esempio il consorzio FastWeb MetroWeb offre connettività ad Internet con fibra ottica e banda da 10Mb/sec ad un costo tutto sommato più che ragionevole.

Per maggiori informazioni <http://www.fastweb.it>

19 Modem

Il modem è un oggetto che consente di connettere un calcolatore ad una linea telefonica. Il nome ha origine dall'acronimo MODulatore DEModulatore. Il model infatti consente di trasformare il segnale digitale generato dal calcolatore in un segnale analogico adatto ad essere trasferito su delle normali linee telefoniche analogiche, le vecchie linee del telefono.

Nel caso di linee telefoniche digitali, tipo ISDN, si parla di Modem ISDM ma è un termine improprio; si dovrebbe parlare di Terminal Adapter ISDN infatti in questo caso viene a mancare la funzione di conversione digitale/analogica perché le linee ISDN sono già digitali.

20 Router

Il Router è un dispositivo che consente di instradare dati tra due reti diverse. Ovviamente questa capacità del router ne fa uno strumento idoneo a connettere una rete locale ad Internet. Il router per sua natura è dotato di due interfacce di rete una verso la LAN ed un'interfaccia verso la WAN. Normalmente il router si limita ad intradare correttamente i pacchetti di dati tra le due reti.

In commercio esistono dei piccoli router utilizzati per la connessione di piccole LAN ad Internet mediante una linea telefonica. In questo caso si tratta di router in cui l'interfaccia verso la WAN è sostituita dal un Modem (analogico, ISDN o ADSL)

21 Connessioni Telefoniche

22 PSTN

Con la sigla PSTN si intende la normale connessione telefonica su linea commutata conosciuta come linea analogica. Per connettere un computer ad una linea PSTN è necessario il Modem.

Attualmente i modem analogici consentono velocità massime di connessione di 56 Kbps ovviamente se la qualità della linea telefonica lo permette.

La tariffazione di PSTN segue le normali regole della tariffazione telefonica a tempo oppure per gli operatori che lo prevedono, con le nuove tariffe FLAT in cui si paga un fisso mensile tutto compreso indipendentemente dal numero e dalla durata delle telefonate.

23 ISDN

È l'evoluzione della tradizionale linea telefonica PSTN solo che in questo caso si tratta di linee digitali. ISDN in realtà consente di avere due linee (o canali) indipendenti sullo stesso doppino telefonico. Con la linea ISDN è quindi possibile telefonare e contemporaneamente navigare su Internet. I due canali sono indipendenti. ISDN consente di trasmettere dati alla velocità di 64 Kbps garantiti quindi è leggermente più veloce rispetto alle tradizionali linee analogiche ed inoltre non risente di un degrado di prestazioni se la linea è disturbata: i 64 Kbps di banda di ISDN sono garantiti. Un accesso base ISDN consente di avere due canali indipendenti da 64 Kbps. È possibile sommare i due canali da 64 Kbps per ottenere un unico canale virtuale da 128 Kbps, ovviamente questa caratteristica deve essere supportata anche dal V.s. Provider. Sommando i due canali si raddoppia la velocità ma ovviamente si raddoppia anche il costo della connessione, è come fare due telefonate!

Come nel caso di PSTN anche le linee ISDN consentono connessioni solo per il tempo necessario ovvero connessioni DialUp.

La tariffazione di ISDN segue le normali regole della tariffazione telefonica a tempo oppure per gli operatori che lo prevedono, con le nuove tariffe FLAT in cui si paga un fisso mensile tutto compreso indipendentemente dal numero e dalla durata delle telefonate.

24 ADSL

ADSL è una tecnologia recente usata principalmente per connettersi ad Internet. ADSL si appoggia su una normale linea telefonica Analogica (non funziona con le linee digitali) e prevede l'utilizzo di un particolare Modem ADSL. In modo analogo ad ISDN con ADSL si ha a disposizione la tradizionale linea analogica da utilizzarsi normalmente per le chiamate in fonia o per l'invio dei FAX analogici (gruppo I e II) e si ha contemporaneamente a disposizione un canale per la trasmissione dati che consente velocità di 64Kbps in trasmissione e fino a 640Kbps in Ricezione.

Rispetto ad ISDN si può notare che risulta fino a 10 volte più veloce in ricezione mentre la trasmissione è pari a quella di ISDN, nel caso di ADSL le velocità non sono garantite quindi in caso di affollamento della rete possono calare anche sensibilmente. In realtà c'è anche un'altra differenza direi sostanziale rispetto ad ISDN: ISDN offre una connessione su richiesta (DialUp) mentre ADSL offre una connessione sempre attiva. Un computer connesso ad Internet mediante ADSL è quindi costantemente connesso alla rete ed avrà anche il suo IP statico.

Nel caso di ADSL i Provider prevedono solo un canone di accesso mensile, che si aggira intorno ai 70 Euro a seconda dei fornitori, indipendentemente dal tempo di connessione effettivo. In alcuni casi il fisso mensile prevede un massimo traffico in termini di Mb ricevuti/trasmessi superato i quali si deve corrispondere un tanto a Mb in base ai particolari contratti.

25 CDN

Le CDN sono delle linee dedicate usate per connettere reti di una certa dimensione. Sono linee digitali come ISDN ma possono fornire banda superiore. Il contratto per le CDN è un fisso annuo indipendentemente dal traffico e il costo varia in relazione alla banda che si richiede.

Attenzione contrariamente ad ADSL. PSTN ed ISDN le CDN non sono linee telefoniche: sono solo linee dati.

Per connettersi ad Internet mediante una CDN ovviamente bisogna utilizzare un Router.

26 Connessione ad Internet mediante Modem

Il sistema più classico, che probabilmente avrete utilizzato tutti almeno una volta, consiste nel connettere un singolo computer ad Internet mediante il Modem, la linea telefonica ed il protocollo di accesso remoto.

Come già detto il Modem è lo strumento che consente di connettere un computer alla linea telefonica. In base al tipo di linea telefonica disponibile si utilizza un modem Analogico, un Terminal Adapter ISDN oppure un modem ADSL.

A seconda del tipo di linea usato si possono avere due tipi di connessioni: DialUp per linee analogiche ed ISDN e connessioni permanenti per linee ADSL.

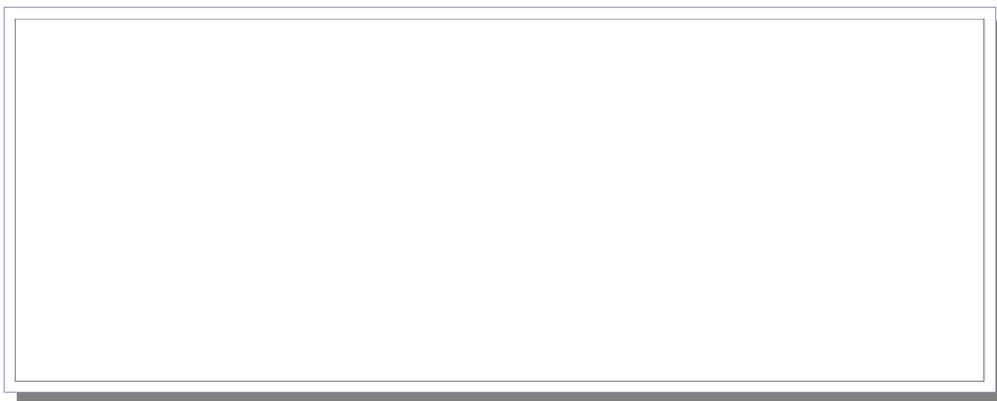
Nel caso delle connessioni DialUp, ovvero su chiamata, si tratta di connessioni temporanee, vengono stabilite componendo un numero telefonico quando si ha necessità di accesso ad Internet e vengono chiuse quando si termina il collegamento.

Nel periodo in cui un computer risulta connesso ad Internet mediante un Modem è a tutti gli effetti un computer visibile su Internet anche da parte di tutti gli altri utenti di Internet. Se il computer non è dotato di opportuni meccanismi di sicurezza ma semplicemente condivide il suo disco, un qualsiasi utente da Internet può leggere e/o cancellare i dati memorizzati sul computer.

La connessione ad Internet mediante Modem è quindi la più insicura che esista e quella che espone la macchina al maggior rischio. Chiaramente nel caso di una connessione in DialUp il rischio di intrusioni è limitato dalla durata della chiamata.

Nel caso di connessioni mediante Modem ADSL occorre tenere presente che la connessione è permanente ovvero se il calcolatore è acceso e non opportunamente protetto, questo sarà anche a disposizione di tutti i malintenzionati che giocano su Internet. Una macchina connessa direttamente con ADSL richiede sicuramente oltre all'antivirus aggiornato anche un minimo di firewall per prevenire accessi.

FIGURA 1 – ESEMPIO DI CONNESSIONE DI UN PC AD INTERNET MEDIANTE MODEM



Naturalmente questo non è l'unico modo per connettere la mia rete ad Internet. Sono poi possibili molte varianti per connettere la LAN ad Internet. Ad esempio se il PC che connesso mediante un modem ad Internet è un PC che fa anche da Proxy server, questo può consentire la connessione ad Internet anche da parte delle altre macchine eventualmente connesse in LAN con lui. In questo caso comunque iniziamo a scendere troppo nei dettagli.

27 Connessione ad Internet mediante Router

Il Router è un dispositivo che consente la connessione di una rete (LAN Local Area Network) di calcolatori ad un'altra rete (LAN o WAN o Internet).

Il Router può essere sia hardware che software. Nel caso di Router hardware ovviamente si parla di dispositivi che contengono al loro interno (come firmware) il software necessario a svolgere il compito del Router. Nel caso di Router software si tratta di programmi in esecuzione in background o come servizi, su calcolatori che svolgono altre funzioni oltre ovviamente le funzioni di Router.

Dire che il Router consente la connessione di una LAN ad INTERNET è limitativo nei confronti delle funzioni dei Router. I Router consentono l'interconnessione tra due reti, possono essere rappresentati come degli scambi che instradano i pacchetti in transito (dati) da una rete all'altra. Ovviamente se una rete è la nostra rete locale (LAN) e la seconda rete è l'accesso remoto mediante modem al server Internet del nostro Provider ottengo un ponte tra la LAN ed Internet: in questo caso uso il Router per connettere la LAN ad Internet.

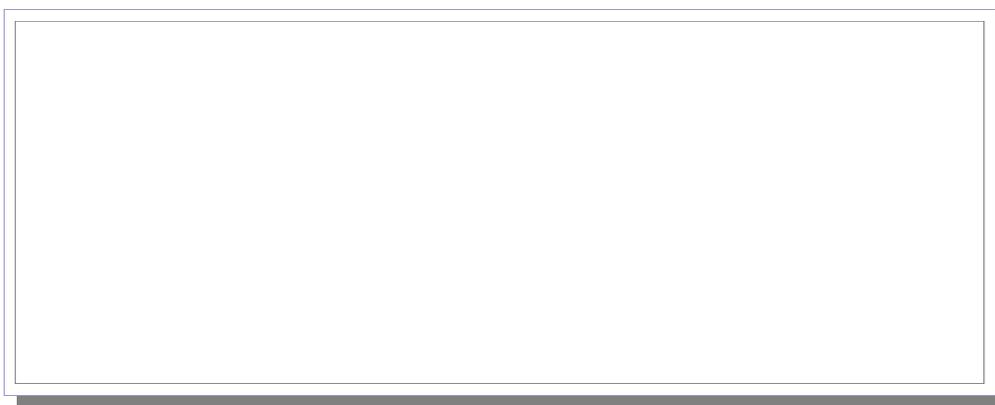
Nulla vieta ovviamente di utilizzare il Router come connessione tra due reti locali (LAN) della stessa società ma in sedi diverse per realizzare una rete geografica (WAN): in questo secondo caso utilizzo il Router per una connessione LAN to LAN.

Quasi tutti i Router in commercio nella fascia economica tra cui segnalo gli ottimi ZYXEL 100 HW analogici e ZYXEL 100 IH per le linee ISDN, consentono la connessione della LAN ad Internet come SUA (Single User Account) ovvero sfruttando un unico Account Utente.

Dal punto di vista del Provider vede il Router come un unico utente connesso. È compito del Router gestire il corretto instradamento dei vari pacchetti provenienti dai vari calcolatori connessi alla LAN con un algoritmo chiamato NAT (network address translation). In questo modo tutti gli utenti della LAN possono accedere ad Internet anche contemporaneamente sfruttando un unico Account ed ovviamente utilizzando la banda in modo condiviso.....quindi più lento all'aumentare degli utenti connessi. Nel caso di connessioni in DialUp si deve inoltre considerare che la chiamata telefonica è una sola, occupa quindi una sola linea del telefono ed ovviamente pago solo per una telefonata urbana anche se stanno usando Internet in contemporanea più utenti.

Chiaramente quando si utilizzano dei Router per condividere la connessione ad Internet sulla rete le procedure di configurazione del PC saranno leggermente diverse, non si utilizza la connessione di ACCESSO REMOTO ma si configura l'accesso via LAN

FIGURA 2 – ESEMPIO DI CONNESSIONE DI UNA LAN AD INTERNET MEDIANTE ROUTER



Questo metodo è ovviamente usabile solo per reti di piccole dimensioni o almeno a basso traffico altrimenti potrebbero esserci eccessivi rallentamenti. Con questo sistema se n utenti richiedono una determinata pagina Internet questa viene letta n volte....non vi è nessuna ottimizzazione di banda utilizzata ed oltre tutto non vi è nemmeno nessuna possibilità di controllo del traffico Internet.

28 Connessione ad Internet mediante Proxy Server

Al crescere delle dimensioni della LAN che si desidera connettere ad Internet si deve cercare di ottimizzare il traffico verso Internet, il collo di bottiglia è in genere la ridotta banda verso Internet. Questa banda è sempre scarsa e cara, si deve quindi utilizzarla al meglio evitando di ricaricare eventuali pagine già lette da altri utenti.

Allo scopo si utilizza un Proxy Server ovvero un server dedicato allo scopo oppure un programma che gira su di un server che ad esempio svolge anche la funzione di Mail server.

Il proxy Server è una specie di Cache, ovvero di memoria temporanea, di pagine WEB. È un vero e proprio server WEB che fa parte dell'eventuale Intranet, al quale vengono indirizzate tutte le richieste di pagine WEB e che a sua volta provvede a restituirne i relativi contenuti al programma che le ha richieste, tipicamente il browser degli utenti (Explorer, Netscape ecc.).

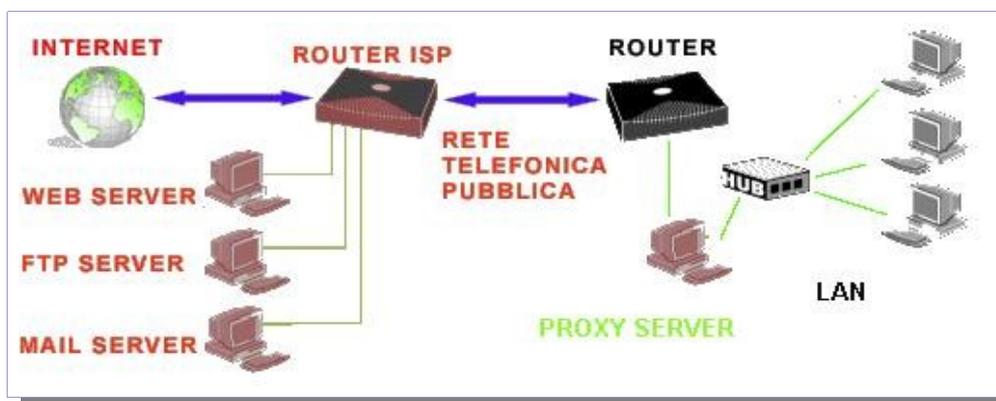
È un programma (o meglio una macchina perché generalmente è un calcolatore esclusivamente dedicato alla funzione di Proxy Server) che consente di migliorare la velocità di navigazione in Internet tentando di mantenere una copia locale dei files recenti e più consultati.

Il compito del Proxy Server è quello di mantenere una copia in locale (Cache) delle pagine richieste in modo di velocizzare la navigazione qualora la stessa pagina sia richiesta più volte vuoi dallo stesso utente che da utenti diversi. Per ogni richiesta di una pagina il Proxy Server prima controlla se è già disponibile nella propria Cache, se è disponibile si limita a richiedere al vero server Web che ospita la pagina se è ancora valida o se ha subito aggiornamenti. Se la pagina nella cache del proxy è ancora valida il relativo contenuto verrà restituito al browser dell'utente che l'ha richiesta, in caso contrario la pagina verrà scaricata da Internet prima nella cache del proxy quindi verrà restituita al browser dell'utente. Il beneficio in termini di velocità si ottiene perché si presume che il proxy server sia in grado di evadere le richieste di pagine in Cache più velocemente di quelle richieste direttamente da Internet per problemi di banda disponibile.

Ovviamente il principale requisito di un proxy server è un discreto spazio sul disco per mantenere la cache delle pagine scaricate. Più è grande la cache e maggiore è la possibilità che le pagine richieste si trovino già nella cache del proxy e che quindi l'utente riesca a consultarle con maggiore velocità.

Si tenga inoltre presente che l'uso del proxy server offre reali vantaggi solo se c'è probabilità di effettuare richieste ripetute delle stesse pagine: nel caso in cui vengano sempre e solo consultate delle pagine diverse l'utilizzo del proxy porterebbe ad un degrado delle prestazioni perché le pagine devono essere prima lette dal proxy quindi passate al browser dell'utente.

FIGURA 3 – ESEMPIO DI CONNESSIONE DI UNA LAN AD INTERNET MEDIANTE PROXY SERVER



Nelle opzioni di configurazione del proxy server è in genere consentito specificare un set di domini ai quali si deve accedere direttamente senza passare dal proxy. In genere per le pagine disponibili in Intranet non si passa dal proxy essendo un lavoro inutile quindi il dominio dell'Intranet viene sicuramente escluso.

Oltre ad ottimizzare l'utilizzo della banda di connessione ad Internet il Proxy consente in qualche modo di monitorare l'attività degli utenti ed in qualche caso limitarla.

I Proxy infatti possono mantenere dei Log delle pagine scaricate dai singoli utenti. Con opportuni programmi di analisi dei Log è quindi possibile effettuare delle statistiche sulle pagine più consultate e sui tempi di connessione ad Internet dei singoli utenti.

In genere i Proxy server consentono anche di aggiungere delle regole: ad esempio è possibile specificare una lista di siti che non possono essere consultati. I Proxy server possono anche essere utilizzati per autorizzare o meno determinati utenti all'accesso ad Internet. E' quindi possibile specificare delle liste di utenti (coppie Login/password) abilitati. Ovviamente in questo caso l'accesso al Proxy server richiede un'autenticazione da parte degli utenti.

29 Sicurezza delle Reti

Parlando di reti sia Locali che Geografiche si deve tenere ovviamente in considerazione gli aspetti legati alla sicurezza. Quando uno o più calcolatori sono connessi ad altre reti o scambiano documenti e/o programmi con altri utenti, ad esempio mediante dischetti, il primo rischio è costituito dai virus. Se i calcolatori fanno inoltre parte di una LAN connessa in modo permanente ad Internet si deve prestare anche attenzione al problema delle intrusioni da parte di persone interessate per qualsiasi motivo a violare i sistemi altrui. Occorre quindi prendere le massime protezioni nei confronti degli attacchi da virus e/o da pirati informatici.

Dato un qualsiasi calcolatore si deve prendere le massime precauzioni perché sia il più sicuro possibile nei confronti di attacchi esterni. Non si deve dimenticare che un calcolatore violato oppure infetto da virus, può rappresentare anche una seria minaccia anche per le altre macchine connesse ad Internet. Il fatto di non avere nulla di importante sulla macchina non esonera dal prendere le massime precauzioni.

Ovviamente parlando di sicurezza in termini informatici è difficile quantificare la protezione necessaria a difendere la macchina da attacchi comunque sicuramente è necessario un buon antivirus mantenuto costantemente aggiornato ed un piccolo firewall, anche software, per proteggere la macchina da accessi esterni.

30 Firewall

Il firewall è un dispositivo di sicurezza che viene inserito nelle reti per difenderle da attacchi. Concettualmente è un dispositivo che consente di analizzare il traffico di rete a livello di pacchetti dati TCP/IP e di confrontarli con delle regole che sono state preimpostate dall'utente.

Generalmente il Firewall è una macchina dedicata (Appliance) oppure un normalissimo calcolatore con opportuno software, che viene inserito tra la rete locale e la connessione ad Internet per difendere la rete locale dagli accessi non autorizzati da Internet. E' quindi un programma in cui compito è fare da barriera nei confronti delle intrusioni.

I Firewall rappresentano la difesa delle reti contro gli attacchi. Sono dei programmi scritti in modo di potere analizzare il traffico in arrivo e in uscita dalla rete: sono delle vere e proprie barriere utilizzate per separare la rete interna (LAN) dalla rete esterna (INTERNET) in modo di potere adottare delle opportune politiche di difesa.

Questi programmi sono in genere configurabili mediante regole: ad esempio si può istruire il Firewall in modo tale che lasci passare solo i pacchetti TCP/IP destinati ad un certo indirizzo IP e ad una determinata porta fermando tutti gli altri pacchetti. Volendo fare un esempio con una piccola rete composta da una decina di calcolatori, un server WEB, un server MAIL ed un file server una possibile configurazione del firewall ad esempio potrebbe essere:

- accettare in ingresso tutti i pacchetti HTTP indirizzati al WEB server sulla porta 80
- accettare in ingresso tutti i pacchetti SMTP indirizzati al MAIL server sulla porta 25 Tcp e 25 Udp
- accettare tutti i pacchetti in uscita verso qualsiasi indirizzo per la porta 80

- accettare tutti i pacchetti SMTP in uscita dal MAIL server alla porta 25 Tcp e 25 Udp
- accettare tutti i pacchetti in uscita relativi al traffico ICMP per il comando PING
- accettare tutti i pacchetti in uscita relativi alle richieste al DNS

Con una configurazione di questo tipo isolo la LAN dal mondo Internet ovviamente escludendo il traffico verso i servizi che mi servono. Quindi gli utenti della LAN possono tranquillamente inviare posta su Internet, consultare pagine WEB ed utilizzare il comando PING come diagnostica in caso di problemi con le connessioni Internet. Gli utenti del mondo Internet possono invece solo consultare le pagine HTTP del mio WEB server ed inviarmi posta. Ogni altro tentativo di accesso è bloccato dalle regole del Firewall.

Il Firewall è una barriera posta a protezione della rete ma non si devono comunque dimenticare le tradizionali norme di prudenza. In qualsiasi caso non è possibile fidarsi ciecamente di un Firewall, occorre almeno verificare dai LOG del Firewall se ci sono stati tentativi di accesso e se eventualmente ci sono stati dei problemi. Non dimenticate che la maggior parte dei Firewall non sono altro che dei normalissimi calcolatori configurati con un opportuno programma. I sistemi operativi di questi calcolatori potrebbero anche avere delle vulnerabilità che consentono a qualche attaccante di aggirare le protezioni del Firewall.

Il Firewall è comunque uno dei tanti tasselli che consente di rendere sicura la LAN nei confronti di possibili attacchi dall'esterno

Nel caso di LINUX esistono vari programmi in grado di realizzare un Firewall sulla rete (ad esempio ipchain), alcuni programmi secondo lo stile di Linux sono gratuiti mentre i più sofisticati sono ovviamente delle normalissime applicazioni commerciali disponibili in genere per le varie piattaforme (Linux, Windows Nt, Unix ecc.)

Le porte sono numerate da 0 a 65535 suddivise in tre intervalli come da tabella che segue.

TABELLA 2 - INTERVALLO NUMERAZIONE PORTE IP

PORTE	INTERVALLO
di sistema	da 0 a 1023.
registrate	da 1024 a 49151
assegnate dinamicamente o private	da 49152 a 65535

31 Personal Firewall

Fino a questo momento ho parlato del firewall a protezione della rete, come calcolatore dedicato posto tra il Router e la rete stessa. Parlando di ambiente windows e singoli PC connessi ad Internet direttamente mediante modem esistono svariati programmi che consentono di implementare le funzioni minime di un firewall ed aumentare la sicurezza del sistema tenendo sotto controllo l'attività del modem: tra i vari programmi segnalo i due programmi di Symantec:

- Norton Internet Security Suite - commerciale
- Symantec Personal Firewall - commerciale
- Tiny Personal Firewall - gratuito

Questi programmi consentono di implementare delle funzioni minime di sicurezza impostando un firewall dotato delle funzioni di base.

Ho citato solo tre programmi anche se la scelta è veramente vasta. I prodotti di Symantec e di McAfee sono compresi nelle loro Internet security suite che comprendono tra i vari programmi anche gli antivirus.

Il terzo programma che ho citato è uno dei tanti programmi gratuiti che implementa un piccolo firewall sul PC. Io lo utilizzo da parecchio tempo e devo ammettere che mi sembra fatto piuttosto bene. Collegandovi ad Internet con il PC ed il modem dopo avere installato un firewall non avete idea di quanti siano i tentativi di accesso dall'esterno. Direi che connettendosi mediante modem da una delle free-Internet tipo clubnet di telecom, libero ecc potreste ricevere una segnalazione in media ogni 15 secondi. Ovviamente il firewall è configurabile per bloccare tutti i tentativi senza dare segnalazione altrimenti...non si lavora.

Riporto a titolo di esempio due schermate di configurazione del personal firewall sul mio portatile. Nella prima si vede quale tipo di traffico è ammesso e quale è vietato. Dalla seconda schermata si vedono invece i servizi attivi sulla macchina al momento. Si può notare che è attivo norton antivirus sulla porta 1027, windows sulle porte del netbios dalla 127 alla 129 ed infine personal firewall sulle sue due porte.

Per quanto riguarda le regole impostabili sono leggermente diverse da quelle di un firewall tradizionale; essendo un programma che gira sulla stessa macchina è in grado di consentire o negare il traffico in base agli indirizzi fisici ma anche ai singoli programmi. Considerando il fatto che per i vari programmi mantiene un database con le chiavi MD5 è in grado di accorgersi che, un determinato programma che ha accesso ad esempio all'esterno, è stato cambiato rispetto alla versione originale quindi chiede conferma per accettare la nuova regola. Oltre alle funzioni di firewall svolge anche delle minime funzioni di IDS (Intruder Detection System)

TABELLA 3 – TINY PERSONAL FIREWALL: REGOLE IMPOSTATE

Rule Description	Protocol	Local	Remote	Application
<input checked="" type="checkbox"/> ANY ← Loopback	UDP/TCP (Both)	[Any port]	[127.0.0.1][Any port]	Any application
<input checked="" type="checkbox"/> ANY → DNS	UDP (Both)	[Any port]	[Any address][53]	Any application
<input checked="" type="checkbox"/> ANY → Outgoing ICMP Echo Request	ICMP (Out)	[Any]	[Any address]	Any application
<input checked="" type="checkbox"/> ANY ← Incoming ICMP Echo Reply	ICMP (In)	[Any]	[Any address]	Any application
<input checked="" type="checkbox"/> ANY ← Incoming ICMP	ICMP (In)	[Any]	[Any address]	Any application
<input checked="" type="checkbox"/> Componente di base del kern...	UDP (Out)	[Any port]	[Any address][Any port]	C:\WINDOWS\SYSTEM\KRNL386.EXE
<input checked="" type="checkbox"/> ANY ← Incoming ICMP	ICMP (In)	[Any]	[Any address]	Any application
<input checked="" type="checkbox"/> Internet Explorer	TCP (Out)	[Any port]	[Any address][Any port]	C:\PROGRAMMI\INTERNET EXPLORER\EXPLORE.EXE
<input checked="" type="checkbox"/> LiveUpdate Engine COM Mod...	TCP (Out)	[Any port]	[Any address][Any port]	C:\PROGRAMMI\SYMANTEC\LIVEUPDATE\LUCDMSE...
<input checked="" type="checkbox"/> Poco Executable	TCP (Out)	[Any port]	[Any address][Any port]	C:\PROGRAMMI\POCMAIL\POCC.EXE
<input checked="" type="checkbox"/> Norton Antivirus Agent	TCP (Out)	[Any port]	[Any address][Any port]	C:\PROGRAMMI\NORTON ANTIVIRUS\NAVAPW32.EXE
<input checked="" type="checkbox"/> Programma di trasferimento file...	TCP (Out)	[Any port]	[Any address][Any port]	C:\WINDOWS\FTP.EXE
<input checked="" type="checkbox"/> Programma di trasferimento file...	TCP (In)	[Any port]	[Any address][Any port]	C:\WINDOWS\FTP.EXE
<input checked="" type="checkbox"/> ANY → Outgoing ICMP	ICMP (Out)	[Any]	[Any address]	Any application
<input checked="" type="checkbox"/> PageMill Application	TCP (Out)	[Any port]	[Any address][Any port]	C:\PROGRAMMI\ADOBE\PAGEMILL 3.0\PAGEMILLE.EXE
<input checked="" type="checkbox"/> Acrobat Reader 5.0	TCP (Out)	[Any port]	[Any address][Any port]	C:\PROGRAMMI\ADOBE\ACROBAT 5.0\READER\ACR...

TABELLA 4 – TINY PERSONAL FIREWALL: MONITOR ATTIVITA' SISTEMA

Application	Protocol	Local Address	Remote Address	State	Creation Time	Rx [Bytes]	Rx Speed [kB/s]	Tx [Bytes]	Tx Speed [kB/s]
NAVAPW32.EXE	TCP	localhost:1027	Listening	12/Jun/2002 14:52:26	0	0	0	0
PERSFW.EXE	TCP	all:44334	Listening	12/Jun/2002 14:52:16	0	0	0	0
PERSFW.EXE	TCP	all:44334	localhost:1058	Connected In	12/Jun/2002 18:43:02	1684	0.04	25246	0.68
PERSFW.EXE	UDP	all:44334	Listening	12/Jun/2002 14:52:16	0	0	0	0
PFWADMIN.EXE	TCP	all:1058	localhost:44334	Connected Out	12/Jun/2002 18:43:02	25246	0.68	1684	0.04
SYSTEM	TCP	192.168.1.200:139	Listening	12/Jun/2002 14:51:40	0	0	0	0
SYSTEM	UDP	192.168.1.200:137	Listening	12/Jun/2002 14:51:40	4144	0	1682	0
SYSTEM	UDP	192.168.1.200:138	Listening	12/Jun/2002 14:51:40	12308	0	5668	0

Per maggiori informazioni

<http://www.tinysoftware.com/pwall.php>

32 IDS Intruder Detection System

Quando si parla di sicurezza di una rete si deve anche parlare di IDS ovvero dei programmi in grado di rilevare le intrusioni nei sistemi e dare in qualche modo un allarme. Volendo fare un paragone con la vita quotidiana i sistemi di IDS sono come degli antifurto, se il ladro tenta di entrare...suonano.

Il compito degli IDS è quello di monitorare lo stato delle macchine critiche. Nel caso di una grossa LAN aziendale, le macchine critiche sono i server. Occorre quindi verificare che queste macchine non subiscano attacchi dall'esterno. Attenzione l'IDS non impedisce l'attacco ma lo rivela così come l'antifurto non impedisce il furto ma lo rivela. Un IDS è quindi in grado di generare un allarme se riconosce che un qualche sistema è stato compromesso. Per fare questo uno dei metodi più semplici è tenere sotto costante controllo l'integrità delle aree critiche del file system. Se si vede che qualche parte del sistema operativo di un server è stata modificata oppure se si vede che risulta attivo qualche servizio in più il sistema IDS genera l'allarme. A questo punto chiaramente dovrà intervenire il responsabile del sistema e prendere il provvedimento del caso. La prima cosa da fare se ci si accorge che il sistema è stato compromesso è quella di mantenere la calma. A priori non è detto che un sistema compromesso debba per forza essere immediatamente fermato. Occorre analizzare il tipo di problema che si è riscontrato e controllare i processi attivi sulla macchina. Certamente ci possono essere dei casi in cui è meglio fermare immediatamente il sistema o almeno isolarlo dal mondo esterno ad esempio da Internet. Qualora si sia sicuri di un intrusione sul sistema alla lunga la miglior soluzione è il ripristino della macchina da una copia di salvataggio sicuramente sana.

33 Antivirus

Il software antivirus è un altro fondamentale tassello per quanto riguarda la sicurezza delle reti informatiche. Ogni calcolatore, soprattutto se esposto ad Internet o a ricevere dati dall'esterno mediante floppy e/o cd deve assolutamente essere protetto da un programma antivirus mantenuto costantemente aggiornato. Purtroppo i programmi antivirus non possono fare miracoli, nonostante la presenza di programmi antivirus anche aggiornati i virus possono sempre trovare la strada per colpire i sistemi. Ad esempio nel caso di un virus nuovissimo a forte diffusione, può capitare che il virus attacchi il sistema prima che la società produttrice dell'antivirus abbia avuto la possibilità di rilasciare un nuovo file delle firme dei virus e quindi prima che il programma sia in grado di riconoscerlo ed intercettarlo.

Non ci si deve quindi accontentare del senso di protezione dato dall'installazione del programma antivirus. Occorre sempre essere vigili e rispettare alcune norme elementari di comportamento, che in genere per le grandi organizzazioni sono racchiuse tra le regole aziendali.

34 Intranet

Normalmente con il termine INTRANET si intende l'utilizzo delle tecnologie tipo Internet (quindi TCP/IP) per realizzare una LAN interna con funzioni tipiche di Internet quindi dotata di risorse tipo WEB server, FTP server e MAIL server.

35 WEB server

Il server Web è una macchina che si occupa di pubblicare delle pagine ipertestuali pubblicate dagli utenti. Gestisce le richieste http da parte dei client (pc degli utenti) e rende il contenuto delle pagine consultate ai programmi (browser) che ne fanno richiesta.

Su una rete locale ci sono svariate possibilità di implementare un server WEB, in ambiente microsoft su windows NT server tipicamente si utilizza Internet Information Server mentre in ambiente Linux si utilizza il server Apache (un ottimo programma gratuito disponibile anche per NT).

Attualmente i server WEB basati su sistema operativo Linux e web server Apache sono tra i più diffusi dato il loro costo contenutissimo e le loro doti di robustezza ed affidabilità.

Su internet è molto diffusa la sigla LAMP che identifica un particolare tipo di server web configurato con Linux, Apache, Mysql e Php.

36 FTP server

Il server ftp è una macchina che gestisce il protocollo FTP (file transfer protocol) ovvero che consente agli utenti di trasferire i file.

Su una rete locale ci sono svariate possibilità di implementare un server WEB, in ambiente microsoft su windows NT server tipicamente si utilizza Internet Information Server mentre in ambiente Linux tipicamente si utilizza il server wsFTP o altre implementazioni.

Esiste anche una precedente versione di FTP che si chiama TFTP ovvero Trivial FTP tipica dei sistemi Unix datati che oggi è caduta in disuso. È possibile ancora trovare il TFTP come meccanismo per salvare in locale la configurazione di qualche Router.

37 MAIL server

È il server di gestione della posta elettronica, si occupa di mantenere le caselle postali degli utenti e di gestire l'inoltro dei messaggi. In un Intranet il mail server gestisce sia la posta interna che la posta esterna (vedi caselle postali su Internet).

In ambiente Microsoft sono usati Microsoft Exchange Server oppure Lotus Notes, su Novell Neware è disponibile Group Wise e su Linux è disponibile sendmail (più svariate altre alternative).

38 News server

Il news server è una macchina dedicata alla gestione del protocollo NTTP ovvero il protocollo che consente di realizzare i newsgroup. Praticamente si basa su un mail server con qualche funzione aggiuntiva.

I newsgroup o gruppi di discussione, sono l'equivalente elettronico delle bacheche in cui ogni utente può affiggere un proprio messaggio. Ovviamente la grande differenza rispetto alle tradizionali bacheche, è costituita dalla visibilità a livello quasi mondiale. I newsgroup, essendo visibili via Internet, sono visti da un gran numero di persone sparse per il mondo. Una tradizionale bacheca, per tanto sia disposta in modo strategico in un punto di passaggio per molte persone, non potrà mai avere la visibilità di un newsgroup.

Ci sono molti programmi in grado di funzionare come server per le NEWS, In ambiente linux tutte le distribuzioni propongono un loro news server liberamente installabile ed utilizzabile.

39 Servizi basati su TCP/IP

Internet viene normalmente identificata con le pagine ipertestuali del WWW oppure con i servizi di posta elettronica ed i newsgroup. In realtà con Internet identifichiamo una rete di calcolatori, con estensione mondiale, che comunicano tra loro mediante protocollo TCP/IP.

È quindi possibile utilizzare le infrastrutture di Internet per realizzare delle vere e proprie reti virtuali. I servizi che possono essere offerti su Internet possono quindi essere molteplici. In questo periodo possiamo trovare vari servizi che offrono gateway FAX o SMS mediante email oppure che offrono spazio su disco su server Internet per realizzare dei veri e propri dischi virtuali.

Navigando sui vari portali Internet si trovano inoltre numerosi servizi basati su WebCam.

40 HD virtuali su Internet

Alcuni siti offrono la possibilità di ottenere dello spazio sui dischi da utilizzarsi come disco fisso virtuale. Questo spazio è profondamente diverso dallo spazio sui server WEB con cui è possibile realizzare delle proprie pagine. In questo caso viene offerto uno spazio per realizzare un vero e proprio disco virtuale sul quale è possibile memorizzare dei files proprio come se fossero memorizzati sul disco fisso del proprio PC solo che è possibile accedere a questi files solo mediante un calcolatore con la connessione ad Internet attiva (per intenderci pagando la telefonata). Chiaramente un file memorizzato sul proprio PC è più semplice da utilizzare perché non richiede connessione ad Internet e nessun altro tipo di precauzione ma si deve ovviamente essere davanti al proprio PC. Questi dischi virtuali consentono di memorizzare files che possono essere visti ed utilizzati in qualsiasi posto uno si trovi ovviamente a patto di avere un calcolatore connesso ad Internet ed ovviamente su cui sia installato un programma uguale o compatibile a quello utilizzato per memorizzare i documenti. Un documento di testo di microsoft word ovviamente richiederà microsoft word nella versione corretta per essere aperto, oppure un programma in grado di leggere i files di word come StarOffice di Sun.

Questi dischi virtuali sono ovviamente personali, per accedere ai files memorizzati è necessario fornire il proprio UserId e la propria Password.

Chiaramente fino a questo momento non abbiamo detto nulla di nuovo: uno dei vantaggi di questi dischi virtuali è la possibilità di condividere i files memorizzati con un gruppo chiuso di utenti.

Sul WEB è possibile trovare vari siti che offrono questo tipo di spazio per memorizzare i propri files. Ci sono svariati siti che offrono dello spazio anche a titolo gratuito.

Tra i provider che offrono questo servizio a pagamento possiamo sicuramente annoverare FastWeb con la sua offerta di FastHd.

Ad esempio sul sito <http://www.driveway.com> è possibile, previa registrazione, richiedere un proprio spazio di prova gratuito (che varia tra 25 mb e 100 mb). Questo servizio consente la memorizzazione dei propri documenti e la condivisione di tutti o parte dei propri files con altri utenti di driveway. I files possono essere organizzati in direttori in modo tutto simile a come si farebbe sul disco del proprio PC.

Esempio di [accesso ad un disco virtuale](#) sul server <http://www.driveway.com>

41 Gateway FAX via email

In alternativa alle classiche macchine FAX oppure ai servizi di FAX server che consentono l'invio dei FAX direttamente via PC o LAN mediante Modem oggi è possibile utilizzare dei servizi di Gateway Fax via email ovvero si ha la possibilità di ricevere o inviare i fax sotto forma di allegati ad un messaggio di posta elettronica invece che su una macchina fax. Il principale vantaggio dell'utilizzo di un tale servizio è la possibilità di ricevere i propri fax in qualsiasi punto ci si trovi perchè la posta elettronica può essere sempre consultata da tutte le parti a patto di avere un accesso ad Internet mediante un generico calcolatore connesso ad Internet oppure mediante un telefono cellulare ed un calcolatore portatile. Ovviamente l'invio dei fax via email consente di inviare il fax come allegato ad un messaggio di email che verrà recapitato fino al gateway più prossimo al destinatario quindi convertito eventualmente in un fax tradizionale ed inoltrato con le normali linee telefoniche alla macchina fax. Il vantaggio dell'invio in questo modo è duplice, da una parte per fax a lunga distanza mi costa meno ed in secondo luogo è molto semplice l'invio del fax direttamente dal PC senza bisogno di particolari configurazioni.

Oggi ci sono svariati siti che offrono gratuitamente il servizio di ricezione dei FAX via email ad esempio io utilizzo il servizio freefax offerto da comm2000 al sito <http://www.comm2000.it> Per usufruire di questo servizio è necessario registrarsi sul sito di comm2000 al servizio freefax, vi verranno chiesti i V.s. dati anagrafici ed un V.s. UserId e Password per modificare le V.s. informazioni di registrazione. Alla fine della registrazione Vi verrà assegnato un V.s. numero di FAX virtuale ovvero un numero di FAX al quale una persona può inviare i FAX a Voi diretti. Il numero è un tradizionale numero di telefono tipo 02-700.xxx.xxx. Il V.s. numero di FAX virtuale è quello da fornire alle persone che Vi devono inviare dei FAX, per i V.s. corrispondenti è a tutti gli effetti un invio di FAX solo che a voi verrà recapitato come allegato ad un messaggio di posta elettronica. Ovviamente per chi non ha una connessione 24 ore al giorno ad Internet è necessario verificare periodicamente se esiste posta nella casella postale per ricevere i FAX. Dal punto di vista di chi vi deve inviare un FAX è più comodo l'invio ad un FAX virtuale perchè è sicuro di avere sempre la linea libera, dal V.s. punto di vista ricevete i FAX via email quindi li potete consultare ovunque vi troviate.

Comm2000 offre gratuitamente la ricezione dei FAX e come abbonamento a pagamento (un tanto a pagina spedita) la possibilità di inviare FAX mediante Internet a qualsiasi macchina FAX. In questo caso è possibile usufruire di una tariffa inferiore a quella dell'invio tradizionale dei FAX perchè il FAX viene inoltrato via Internet fino al nodo più vicino quindi viene inoltrato in rete telefonica commutata. Rispetto ai FAX tradizionali ho quindi un risparmio per l'invio di FAX all'estero o almeno in intercomunale. Per i FAX inviati in rete urbana ovviamente non ho un vantaggio perchè le tariffe di Internet e quelle della rete urbana in genere coincidono.

Oltre a Comm2000 esistono altre società ad offrire il servizio di Gateway FAX. Io ho citato comm2000 perchè è il servizio che utilizzo abitualmente quindi lo conosco bene. Un analogo servizio gratuito ed in sola ricezione è offerto anche da Tiscali (<http://www.tiscalinet.it>)

42 WebCam

Le WebCam sono delle telecamere, in genere fisse, puntate su particolari punti. Ad esempio esistono delle WebCam che riprendono il traffico sulla tangenziale di Milano. Queste telecamere riprendono delle immagini a bassa risoluzione e le rendono disponibili via Internet a chi desidera consultarle. Oggi è abbastanza diffuso trovare delle WebCam puntate su strade ad alto traffico per fornire una visione in tempo reale delle condizioni di viabilità. Esistono anche tantissime WebCam puntate su zone turistiche e/o città per fornire una visione in tempo reale ad esempio delle condizioni meteorologiche.

L'utilizzo delle webcam offre delle interessanti possibilità per realizzare, a costi contenuti, dei servizi di monitoraggio a distanza.

Con due PC dotati di WebCam e connessione Internet abbastanza veloce (almeno ISDN) è possibile crearsi un proprio sistema economico di videoconferenza che, sfruttando Internet, consente di effettuare chiamate anche internazionali alla tariffa urbana di Internet.

In genere si possono trovare i link per accedere alle varie WebCam semplicemente partendo dai Portali dei principali Provider Internet o dei Motori di ricerca. Ad esempio dal sito di quattroruote è possibile accedere ai link per le WebCam su traffico <http://www.quattroruote.it>

43 Protezioni

Spesso utilizzando i calcolatori ci si dimentica delle più elementari norme di protezione relative all'alimentazione elettrica. I Calcolatori sono attrezzature elettroniche che richiedono una fonte di energia pulita e garantita. Improvvisi sbalzi o mancanze di tensione possono arrecare gravi danni alle attrezzature elettroniche e soprattutto ai dati in esse contenuti. Una delle prime norme di sicurezza consiste quindi nel dotare le reti di calcolatori di opportuni gruppi di continuità dimensionati in modo tale da consentire il corretto spegnimento dei sistemi in caso di mancanza prolungata di alimentazione oppure di sopprimere a brevi interruzioni nell'alimentazione.

Nel caso di locali adibiti a CED sono poi necessarie anche protezioni di tipo fisico per minimizzare il rischio di furti o danni da parte di malintenzionati.

Questo tipo di protezioni, oltre ad essere dettate dal buon senso e dal valore delle macchine da custodire, sono anche rese in qualche forma obbligatoria dalla recente Legislazione della privacy DL 196/2003.

44 Gruppo di continuità

Un sistema dotato di un buon gruppo di continuità è sicuramente un sistema che offre migliori garanzie di funzionamento.

Parlando di gruppi di continuità è comunque necessario puntualizzare una cosa, trattandosi di dotazioni di emergenza devono essere mantenute efficienti altrimenti in caso di necessità non entrano correttamente in funzione.

Nel caso dei gruppi di continuità le ordinarie procedure di manutenzione prevedono il controllo del corretto stato di carica delle batterie. Alcune batterie di vecchio tipo, soggette ad effetto memoria, richiedevano inoltre dei cicli di carica/scarica completi da effettuarsi periodicamente secondo indicazioni del costruttore.

Se si saltano queste operazioni di ordinaria manutenzione si rischia di ritrovarsi, in caso di reale necessità, con dei gruppi di continuità con le batterie esaurite o non sufficientemente cariche e che quindi non garantiscono le prestazioni nominali.

45 Stabilizzatore di tensione

Gli stabilizzatori vengono utilizzati solo come filtri per evitare picchi di tensione, non sono dei gruppi di continuità quindi non proteggono gli apparati in caso di interruzioni dell'alimentazione elettrica ma garantiscono una buona protezione contro le sovratensioni. Sono particolarmente utili se ci si trova in zone disagiate soggette a molte oscillazioni nel valore medio della tensione di alimentazione.

46 Protezione elettriche

L'alimentazione è spesso fonte di dispiaceri legati a guasti improvvisi delle macchine. Un fulmine su una linea non protetta può portare delle sovratensioni o delle sovracorrenti

all'alimentazione dei calcolatori. E' molto facile che i danni non si fermino agli alimentatori ma che arrivino a danneggiare seriamente le macchine.

E' quindi importante assicurarsi che l'impianto elettrico sia realizzato nel migliore modo possibile e che preveda almeno la protezione contro sovratensioni e contro sovracorrenti.

47 Climatizzazione

Uno dei principali nemici dei calcolatori, soprattutto delle sale macchina contenenti i server, è il calore. Le macchine per funzionare correttamente senza rischi devono essere installate in opportuni locali climatizzati con temperatura ed umidità controllati.

E' essenziale che la temperatura si mantenga entro certi limiti per prevenire guasti e malfunzionamenti.

48 Antincendio

Nel caso di locali adibiti a sala macchine in cui vengono ospitati diversi calcolatori che vengono mantenuti sempre in funzione anche senza la presenza umana è necessario dotare i locali di opportuno impianto automatico antiincendio. Con apparecchiature elettriche in funzione c'è sempre qualche rischio di incendio.

49 Antifurto

Sempre per le sale macchina è necessario dotarle di opportune protezioni per minimizzare il rischio del furto dei server. Oltre al valore delle macchine in caso di furto, si deve considerare il costo del blocco del sistema in attesa di ripristinare la rete.

50 Crediti, Ringraziamenti, Licenza

51 Crediti

52 Ringraziamenti

A tutti i volontari che ogni giorno dedicano parte del loro tempo per realizzare le migliaia di applicazioni Open Source e a tutti gli utenti che accettano di impegnarsi nella migrazione dalle applicazioni commerciali a cui sono abituati, alle nuove applicazioni Open Source.

In particolare per gli spunti sull'impaginazione grafica del modello ringrazio Mirto Silvio Busico e Gianluca Turconi.

53 Licenza

È garantito il permesso di copiare, distribuire e/o modificare questo documento seguendo i termini della GNU Free Documentation License, Versione 1.1 o ogni versione successiva pubblicata dalla Free Software Foundation; mantenendo:

- Il Testo Copertina con il riferimento all'autore
- Senza Sezioni non Modificabili
- Il testo deve essere ridistribuito con la stessa licenza

Una copia della licenza può essere ottenuta presso Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

Copyright © 2005 Andrea Guido Sommaruga

STUDIO SOMMARUGA
INFORMATION TECHNOLOGY & NETWORKING

ing. sommaruga andrea guido

VIALE TUNISIA, 25 Tel **02-295.25.995**
20124 MILANO MI Cell **338-39.45.273**

web <http://www.stnet.net/sommaruga>
eMail sommaa@stcom.com

P.IVA 09922570156 C.F. SMMNRG59S24F205H

54 Impaginazione di questo documento

In questo modello sono stati introdotti vari stili di paragrafo personalizzati :

Text body 1,2 e 3 rispettivamente per il corpo del testo seguente le intestazioni Heading 1,2 e 3 (Intestazione 1,2,3,4 nella versione localizzata). L'impostazione di questi stili avviene automaticamente ogni volta che si va a capo dopo una delle intestazioni citate. Utilizzano il carattere Times.

Titolo Copertina, Times 32pt.

Testo riportato. E' utile per riportare brevi testi contenenti esempi ecc. Utilizza il carattere Courier 12pt.

Nel caso non vengano automaticamente attivati, questi stili si possono applicare manualmente, selezionandoli tra gli stili personalizzati (Modelli Utente) contenuti nello Stilista (premere il tasto F11 per visualizzarlo/nascondere)

Sono stati modificati anche 3 degli stili standard e cioè Heading 1,2,3 (Intestazione 1,2,3 nella versione localizzata), con uno sfondo giallo, ombreggiato con riquadro grigio-azzurro, esattamente come i titoli riportati in queste pagine.

Nelle righe d'intestazione della pagina sono riportati automaticamente i titoli dei capitoli modificati con lo stile Heading 1 (Intestazione 1) più il numero di versione che deve essere modificato manualmente dalla pagina di copertina. Il numero di versione è inserito come variabile utente ed è riportato nelle intestazioni automaticamente.

Nel piè di pagina è indicata la data corrente e il numero di pagina. Dal momento che questo documento è stato pensato per la stampa, i due campi sono alternativamente posizionati a destra e a sinistra, utilizzando due stili di pagina diversi, in modo da rispecchiare l'andamento delle pagine stampate. Per lo stesso motivo è stata introdotta una pagina di retro-copertina.

L'indice è modificabile in automatico a patto che si siano utilizzati gli stili contenuti nello Stilista. E' sufficiente posizionare il cursore lampeggiante al suo interno (1 click sinistro) e poi cliccare col tasto destro su di esso, scegliendo **Aggiorna Indice**.

Il grassetto è ottenuto con lo stile **Enfasi Forte**.

Lo stile *Enfasi* serve invece per *evidenziare il testo con il corsivo*.

C'è inoltre lo stile per le cornici delle immagini.