NAT Port Forwarding e VideoSorveglianza Remota

di Simone Soldati per la:

Il Presente documento è stato scritto allo scopo di fornire una spiegazione, più semplice ed esauriente possibile, sul funzionamento dei meccanismi NAT/PAT e Port Forwarding.
L'obiettivo finale è rendere raggiungibile, da qualsiasi parte del mondo (Internet), una videocamera di sorveglianza (IPCAM) e/o un Video Registratore Digitale (DVR IP) interni ad una rete LAN Privata, connessa ad Internet attraverso un Router Gateway. All'utente sono richieste conoscienze di base delle reti IP.

Per gli utenti FastWeb non esiste attualmente (Marzo 2007) la possibilità di rendere raggiungibile, da Internet, un host interno (vedi Appendice B).

N.B. Rendere accessibile un host interno ad una rete privata può comportare uno svantaggio in termini di sicurezza. L'autore declina ogni responsabilità connessa ad eventuali danni provocati dall'uso improprio delle informazioni contenute nel presente documento.

CENNI PRELIMINARI

La procedura riportata di seguito mostra le impostazioni necessarie per consentire ad un utente remoto (connesso ad Internet in qualsiasi parte del mondo) di stabilire una connessione con una Telecamera IP installata all'interno di una rete locale (LAN) gestita (e protetta) da un Router-Gateway (Fig.1).
In fig.1 è riportato lo schema di una delle situazioni più frequenti.

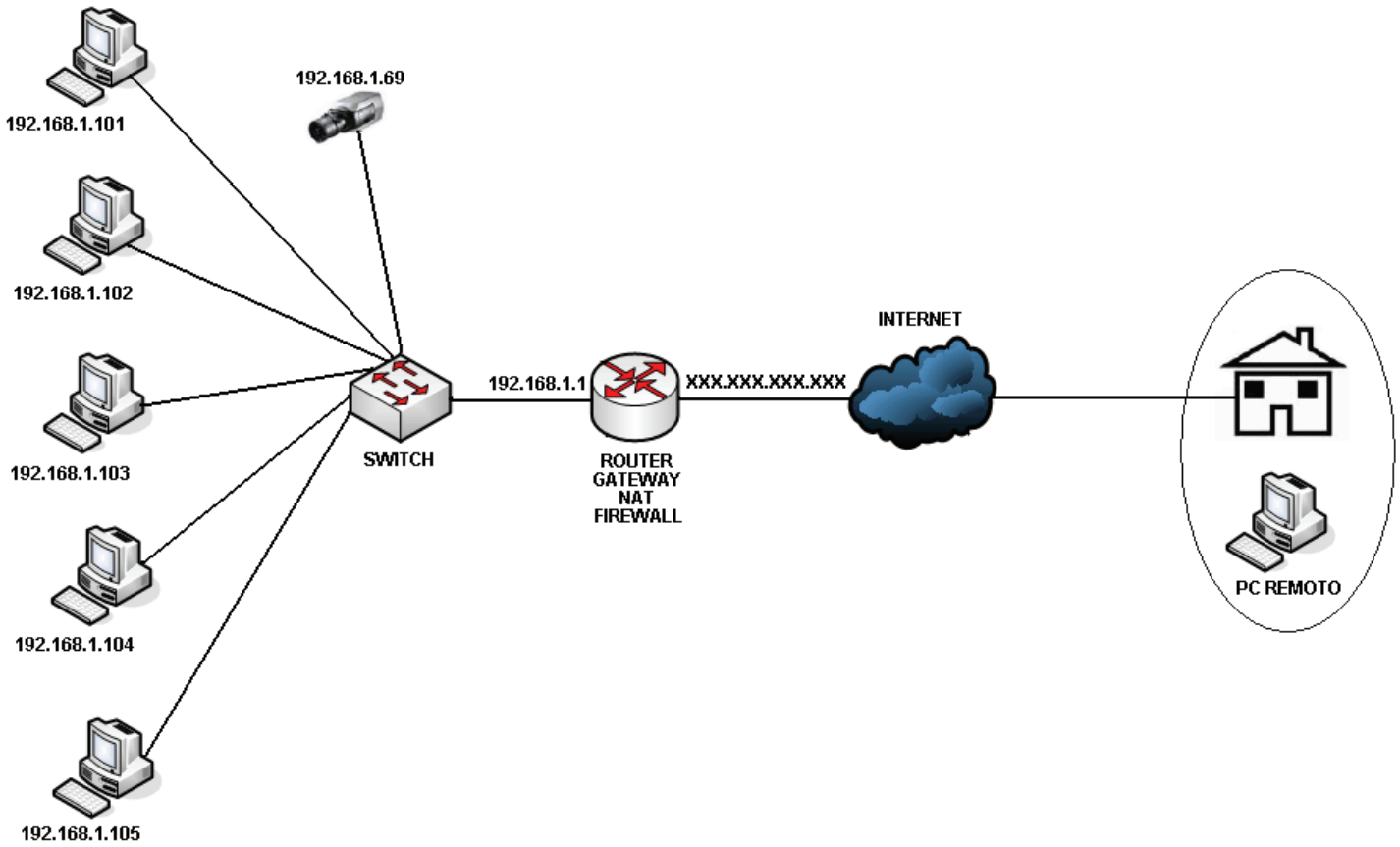

Fig.1

In tale situazione, il router svolge anche le funzioni di NAT (Network Address Translator – Traduttore Indirizzi di Rete) e di FireWall (letteralmente: Muro di Fuoco). Per capire come e dove intervenire, è necessario sapere come funzionano i meccanismi di NAT, Port Forwarding e di FireWall.

NAT:
NAT è una funzione che consente a più computer appartenenti alla stessa LAN (a sinistra in Fig.1) di andare su Internet utilizzando un unico abbonamento al Provider (Alice, Tiscali, Infostrada, Tele2 etc.etc.).Ad ogni abbonamento corrisponde un **Unico Indirizzo IP Pubblico** (xxx.xxx.xxx.xxx nella Fig.1).
Quando un utente della rete LAN vuole uscire su Internet, il router memorizza il suo **indirizzo IP Privato** (es. 192.168.1.103) e lo sostituisce con l'indirizzo IP Pubblico assegnato dal Provider. I pacchetti di ritorno vengono associati al PC che ha originato la connessione e inoltrati a quest'ultimo in maniera del tutto trasparente (l'utente non si accorge del processo). Per capire meglio il processo, facciamo un esempio pratico:

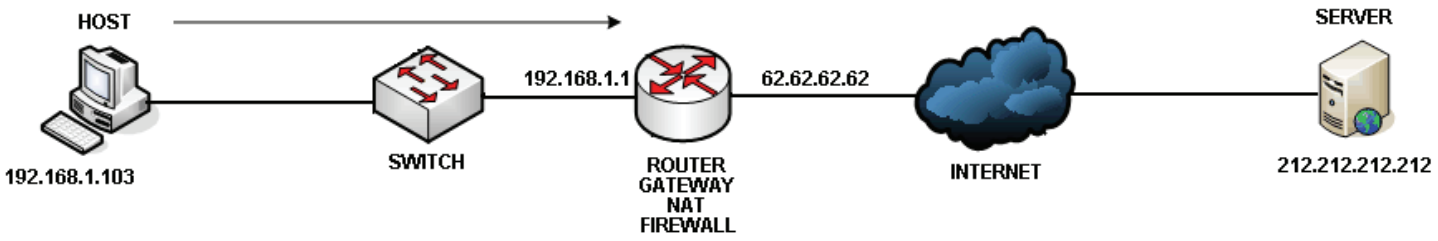

Fig.2

Il PC HOST con indirizzo 192.168.1.103 richiede di connettersi ad un sito Internet avente indirizzo 212.212.212.212.

- Come prima cosa, l'host locale invierà i "pacchetti" al proprio Router Gateway (Fig.2).
- Il Router Gateway modificherà il campo "Source Address" nell'header del pacchetto, inserendo, al posto dell'indirizzo IP dell'host (192.168.1.103), l'indirizzo IP dell'interfaccia esterna del Router Gateway (62.62.62.62).
- Una volta modificato l'header del pacchetto, il Router lo invia, attraverso Internet, al Server WEB (212.212.212.212) (Fig.3).

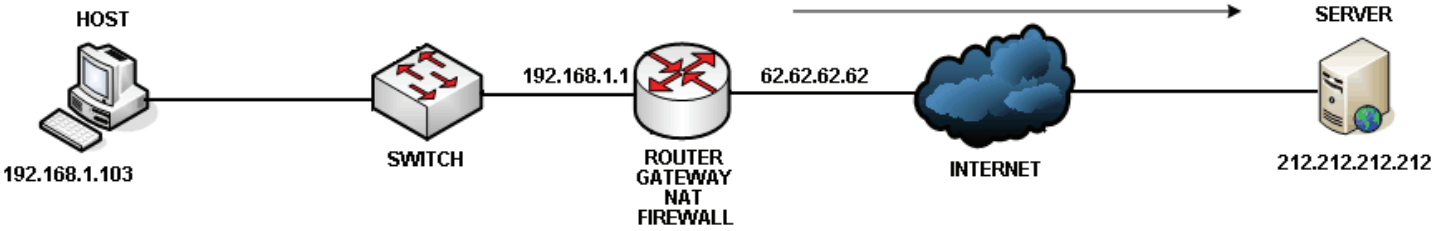

Fig.3

- Il Server risponderà alla richiesta inviando i pacchetti all'interfaccia esterna del router (62.62.62.62) (Fig.4)

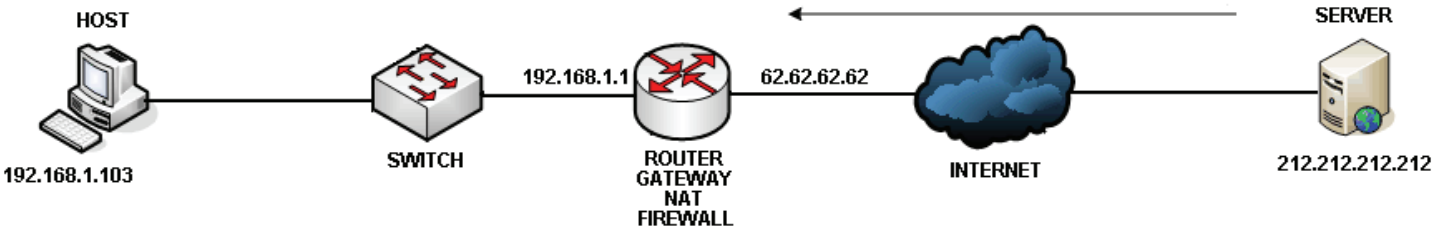

Fig.4

- I pacchetti provenienti dal Server (212.212.212.212), saranno elaborati dal Router Gateway, il quale sarà in grado di "ricordare" quale host della rete interna (LAN) aveva precedentemente avviato una connessione verso l'indirizzo IP dal quale proviene il pacchetto analizzato. Nel nostro caso il Router Gateway inoltrerà i pacchetti verso l'host 192.168.1.103 poichè era stato questo host a richiedere la connessione al Server 212.212.212.212 (Fig.5)

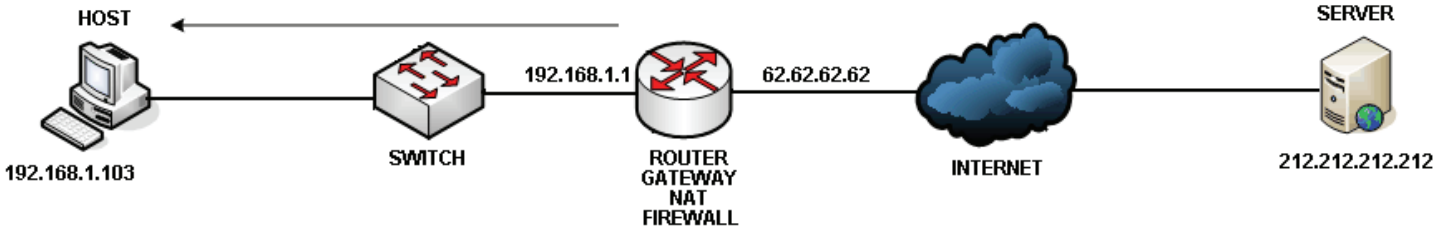

Fig.5

- I pacchetti che non sono associati a nessuna connessione già stabilita da un PC interno, vengono scartati semplicemente perché il router non sà a quale, tra i molteplici PC della rete, è destinato il pacchetto entrante.Questo aumenta la sicurezza della rete poiché, di fatto, impedisce ad un host remoto (potenzialmente ostile) di connettersi ad uno dei nostri PC. (Fig.6)

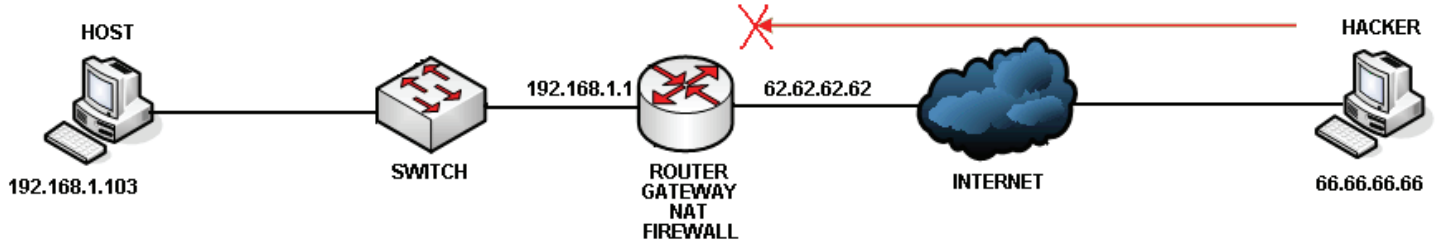

Fig.6

COME FUNZIONA UNA TELECAMERA IP (Network Camera)

Una Network Camera, una volta connessa alla rete e configurata con un opportuno indirizzo IP (che dovrà essere coerente con gli altri host della rete), offre la possibilità di collegarsi ad essa tramite un Browser (Internet Explorer, Firefox, Opera, etc.) e di visualizzare le immagini sulla finestra del browser stesso.
Questo è possibile poichè, integrato nel chipset della telecamera, c'è un Server Web che, come tutti i Server Web, accetta connessioni sulla sua porta 80 TCP. Alcuni produttori di videoregistratori digitali forniscono anche un applicativo Client, da installare su uno dei PC della rete, che consente di connettersi con il DVR per visualizzare le immagini, modificare le varie configurazioni e gestire lo storico delle registrazioni. Per rendere possibile la connessione tramite questi applicativi, un DVR dovrà avere una porta TCP (in aggiunta alla porta 80 TCP) aperta in modalità listening (ascolto) in grado di accettare connessioni da parte dell'applicativo Client.
Per esmpio, il DVR utilizzato per le prove riportate nel presente documento (ST 400 Series) utilizza le porte:

TCP 80 (Protocollo HTTP – Utilizzata dal browser)
TCP 7000 (Protocollo Proprietario – Utilizzata dall'applicazione Client fornita dal produttore)

In pratica dobbiamo considerare una Network Camera (o un DVR IP) semplicemente come un Server che offre servizi agli host (Client) sulla porta 80 TCP e, eventualmente, su altre porte specificate dal costruttore nel manuale utente.

IL PORT FORWARDING

Come abbiamo visto, il meccanismo di NAT/PAT rende impossibile stabilire una connessione da un host remoto ad un host locale. Per ovviare a questa limitazione, la maggior parte dei Router in commercio offre la possibilità di configurare una procedura detta "Port Forwarding".
Tale procedura è stata introdotta per consentire, agli amministratori delle reti aziendali, di installare e rendere raggiungibili da Internet, vari tipi di Servizi quali ad esempio:

Servizio (Server)	Descrizione	Porta TCP o UDP
VPN	Connessioni sicure che permettono ai dipendenti di lavorare da remoto	Configurabile
FTP	Consente di gestire archivi di file remoti	TCP 20-21
HTTP	Sito Web	TCP 80
HTTPS	Sito Web Sicuro (per home-banking e inserimento dati sensibili)	TCP 443
SMTP	Invio e-mail	TCP 25
POP	Ricezione e-mail	TCP 110
TELNET	Terminale remoto (non sicuro)	TCP 23
SSH	Terminale remoto (sicuro)	TCP 22
DNS	Risolve i nomi delle risorse in indirizzi IP	UDP 53
DHCP	SERVER - Assegna automaticamente indirizzi IP agli host	UDP 67
	CLIENT - Riceve automaticamente un indirizzo IP dal Server	UDP 68

Tab.1

Le associazioni tra porte e servizi, riportate nella tabella, sono stabilite dalla "IANA" (Internet Assigned Number Authority) per uniformare lo standard. Questo significa che, per esempio, un Server Web sarà "in ascolto" e risponderà sempre sulla porta 80, su qualsiasi Server in qualsiasi parte del mondo. (Vedi appendice A – Porte Server e Client).
Il nostro apparato di VideoSorveglianza (sia esso una Network Camera o un DVR IP), come abbiamo visto, è assimilabile ad un Server HTTP (Sito Web).
Con il Port Forwarding possiamo configurare il Router affinché inoltri, ad un host specificato da noi, tutti i pacchetti provenienti dall'esterno e diretti verso la porta TCP 80 (quella del Server Web integrato nel chipset del dispositivo).

Ovviamente ogni produttore di Router offre interfacce di gestione personalizzate e i menu di configurazione possono apparire più o meno intuitivi da utilizzare. Alcuni produttori inseriscono la funzionalità Port Forwarding all'interno del menù "Application & Gaming" vista la diffusione sempre maggiore di giochi on line e programmi di file sharing (e-Mule, DC++, Kazaa, etc.)
Nel nostro caso specifico è riportata la configurazione di un Router Zyxel Prestige 660H-61.

FIREWALL:

I FireWall sono dispositivi di sicurezza (possono essere Hardware o Software) che hanno il compito di controllare i pacchetti in ingresso e in uscita, inoltrandoli o scartandoli in funzione della configurazione impostata. Su molti Router disponibili in commercio è ormai integrato un firewall che, se attivato, necessita di opportuna configurazione affinchè riconosca i pacchetti destinati alla telecamera e li lasci passare.

PROCEDURA CONFIGURAZIONI per CONNESSIONE REMOTA IP CAMERA

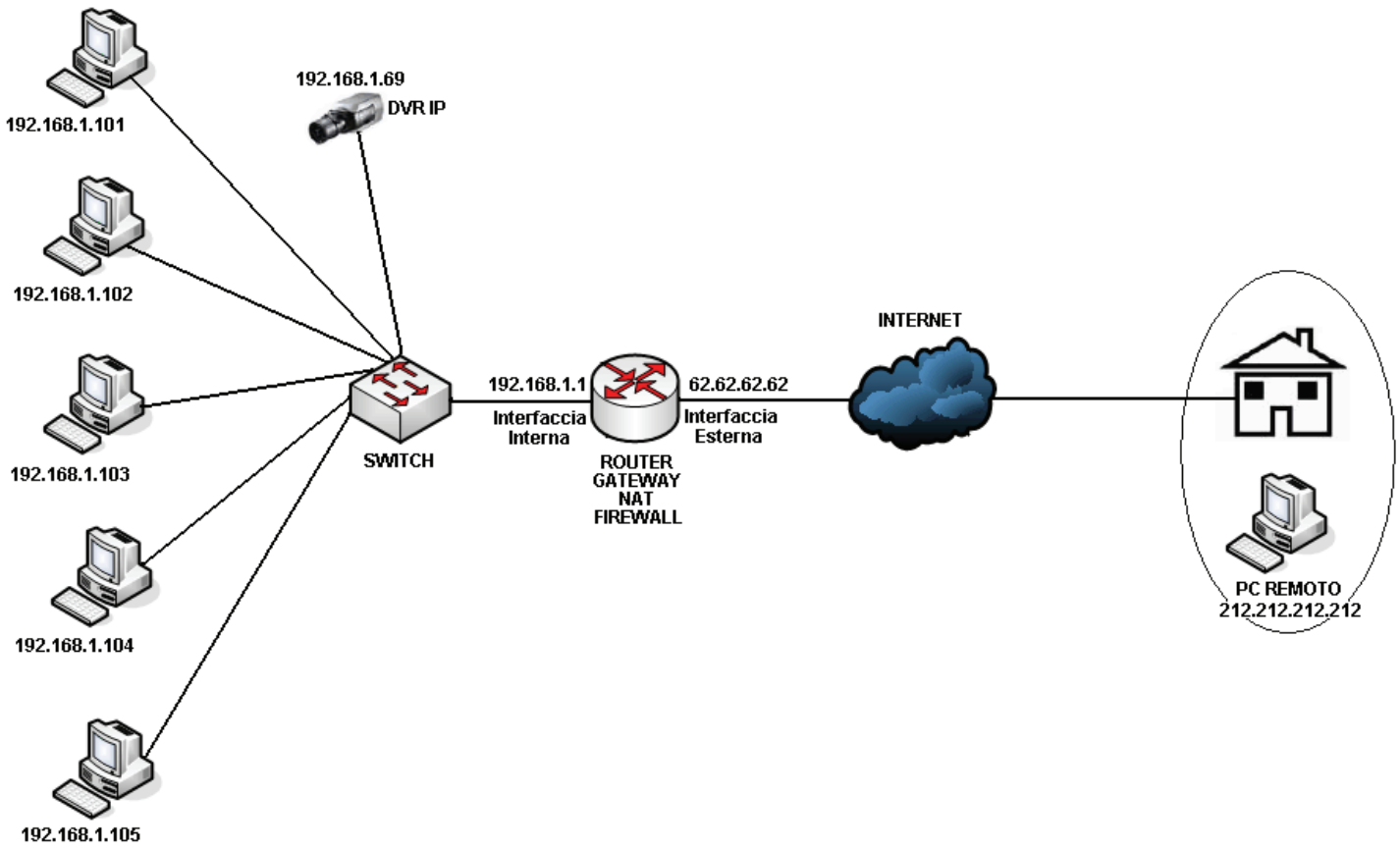

Fig.7

La figura 7 mostra la topologia logica della rete in esame:

Il DVR IP è configurato con indirizzo IP 192.168.1.69 e porta TCP 80 e TCP 7000, il Router è uno Zyxel Prestige 660H-61.
L'Interfaccia Interna del Router ha indirizzo 192.168.1.1 (ILA), mentre l'indirizzo IP Pubblico (IGA) assegnato dal Provider all'Interfaccia Pubblica è 62.62.62.62.
Il PC Remoto, Connesso ad Internet, ha indirizzo 212.212.212.212.

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	80	80	192.168.1.69
3	7000	7000	192.168.1.69
4			

Fig.8

La figura 8 riporta l'interfaccia di configurazione del Router Zyxel Prestige 660H-61, relativa ai settaggi NAT Port Forwarding. Come possiamo vedere la porta 80 e la porta 7000 sono associate all'indirizzo IP 192.168.1.69 (DVR IP).
Questo fa in modo che ogni pacchetto proveniente dall'esterno e destinato alla porta 80 o alla porta 7000 sia inoltrato all'indirizzo IP 192.168.1.69.
I campi "Start Port No." e "End Port No." servono per definire un range di porte. Esistono, infatti, applicazioni che utilizzano 2 o più porte per il corretto funzionamento, se queste porte sono consecutive, è conveniente specificarne l'intervallo. Nel nostro caso invece, dovendo specificare 2 singole porte distanti tra loro, i campi "Start Port No." E "End Port No." coincidono.

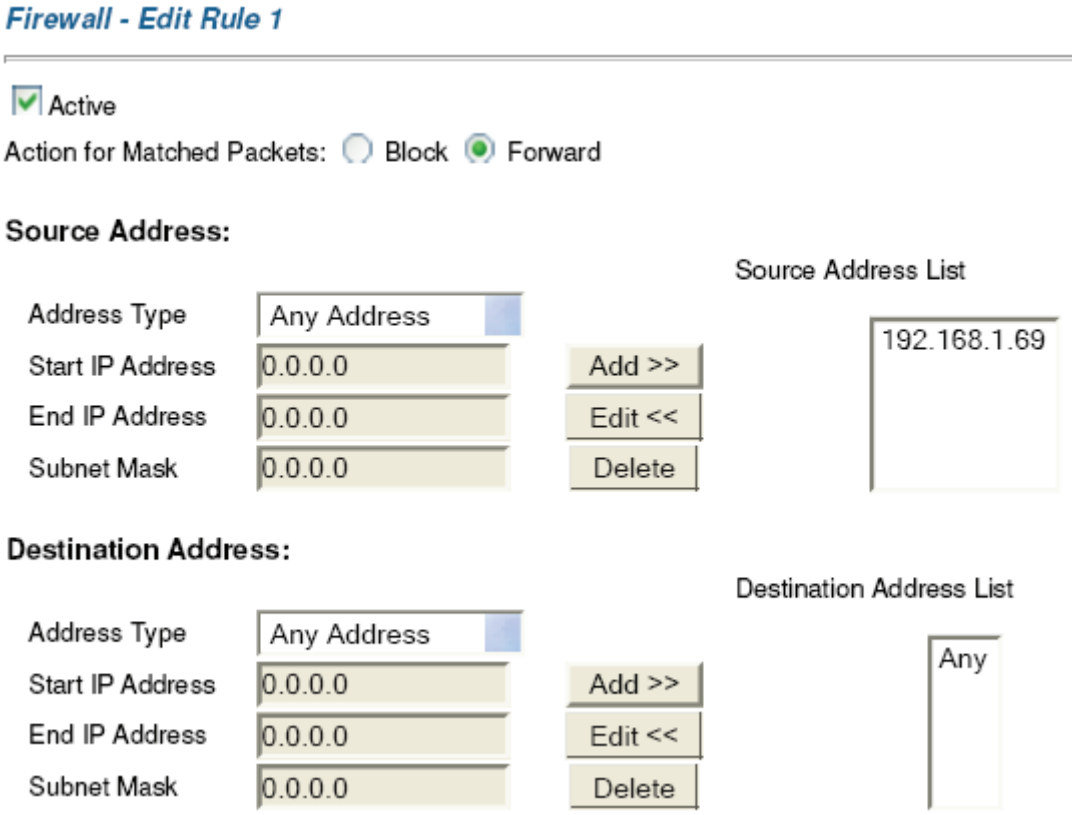

Fig.9

La Figura 9 riporta l'interfaccia di configurazione del Router Zyxel Prestige 660H-61, relativa ai settaggi Firewall LAN to WAN. Con WAN (Wide Area Network) si intende in pratica la rete Pubblica Mondiale Internet, e il traffico LAN to WAN viene detto "Traffico Uscente". Le impostazioni configurate in questo menù interessano i pacchetti in transito tra l'Interfaccia Interna e l'Interfaccia Esterna del Router (vedi fig.7). Nel campo "Source Address" abbiamo specificato l'indirizzo IP del DVR IP (192.168.1.69). Nella voce "Action for Matched Packets" abbiamo selezionato "Forward" (Inoltra). La regola nel suo insieme può quindi essere letta:

"L'host 192.168.1.69 (DVR IP) può inviare pacchetti, dalle sue porte 80 e 7000, verso qualsiasi host remoto su qualsiasi porta."

Nell'immagine non sono visibili i settaggi relativi alle porte:

- Source Port 80
- Source Port 7000
- Destination Port Any

In situazione di traffico uscente, le Source Port sono le porte lato Server (quelle del DVR IP) che sono note e fisse (80 e 7000). Le Destination Port sono le porte lato Client (quelle del PC Remoto) il cui valore può variare da 1024 a 65535. Dato che è impossibile conoscere a priori quale porta utilizza il Client per la connessione, è importante specificare "Any" (Tutti) nel campo "Destination Port" (Vedi appendice A – Porte Server e Client).

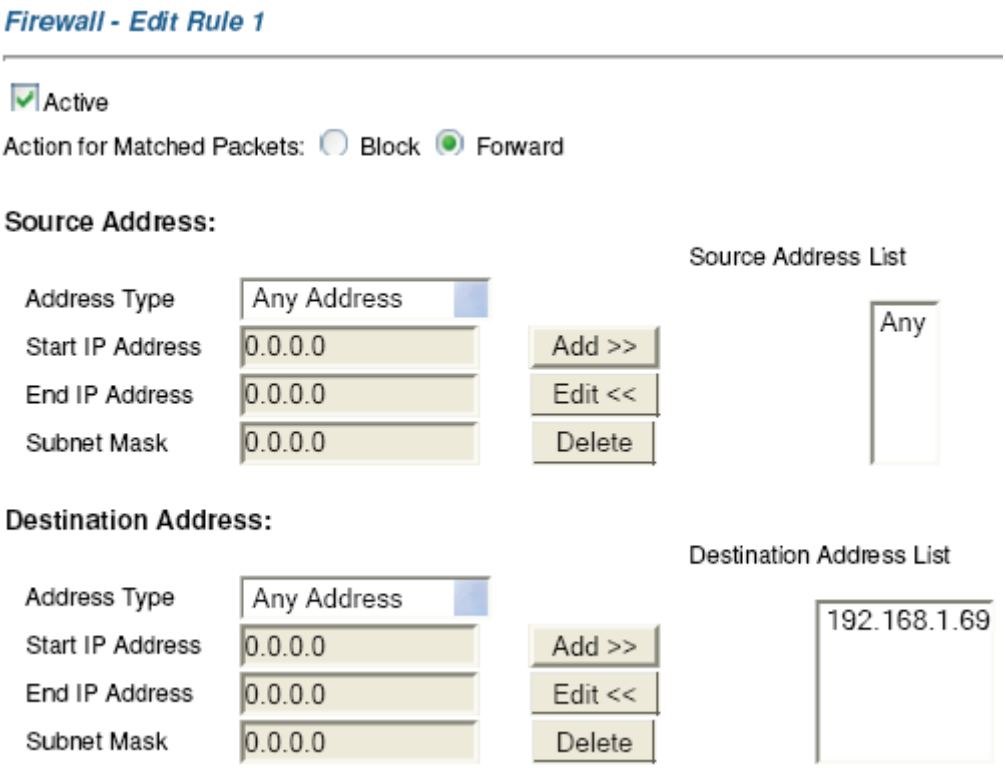

Fig.10

La Figura 10 riporta l'interfaccia di configurazione del Router Zyxel Prestige 660H-61, relativa ai settaggi Firewall WAN to LAN. Con WAN (Wide Area Network) si intende in pratica la rete Pubblica Mondiale Internet, e il traffico WAN to LAN viene detto "Traffico Entrante". Le impostazioni configurate in questo menù interessano i pacchetti in transito tra l'Interfaccia Esterna e l'Interfaccia Interna del Router (vedi fig.7). Nel campo "Destination Address" abbiamo specificato l'indirizzo IP del DVR IP (192.168.1.69). Nella voce "Action for Matched Packets" abbiamo selezionato "Forward" (Inoltra). La regola nel suo insieme può quindi essere letta:

"Qualsiasi PC remoto può inviare pacchetti, da qualsiasi sua porta, verso le sole porte 80 e 7000 del singolo host 192.168.1.69 (DVR IP)"

Nell'immagine non sono visibili i settaggi relativi alle porte:

- Source Port Any
- Destination Port 80
- Destination Port 7000

In situazione di traffico entrante, le Destination Port sono le porte lato Server (quelle del DVR IP) che sono note e fisse (80 e 7000). Le Source Port sono le porte lato Client (quelle del PC Remoto) il cui valore può variare da 1024 a 65535. Dato che è impossibile conoscere a priori quale porta utilizza il Client per la connessione, è importante specificare "Any" (Tutti) nel campo "Source Port" (Vedi appendice A – Porte Server e Client).

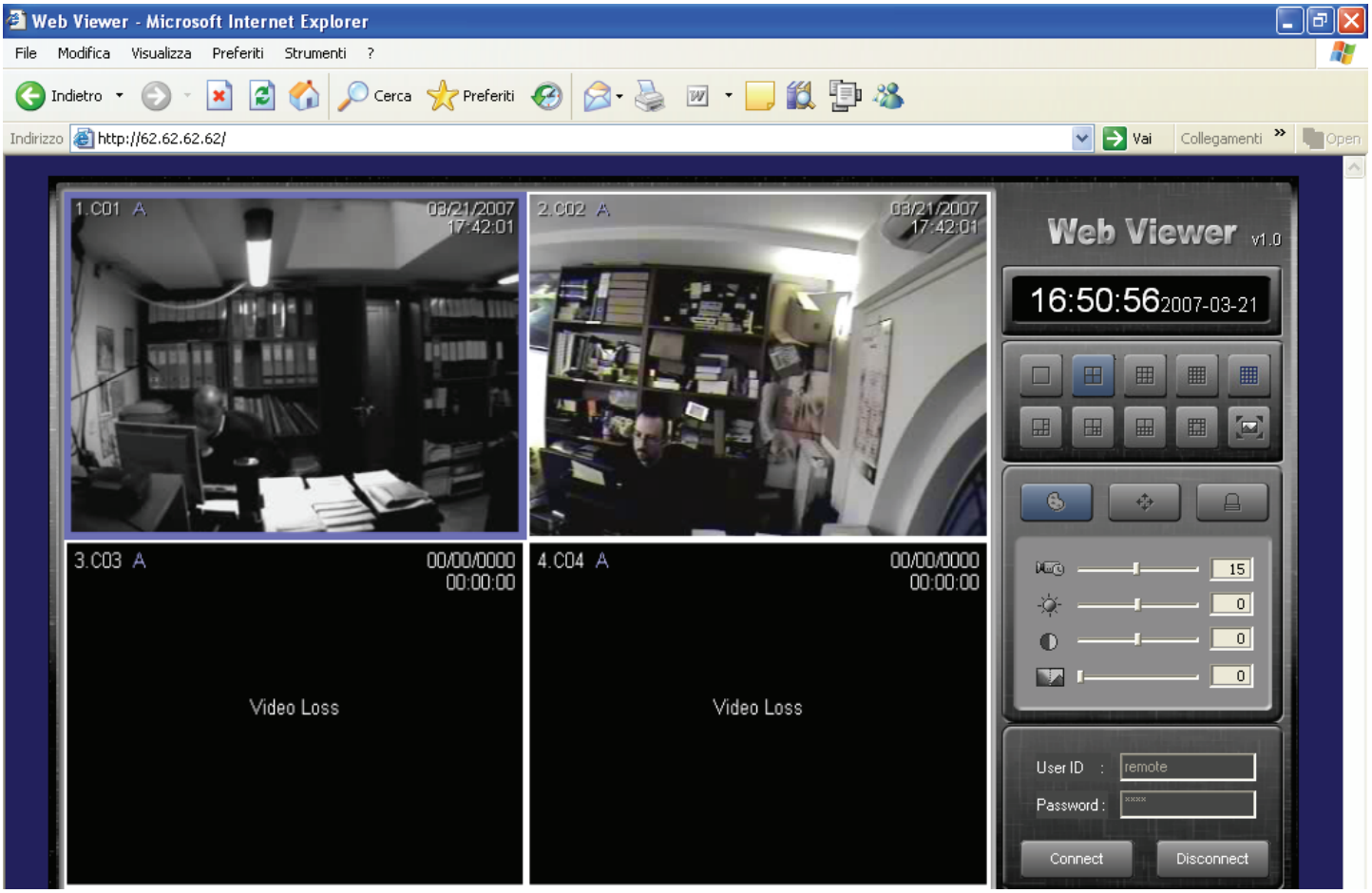

Fig.11

Dal PC Remoto connesso ad Internet (212.212.212.212), siamo riusciti a stabilire la connessione con il DVR IP (ST-ET Series). Notare che nella barra degli indirizzi del browser è specificato l'indirizzo IP 62.62.62.62 che è l'indirizzo dell'interfaccia Pubblica del Router (vedi Fig.10), invece del vero indirizzo assegnato al DVR IP (192.168.1.69). Questo è possibile perché, le impostazioni di Port Forwarding, reinstradano la connessione in maniera a noi del tutto trasparente.

Ovviamente nell'esempio gli indirizzi IP sono inventati (qualsiasi riferimento ad indirizzi IP realmente assegnati è puramente casuale).
In un caso reale, per conoscere l'indirizzo IP privato (ILA – Inside Local Address) assegnato al nostro PC all'interno della LAN, basta aprire una finestra del DOS (Start -> Esegui -> cmd) e digitare il comando: ipconfig (Fig.12)

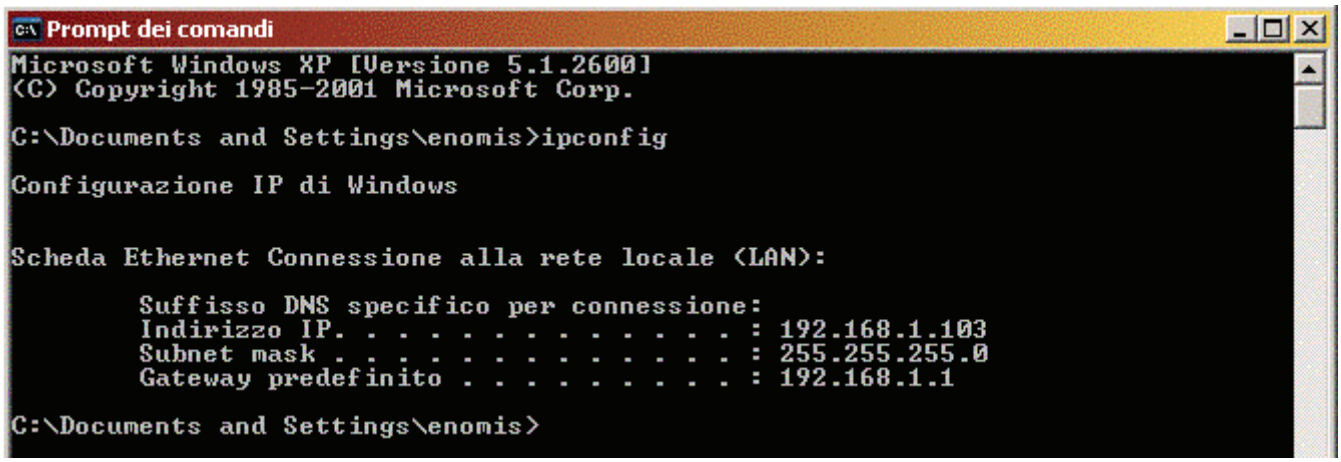

Fig.12

Per conoscere l'indirizzo IP Pubblico (quello con cui ci presentiamo al resto del mondo Internet) esistono dei siti che visualizzano sullo schermo l'indirizzo IGA (Inside Global Address) che corrisponde all'indirizzo IP Pubblico che il Provider Internet (Alice, Tiscali, Infostrada, Tele2 etc.etc.) ha assegnato all'interfaccia esterna del nostro Router Gateway:

www.myip.it

www.cisssrl.it

www.antispionaggio.it/ipaddress.php

Fig.13

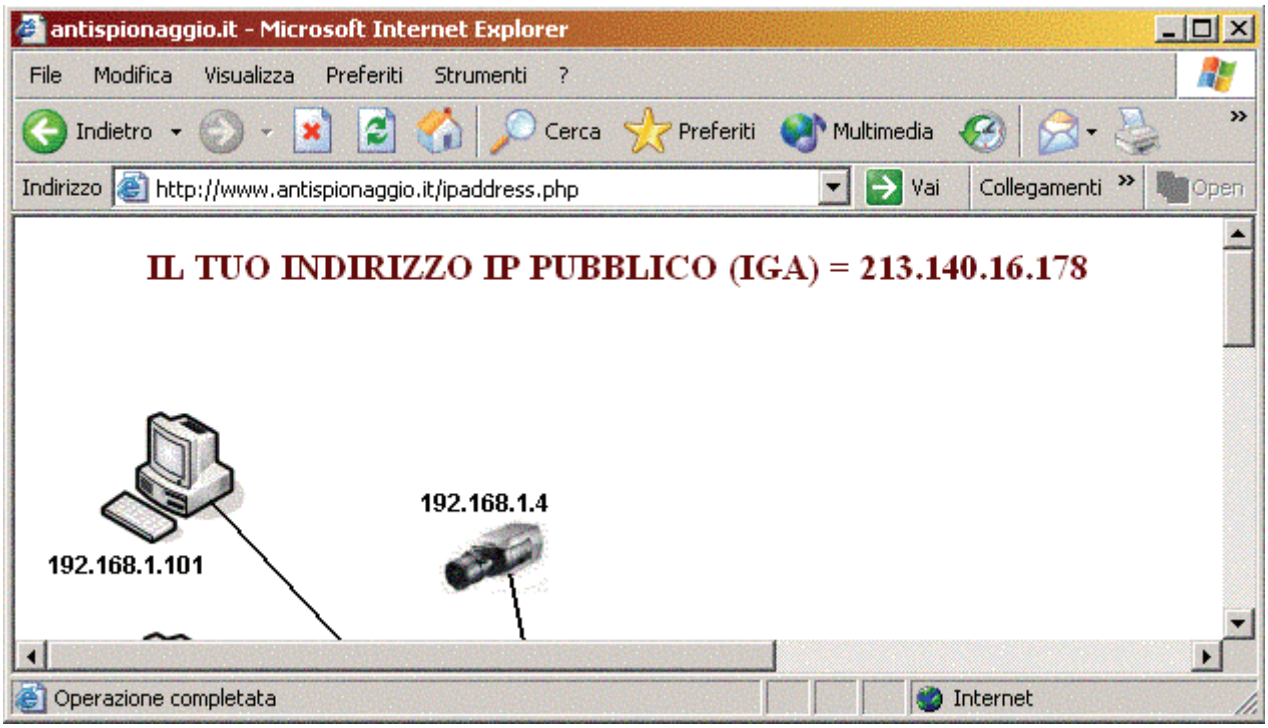

Fig.14

Appendice A

PORTE SERVER e CLIENT

Le porte sono canali di comunicazione che il Sistema Operativo di un Computer crea quando un'applicazione (o un servizio) richiede funzionalità di Rete (sia essa Internet o LAN). Il valore assegnato alle porte è rappresentato da un registro a 16 bit, quindi i valori possibili vanno da 0 a 65535.
Possiamo dividere le porte in 2 categorie:

- Porte lato Server (Wellknown Port – Porte Ben Note)
- Porte lato Client (Dynamic Port – Porte Dinamiche)

Per capire che differenza c'è tra porte lato Server e porte lato Client, è opportuno innanzitutto chiarire che cosa si intende con i termini Server e Client.
Un PC Server (Servitore) è un Computer che ha il compito di offrire servizi attraverso la rete (sia essa Internet o LAN), un Client (Cliente) è invece un Computer che usufruisce di un servizio messo a disposizione da un Server. Di conseguenza sarà sempre il PC Client a iniziare la connessione verso il PC Server e mai il contrario.
Per chiarire meglio il discorso, pensiamo ad un PC Server come se fosse un enorme palazzo, adibito a centro uffici, con 65535 Interni, situato in Corso Italia 69. In questa situazione ipotetica, l'edificio rappresenta il PC Server, "Corso Italia 69" rappresenta l'indirizzo IP e il numero dell'ufficio interno rappresenta la porta.
Ad ogni ufficio interno è associato uno specifico servizio, per esempio, se vogliamo spedire una lettera dobbiamo rivolgerci all'interno 25 (SMTP), se vogliamo ricevere la nostra posta dobbiamo rivolgerci all'interno 110 (POP), se vogliamo visitare il sito Web dobbiamo rivolgerci all'interno 80 (HTTP), se vogliamo gestire il nostro archivio di documenti dobbiamo rivolgerci all'interno 20 e 21 (FTP).
Ovviamente è indispensabile che, indipendentemente dal server, ad ogni servizio attivo sia associata sempre la stessa specifica porta, per questo la IANA (Internet Assigned Number Authority – Autorità per l'Assegnazione di Indirizzi Internet) ha riservato le porte da 0 a 1023 (Wellknown Port – Porte Ben Note) ai servizi principali, e ha uniformato lo standard associando, ad ogni servizio, una porta convenzionale (vedi Tab.1). In questo modo il programmatore che scrive un'applicazione Browser, specificherà Destination Port = 80 per la formattazione dei pacchetti; il programmatore che scrive un'applicazione Client di posta elettronica (tipo MS Outlook) saprà già che, per l'invio, dovrà specificare la porta 25 mentre per la ricezione dovrà specificare la porta 110.
Un PC Client, come abbiamo visto, è un PC che non offre servizi ad altri utenti e non ha quindi bisogno di avere porte standard in ascolto. Le porte, in un PC Client, vengono create dal Sistema Operativo nel momento in cui un'applicazione ha necessità di connettersi ad un qualunque servizio di rete (Web, File-Sharing, FTP, DNS, etc.). Il valore attribuito alla porta creata, può teoricamente variare da 1024 fino a 65535 ed è associato al processo che l'ha generato. Per capire meglio il concetto, vediamo cosa succede quando un host Client apre 2 processi Internet Explorer (IExplorer) per visitare 2 siti differenti.

- IExplorer 1 crea un socket TCP sulla porta 1810
- Il Client invia la richiesta verso la porta 80 del Server Web 1
- Il Server Web 1 riceve la richiesta proveniente dalla porta 1810 del Client
- Il Server Web 1 invia la risposta verso la porta 1810 del Client
- Il Client riceve il pacchetto dal Server Web 1 verso la porta 1810
- Il Client associa il numero di porta con l'applicazione che l'aveva creata
- Il pacchetto viene consegnato al processo IExplorer 1 che lo elabora.
- IExplorer 2 crea un socket TCP sulla porta 1880
- Il Client invia la richiesta verso la porta 80 del Server Web 2
- Il Server Web 2 riceve la richiesta proveniente dalla porta 1880 del Client
- Il Server Web 2 invia la risposta verso la porta 1880 del Client
- Il Client riceve il pacchetto dal Server Web 2 verso la porta 1880
- Il Client associa il numero di porta con l'applicazione che l'aveva creata
- Il pacchetto viene consegnato al processo IExplorer 2 che lo elabora.

In un PC Client il numero di porta serve, al Sistema Operativo Multitasking, per stabilire la correlazione con le applicazioni, affinché ogni pacchetto ricevuto possa essere associato al processo che ne aveva fatto richiesta.

Appendice B

FASTWEB

FastWeb merita un discorso a parte poichè differisce da tutti gli altri provider Internet. Gli abbonati FastWeb infatti non dispongono di un indirizzo IP Pubblico univoco perchè sono parte di una MAN (Metropolitan Area Network – Rete a Copertura Metropolitana) che altro non è se non una Rete LAN Privata delle dimensioni di un'intera città. In questa situazione, all'utente viene assegnato un indirizzo IP Privato FastWeb e le connessioni verso Internet passano attraverso il Router Gateway NAT/PAT di FastWeb. L'utente Fastweb è quindi nelle stesse condizioni di un host su una rete LAN, con la differenza che non potrà mai intervenire sulla configurazione del router per abilitare il Port Forwarding.

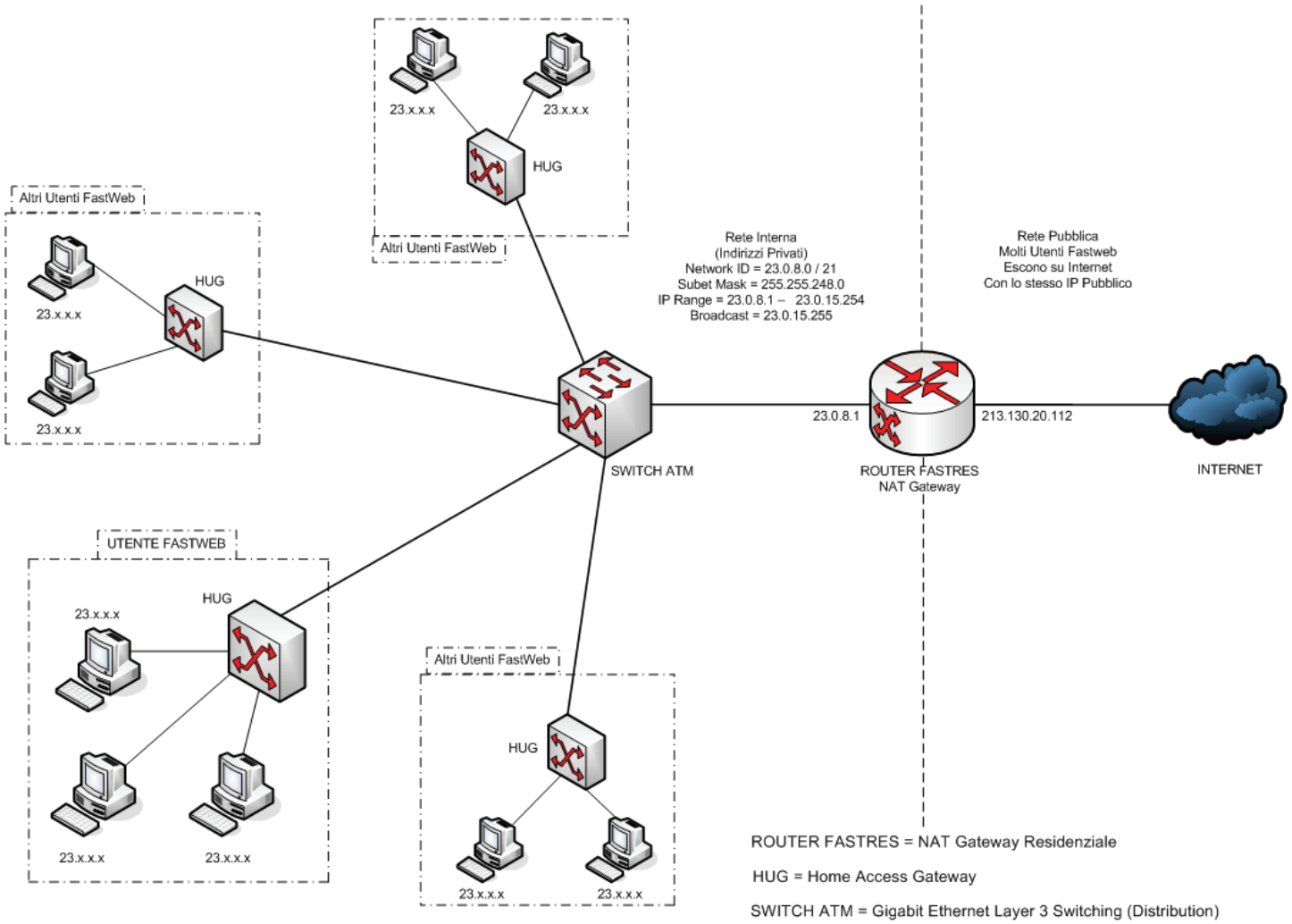

Fig.15

Nelle figure 16 e 17 viene mostrato l'Home Access Gateway che ogni utente fastweb si è visto installare in casa al momento dell'allaccio. Questo device è del tutto simile, come funzioni di base, ad uno switch. Come possiamo vedere dalla figura 15, ogni HUG è collegato ad uno switch principale, che potremmo chiamare "concentratore", che a sua volta è collegato al Router-Gateway FastWeb il quale fà anche da PAT (Port Address Traslating).
E' chiaro dunque che, per un utente FastWeb, è impossibile accettare connessioni che provengono dall'esterno poichè il Router FastRes (Fig.15) le bloccherà.
Modificare la configurazione del Router FastRes (FastWeb Residenziale) non è possibile sia per motivi legali che tecnici. Il primo è ovvio; il Router appartiene all'amministrazione FastWeb e nessun utente, anche ammesso che riesca a trovare le password, ha il diritto di modificarne la configurazione.
Il secondo motivo invece è di tipo pratico: Se ogni utente potesse modificare le configurazioni impostate precedentemente da altri utenti, in breve il sistema diventerebbe inaffidabile e instabile.

La “Borchia” Pirelli AGE-RA che il tecnico installa presso il domicilio dell’utente all’atto dell’allaccio. Ne esistono diverse versioni differenti per aspetto esterno ma pressochè uguali nelle caratteristiche funzionali

Fig.16

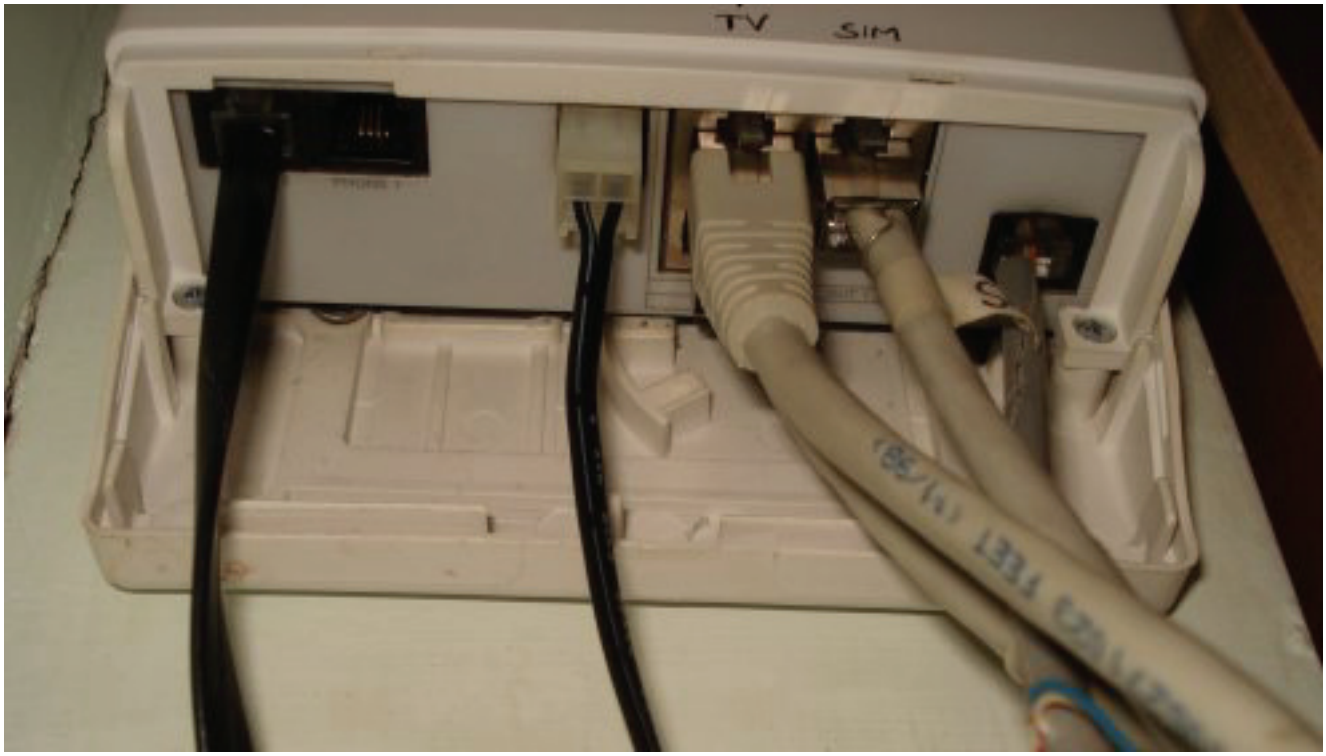

Fig.17
Da Sinistra a destra:

- Prese per telefoni PSTN (i normali telefoni analogici tipo Sirio di Telecom)
- Attacco alimentazione DC
- 3 Porte LAN per collegare PC o VideoStation
- Connettore di allaccio alla rete pubblica (verso lo switch concentratore situato nella centrale telefonica di zona).