Guida generica per i Router Hamlet

www.hamletcom.com

Capitolo 1
Introduzione

Questa guida è stata pensata per un utilizzo avanzato dei Router ADSL Hamlet e per aiutarvi nella comprensione e gestione dei nostri router.
Essendo una guida generica, si consiglia di fare sempre riferimento al manuale del prodotto specifico in proprio possesso, per controllarne le funzionalità e i modi di impostazione, che possono variare in base al modello acquistato.

1.1 Panoramica dei Router ADSL Firewall Hamlet:

Il Router Hamlet ADSL Firewall dispone di una porta per connessione ADSL ad alta velocità e 4 porte Fast Ethernet. Supporta in downstream un tasso di trasmissione fino ad 8Mbps e in upstream un tasso di trasmissione sino a 1024Kbps, inoltre soddisfa il Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2)).
Il prodotto supporta i protocolli PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged oppure routed), PPP over Ethernet (RFC 2516), IPoA (RFC1577) e PPTP-to-PPPoA relaying per stabilire una connessione con l'ISP. Inoltre incorpora un client PPTP per stabilire una connessione VPN con un server remoto PPTP. Il prodotto supporta inoltre VC-based ed il LLC-based multiplexing.
Il prodotto è la soluzione ideale per connettere un piccolo gruppo di PC ad Internet tramite una connessione veloce ADSL. In questo modo molti utenti possono condividere questa connessione ed avere accesso simultaneamente ad Internet.
Il prodotto inoltre offre un Internet Firewall adatto a proteggere la LAN locale da accessi indesiderati.
Possiede oltre alla funzione di NAT, che di per sé è una sorta di prima difesa, anche tutta una serie di caratteristiche proprie che lo rendono adatto a garantire la sicurezza della LAN. Può inoltre essere configurato per impedire ad utenti interni, della LAN, di accedere ad Internet.
Il prodotto fornisce tre livelli di sicurezza. Anzitutto maschera l'indirizzo IP dell'utente della LAN, rendendolo invisibile agli utenti di Internet rendendo, in tal modo, molto più difficoltoso, per un hacker, di localizzare il PC nella LAN. Può inoltre bloccare e fare il redirect di alcune porte per limitare i servizi cui utenti esterni possono accedere. A titolo di esempio, per assicurarsi che alcuni giochi o altre applicazioni possano funzionare correttamente, è possibile aprire alcune porte specifiche per utenti esterni per consentire l'accesso a servizi forniti da PC della LAN. Infine il Router Hamlet ADSL Firewall può smascherare e bloccare tutta una serie di Hacker Patterns non consentendo così all'hacker di accedere alla LAN, inoltre conserverà tutti questi attacchi rilevati (come qualunque pacchetto "intercettato" dal Firewall) in una opportuna tabella che potrà essere poi consultata.
Il servizio DHCP è integrato, client e server, consentendo (sino ad un massimo di 253) ai PC della LAN di ricevere il loro indirizzo IP privato dinamico all'accensione in maniera del tutto automatica. É sufficiente settare il PC come client DHCP e il Router Hamlet ADSL Firewall provvederà a passargli tutte le informazioni necessarie (indirizzo IP, Netmask, DNS, default gateway). Ogni volta che un PC viene acceso, se configurato come client DHCP, viene riconosciuto dal Router ADSL che gli assegna un IP privato istantaneamente.

Per utenti avanzati la funzione di Virtual Service offerta dal prodotto consente la visibilità alla macchina locale con uno specifico server nei confronti di utenti esterni. Un ISP fornisce un indirizzo IP che può essere assegnato al Router ADSL e gli specifici servizi possono essere re-diretti ad uno specifico computer della LAN. Un server Web può essere connesso ad internet attraverso il Router ADSL che quando riceve una richiesta di accesso, via HTML, rigira i pacchetti all'IP della LAN su cui è il PC che ospita il server Web. In questo caso il server Web è protetto da ogni tipo di attacchi grazie al lavoro fatto dal Firewall del Router Hamlet ADSL Firewall.
La funzione di Virtual Service inoltre consente di re-indirizzare a più di un PC diversi servizi. Per esempio è possibile rigirare separatamente servizi diversi a PC diversi che comunque restano protetti dal Firewall presente sul Router Hamlet ADSL Firewall.
Grazie inoltre al server VPN PPTP integrato ed al client Dynamic DNS potrete, da remoto ed utilizzando un semplice modem, chiamare il Router (benché non abbia un contratto con IP fisso) e costruire con esso una sicura VPN. Potrete lavorare pertanto da remoto come se foste nella LAN aziendale senza installare costosi software aggiuntivi poiché tutto l'occorrente è già presente nei sistemi operativi più recenti di Microsoft.

1.2 Contenuto della Confezione

Fare riferimento al manuale specifico del prodotto.

1.3 Caratteristiche del Router Hamlet ADSL Firewall

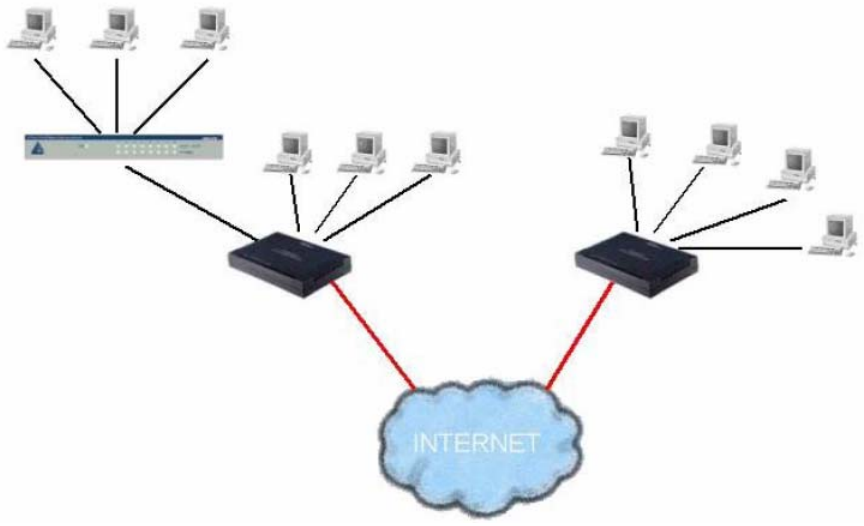
Caratteristiche offerte dal Router Hamlet ADSL Firewall:
• **ADSL Multi-Mode Standard:** Supporta in downstream un tasso di trasmissione fino 8Mbps ed un tasso di trasmissione in upstream sino a1024Kbps, inoltre soddisfa il Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2)).
• **Fast Ethernet Switch:** Grazie allo Switch 4 porte integrato potrete collegare direttamente 4 computer senza bisogno di comprare altri dispositivi. Tutte e 4 le porte supportano automaticamente la funzionalità MDI-II/MDI-X pertanto possono funzionare indipendentemente tanto con cavi dritti che incrociati. Grazie a questa funzionalità è sufficiente collegare i dispositivi, penserà lo Switch ad adeguarsi al tipo di cavo. • **Band Quota:** Le 4 porte incorporate possono essere indipendentemente configurate per assegnare a ciascuna un determinato troughtput massimo. É possibile in questo modo limitare la banda di determinati PC ed ottenere così un uso ottimale delle risorse disponibili.
• **Multi-Protocol per stabilire la connessione:** Supporta PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged oppure routed), PPP over Ethernet (RFC 2516), IPoA (RFC1577) e PPTP-to-PPPoA relaying per stabilire la connessione con l'ISP. Il prodotto supporta inoltre VC-based ed il LLC-based multiplexing.
• **Quick Installation Wizard:** Grazie al supporto di un'interfaccia di configurazione via WEB l'apparato risulta essere facilmente configurabile. É disponibile inoltre una comodissima Wizard che guida passo passo l'utente alla configurazione del Router.
• **Universal Plug and Play (UPnP) e UPnP NAT Traversale:** Grazie alla funzionalità UpnP potrete configurare facilmente tutte quelle applicazioni che hanno problemi nell'attraversamento del NAT. L'utilizzo del NAT Trasversale renderà le applicazioni in grado di autoconfigurarsi automaticamente senza l'intervento dell'utente.

• **Network Address Translation (NAT):** Consente a diversi utenti di accedere alle risorse esterne, come Internet, simultaneamente attraverso un indirizzo IP singolo. Sono inoltre supportate direttamente come web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting e altro.
• **Firewall:** Supporta un SOHO firewall con tecnologia NAT. Automaticamente scopre e blocca l'attacco di tipo Denial of Service (DoS) attack. Supporta inoltre l'URL Blocking e SPI.
L'attacco dell'hacker è registrato e conservato in un'area protetta. Aggiornando il firmware, scaricabile dal sito www.hamletcom.com, è possibile migliorare questa capacità al fine di mantenerla allineata all'evolversi della tipologia di attacchi.
• **Packet Filtering:** Non solo filtra i pacchetti in base all'indirizzo IP ma anche in base alla porta usata (dunque il tipo di pacchetti TCP/UDP/ICMP). Questo può migliorare le prestazioni nella LAN oltre che a provvedere un controllo di alto livello.
• **Sicurezza nei protocolli PPPoA e PPPoE:** Il Router supporta infatti i protocolli PAP (Password Authentication Protocol) e CHAP (Challenge Handshake Authentication Protocol).
• **SPI:** grazie alla funzionalità di Stateful Packet Inspection il Router esamina a fondo ogni pacchetto consentendo il passaggio dei soli pacchetti ritenuti sicuri. Questa tecnica consente di evitare gli attacchi di tipo Spoofing.
• **Domain Name System (DNS) relay:** Un Domain Name System (DNS) contiene una tabella di corrispondenze tra nomi di domini ed indirizzi IP pubblici. In Internet un certo sito ha un unico nome come www.yahoo.com ed un indirizzo IP. L'indirizzo IP è difficile da ricordare (però è assolutamente il modo più efficiente), certamente molto più del nome. Questo compito è svolto appunto dal DNS che grazie alla tabella incorporata riesce a fornire al PC che ne fa richiesta l'indirizzo IP corrispondente al nome del sito (e qualora non l'avesse la richiederà ad altri server DNS di cui conosce l'IP). Il Router ricevuto il pacchetto lo rigira al PC che ne ha fatto richiesta.
• **Dynamic Domain Name System (DDNS):** Il Client Dynamic DNS vi permette di associare ad un indirizzo IP dinamico (che vi viene di volta in volta passato dal server del vostro ISP) un nome statico (host-name). É necessario, per utilizzare il sevizio, effettuare una registrazione gratuita per esempio su http://www.dyndns.org/. Sono supportati oltre 5 client DDNS.
• **Virtual Private Network (VPN):** Permette all'utente di creare un tunnel direttamente per garantire connessioni sicure. L'utente può usare il server PPTP supportato dal Router Hamlet ADSL Firewall per creare una connessione VPN oppure lanciare il client PPTP da un PC remoto e collegarsi col server VPN PPTP del Router. Grazie all'uso della tecnologia DDNS non è necessario che il Router abbia un abbonamento con IP fisso.
• **Virtual Private Network (VPN):** Sono inoltre supportate leVPN in IPSec in modalità ESP, AH, IKE con MD5, SH1, DES, 3DES, ed AES.
• **PPP over Ethernet (PPPoE):** Offre il supporto per stabilire connessioni, con l'ISP, che usano il protocollo PPPoE. Gli utenti possono avere un accesso ad Internet ad alta velocità di cui condividono lo stesso indirizzo IP pubblico assegnato dall'ISP e pagano per un solo account.
Non è richiesto nessuno client software PPPoE per i PC locali. Sono inoltre offerte funzionalità di Dial On Demand e auto disconnesione (Idle Timer).
• **Virtual Server:** L'utente può specificare alcuni servizi che si rendono disponibili per utenti esterni. Il Router Hamlet ADSL Firewall può riconoscere le richieste entranti di questi servizi e rigirarle al PC della LAN che li offre. É possibile, per esempio, assegnare una data funziona ad un PC della LAN (come server Web) e renderlo disponibile in Internet (tramite l'unico IP statico disponibile). Dall'esterno è così possibile accedere al server Web che resta comunque

protetto dal NAT. Grazie all'uso della tecnologia DDNS non è necessario che il Router abbia un abbonamento con IP fisso.
• **Dynamic Host Control Protocol (DHCP) client and server:** Nella WAN, DHCP client può prendere un indirizzo IP dall'ISP automaticamente. Nella LAN, il DHCP server può gestire sino a 253 client IP, distribuendo a ciascun PC un indirizzo IP, la subnet mask ed i DNS. Questa funzionalità consente una facile gestione della LAN.
• **Protocollo RIP1/2 per il Routing:** Supporta una semplice tabella statica oppure il protocollo RIP1/2 per le capacità di routing.
• **SNTP:** Una facile via per avere informazioni sull'ora dal server SNTP.
• **Configurabile (GUI) via Web, Telnet, Seriale o SNMP:** La gestione e la configurazione sono possibili via interfaccia grafica (browser), via CLI (Telnet o Hyperterminal) o SNMP. Dispone di un comodo help in linea che aiuta l'utente. Supporta inoltre la funzione di management remota (Web, SNMP, Telnet)con la quale è possibile configurare e gestire il prodotto. Grazie all'uso della tecnologia DDNS non è necessario, per la gestione remota, che il Router abbia un abbonamento con IP fisso.

1.4 Schema di installazione del Router Hamlet ADSL Firewall

Seguire i seguenti punti per effettuare il cablaggio del dispositivo:
• Collegare la porta WAN (*LINE*) alla linea telefonica per mezzo del cavo RJ11 (in dotazione)
• Il Router Hamlet ADSL Firewall può essere collegato, tramite le 4 porte RJ45 (*LAN*), nelle seguenti modalità:
• Direttamente a 4 **PC**, tramite cavi CAT 5.
• Ad un **Hub/Switch** nella **porta UPLINK** con il cavo CAT (in dotazione).
• Collegare l'alimentatore **AC-DC (1A, 12V)** alla rete elettrica e all'apposito attacco (**POWER**)situato nel pannello posteriore.
• É possibile collegare il Router Hamlet ADSL Firewall ad un PC tramite il cavo RS232 (in dotazione tipo DB9-DB9) per configurarlo o effettuare operazioni di ripristino tramite la Console. É possibile vedere in figura un esempio di cablaggio di una rete (parte sinistra) con diversi PC (si è utilizzato uno Switch). Nella parte destra invece tutti i PC della piccola LAN (sino a 4) sono direttamente collegati al Router.



Capitolo 2
Configurazione

Il Router Hamlet ADSL Firewall può essere configurato col browser Web che dovrebbe essere incluso nel Sistema Operativo o comunque facilmente reperibile in Internet. Il prodotto offre un'interfaccia molto amichevole per la configurazione.

2.1 Prima di iniziare

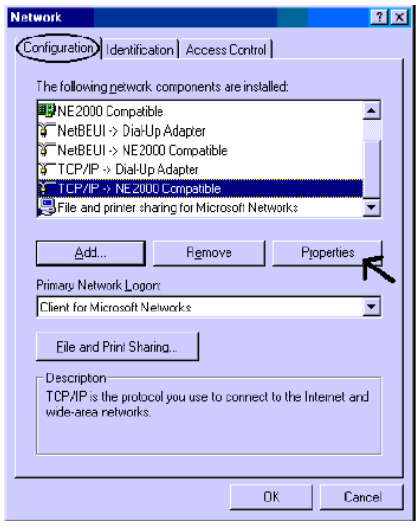
Questa sezione descrive la configurazione richiesta dai singoli PC connessi alla LAN cui è connesso il Router ADSL. Tutti i PC devono avere una scheda di rete Ethernet installata correttamente, essere connessi al Router ADSL direttamente o tramite un Hub/Switch ed avere il protocollo TCP/IP installato e correttamente configurato in modo da ottenere un indirizzo IP tramite il DHCP, oppure un indirizzo IP che deve stare nella stessa subnet del Router ADSL. L'indirizzo IP di default è 192.168.1.254 e subnet mask 255.255.255.0. Certamente la strada più semplice per configurare i PC è quella settarli come client DHCP cui l'IP (ed altri parametri) è assegnato dal Router ADSL.
Anzitutto è necessario preparare i PC inserendovi (qualora non ci fosse già) la scheda di rete. É necessario poi installare il protocollo TCP/IP. Qualora il TCP/IP non fosse correttamente configurato, seguire gli steps successivi:
Qualsiasi workstation col TCP/IP può essere usata per comunicare con o tramite il Router ADSL. Per configurare altri tipi di workstations fare riferimento al manuale del produttore.

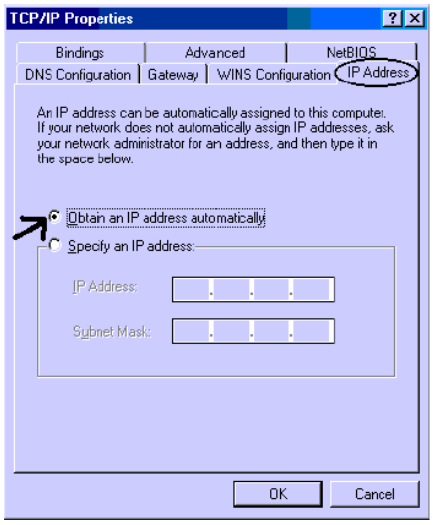
2.2 Collegare il Router Hamlet ADSL Firewall:

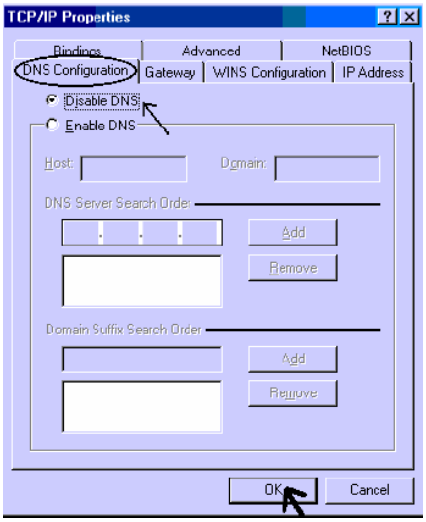
Collegare il Router alla LAN ed alla linea telefonica.
Accendere il dispositivo.
Accertarsi che i LED POWER e SYS siano accesi. Controllare che i LED LAN siano accesi.
Accertarsi che ogni software Firewall sia disinstallato dal vostro PC.
Passare adesso alla configurazione del TCP/IP sui vari PC.

2.3 Configurare i PC:
Configurare il PC con Windows 95/98/ME:

1. Andare in **Start/Settings/Control Panel**. Cliccare 2 volte su **Network** e scegliere **Configuration**.
2. Selezionare **TCP/IP -> NE2000 Compatible**, o qualsiasi Network Interface Card (NIC) del PC.
3. Cliccare su **Properties**.
4. Selezionare l'opzione **Obtain an IP address automatically** (dopo aver scelto **IP Address**).
5. Andare su **DNS Configuration**
6. Selezionare l'opzione **Disabile DNS** e premere su **OK** per terminare la configurazione.



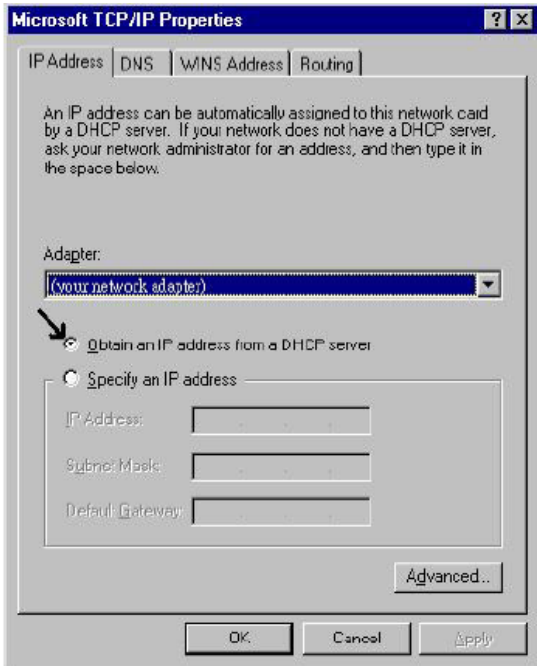


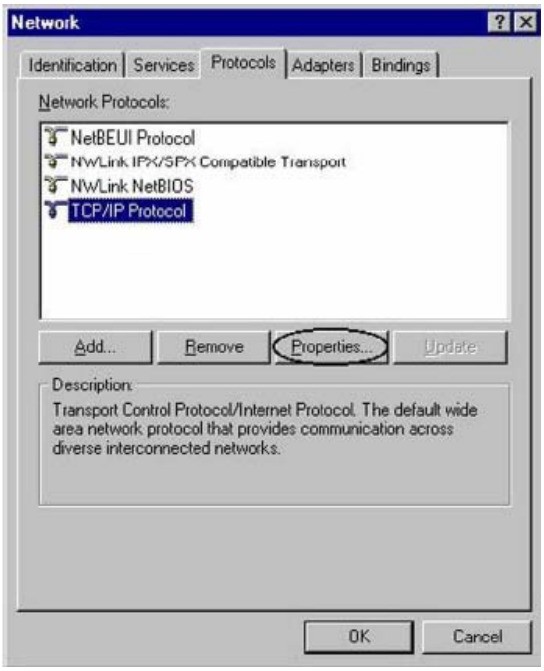


Configurare il PC con Windows NT4.0:

1. Andare su **Start/Settings/ Control Panel**. Cliccare per due volte su N**etwork** e poi cliccare su **Protocols** .
2. Selezionare **TCP/IP Protocol** e poi cliccare su **Properties**.

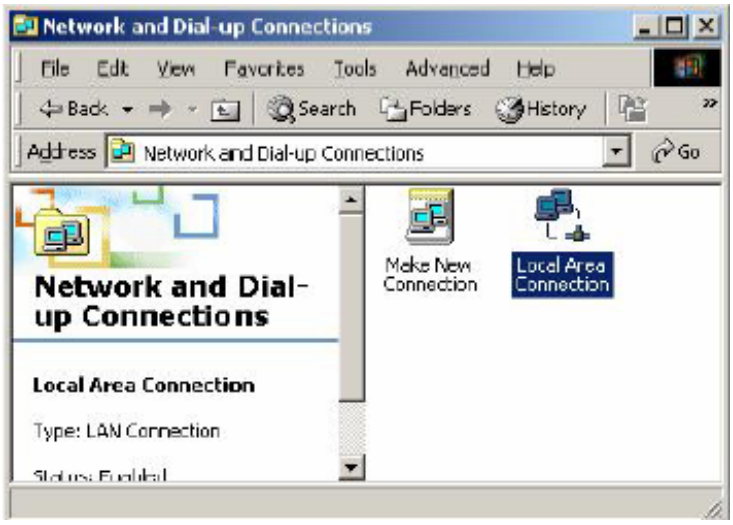
3. Selezionare l'opzione **Obtain an IP address from a DHCP server** e premere **OK**.

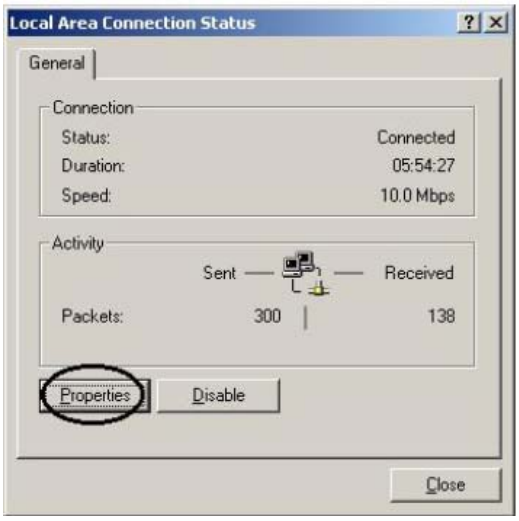


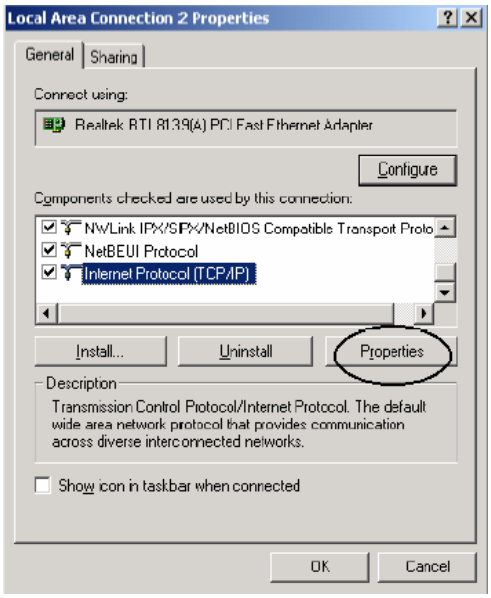


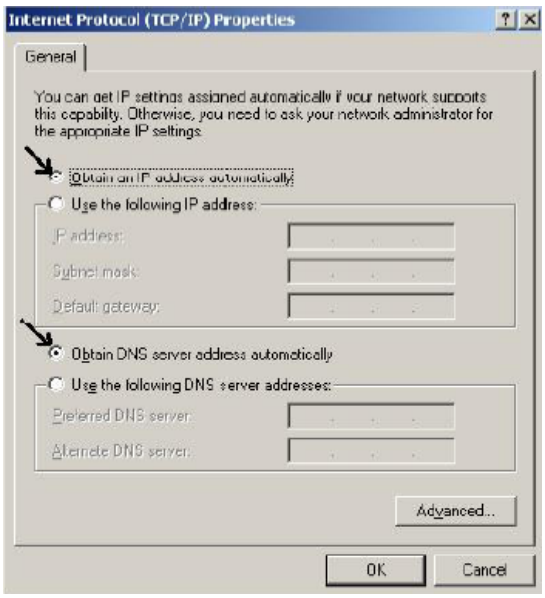
Configurare il PC con Windows 2000:

1. Andare su **Start/Settings/Control Panel**. Cliccare due volte su **Network and Dial-up Connections**.
2. Cliccare due volte su **Local Area Connection**.
3. In **Local Area Connection Status**
cliccare **Properties**.
4. Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties**.
5. Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically**
6. Premere su **OK** per terminare la configurazione



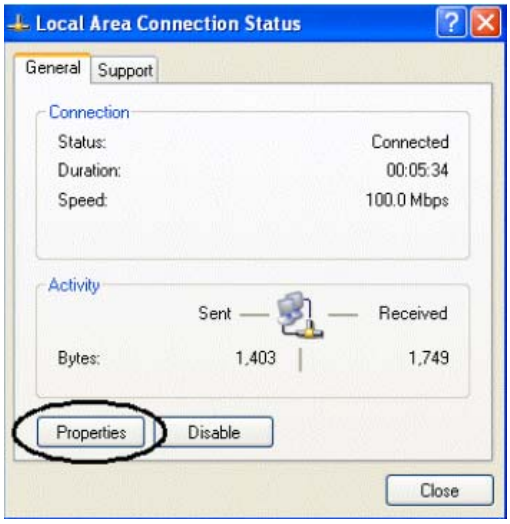


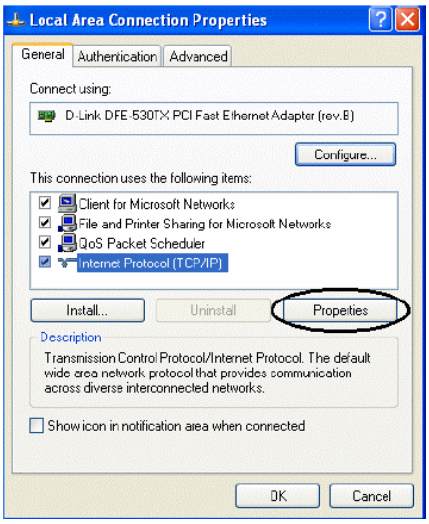


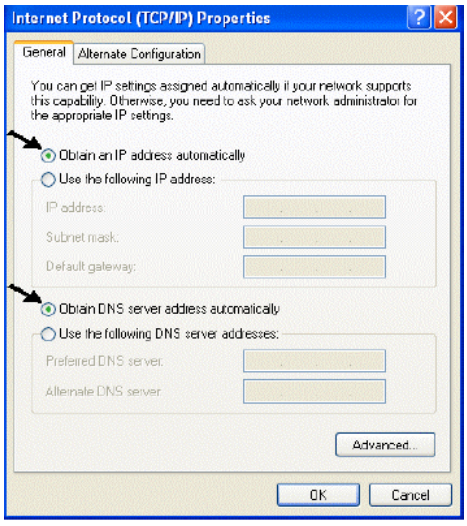


Configurare il PC con Windows XP:

1. Andare su **Start** e poi **Control Panel**. Cliccare due volte su **Network (in Classic View) Connections**.
2. Cliccare due volte su **Local Area Connection**.
3. In **Local Area Connection Status** cliccare **Properties**.
4. Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties**.
5. Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically** .
6. Premere su **OK** per terminare la configurazione.

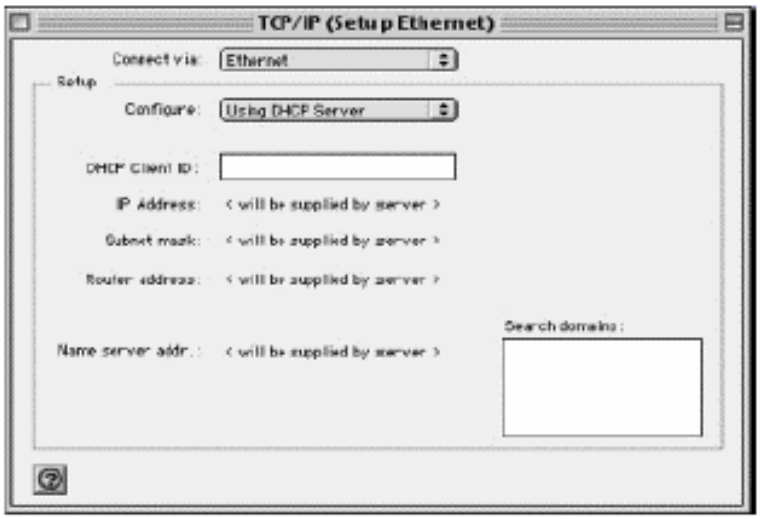






Configurare per MAC:

1. Cliccare sull'**icona Mela** nell'angolo in alto a sinistra dello schermo e selezionare: **Control Panel/TCP/IP**. Apparirà la finestra relativa al TCP/IP come mostrata in figura.
2. Scegliere **Ethernet** in **Connect Via**.
3. Scegliere **Using DHCP Server** in **Configure**.
4. Lasciare vuoto il campo **DHCP Client ID**.



2.4 Verifica della Configurazione:

Per verificare il successo della configurazione (dopo aver riavviato il PC, operazione necessaria su Win98,SE,ME e invece sufficiente ottenere il rilascio dell'IP su XP, 2000), utilizzare il commando **ping**. Da una finestra Dos digitare: **ping 192.168.1.254.**
Se appare il seguente messaggio:
Pinging 192.168.1.254with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 times<10ms TTL=64
Reply from 192.168.1.254: bytes=32 times<10ms TTL=64
Reply from 192.168.1.254: bytes=32 times<10ms TTL=64
Potete procedere andando al punto seguente. Se invece appare il seguente messaggio:
Pinging 192.168.1.254with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Controllate che il led LAN sia acceso (cambiate il cavo qulora non fosse così). Controllate l'indirizzo del vostro PC digitando **winipcfg** per (Win95,98,ME) o **ipconfig** (per Win2000,XP) ed eventualmente reinstallate lo stack TCP/IP. Se non riusciste a risolvere il problema consultare le FAQ nella parte finale di questo manuale.

2.5 Configurare il Browser:

A questo punto è necessario lanciare IE, andare nel menù **Strumenti,** poi scegliere il tab **Connessioni** e scegliere le voci:
• non utilizzare mai connessione remota
• usa connessione remota se non è disponibile una connessione di rete (Vedi figura)

2.6 Settaggi di Default:

Prima di iniziare la configurazione del Router Hamlet ADSL Firewall è necessario conoscere quali siano i settaggi di default:
Web Configurator
Username : **admin**
Password: **admin**
Indirizzo IP e subnet Mask
IP Address : **192.168.1.254**
Subnet Mask : **255.255.255.0**
ISP setting in WAN site : **nessuno**
DHCP server : **DHCP server è abilitato con indirizzi IP da 192.168.1.1 al 192.168.1.199**

2.6.1 Recupero Password:

Quando si configura il Router Hamlet ADSL Firewall con il browser premere su **OK** per entrare (dopo aver introdotto l'username=**admin** e password=**admin**) per la prima volta. É consigliato cambiare la password, al fine di aumentare la sicurezza. Il Router conserva una sola password per volta.
Qualora si perdesse la password premere il tasto Reset (posto nel pannello posteriore) per più 7 secondi. In questo modo il Router caricherà i settaggi di default (Sez 3.6).

2.6.2 Porte LAN e WAN:

I parametri della LAN e wan sono settati di default nella seguente maniera:

Porta LAN		Porta WAN
IP address	192.168.1.254	Nessuno
Subnet Mask	255.255.255.0	
Funzionalità DHCP server	Abilitato	
Indirizzi IP distribuiti ai PC	100 IP disponibili da 192.168.1.1 sino a 192.168.1.199 (Attualmente sono supportati sino a 253 utenti.)	

2.7 Informazione dell'ISP:

Prima di iniziare la configurazione del Router Hamlet ADSL Firewall è necessario ricevere dal proprio ISP il tipo di protocollo supportato per la connessione (PPPoE, PPPoA, RFC1483 oppure IPoA). Può essere utile, prima di iniziare, accertarsi di avere le informazioni riportate nella tabella sottostante:

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password. Opzionali: Service Name e indirizzo IP del Domain Name System (DNS) (può essere assegnato dall'ISP in maniera dinamica, oppure fisso).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password. Opzionali: indirizzo IP del Domain Name System (DNS) (può essere assegnato dall'ISP in maniera dinamica, oppure fisso).
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing e configurare il dispositivo in BRIDGE. Username e Password per la configurazione del Client PPPoE sul PC.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing,indirizzo IP, Subnet mask, Gateway address e indirizzi IP dei Domain Name System (DNS, sono IP fissi).
IPoA	VPI/VCI, IP address, Subnet mask, indirizzo del Gateway e indirizzi IP dei Domain Name System (DNS, sono IP fissi).

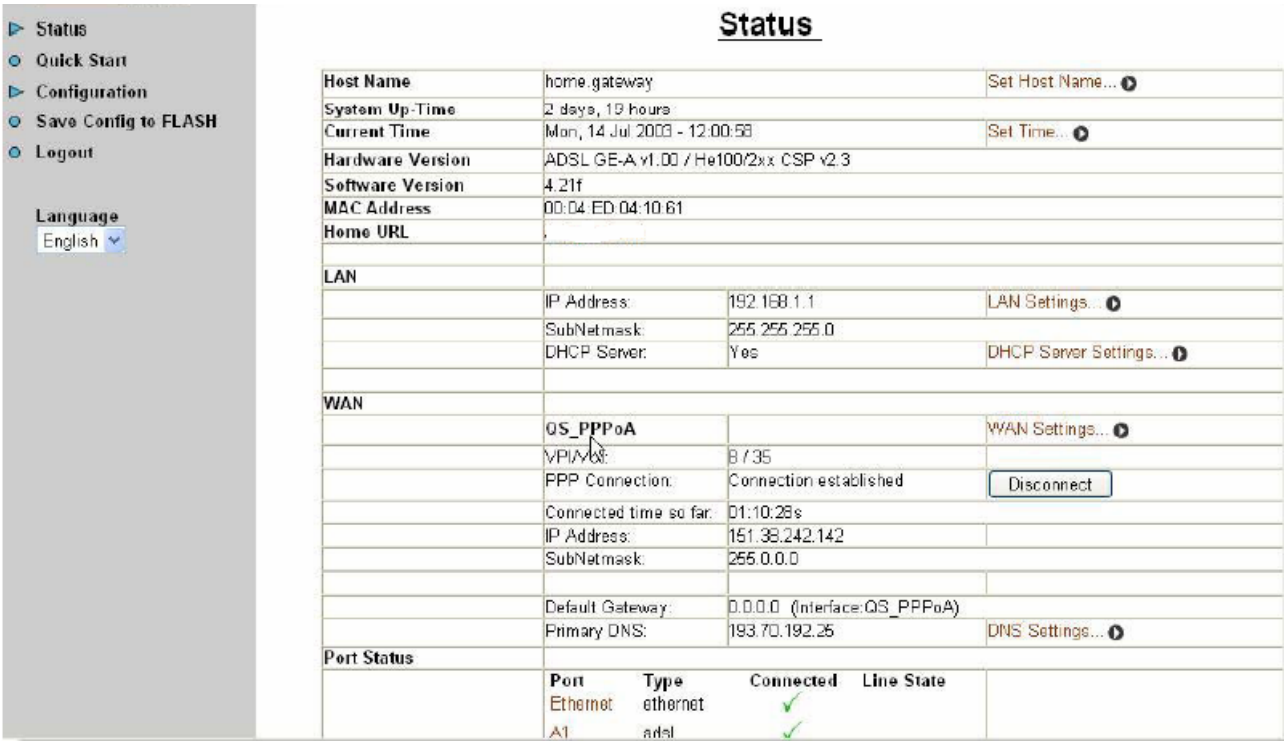
2.8 Configurare il Router tramite Browser:

Accedere col browser web al seguente indirizzo IP (dove si inserisce l'URL) che di default è:

192.168.1.254, e premere il tasto invio.
Immettere l'username e la password (utilizzare **admin** per username e **admin** come password, nel caso di primo accesso). Qualora la password fosse stata cambiata bisogna invece inserirla. Premere **OK** per continuare.

Si raccomanda, una volta configurato il Router di salvare sulla eprom la configurazione cliccando sulla sezione **Save Config To FLASH**. Questo permetterà di rendere permanente ogni modifica. Apparirà a questo punto il Menù Principale, nella parte sinistra si potrà accedere (come se si stessero vedendo i links in una homepage) a tutte le sezioni:

- **Status**
- **Quick Start**
- **Configuration**
- **Save Config to FLASH**
- **Logout**



Cliccando sulla sezione desiderata, si vedrà nello spazio della homepage tutti i settaggi relativi alla configurazione della sezione scelta, oppure si apriranno tutta una serie di sottosezioni tra cui scegliere prima di avere accesso alle configurazione vere e proprie.

2.8.1 Status

In questa sezione del Router è possibile visualizzare tutti gli stati del dispositivo ed avere così un quadro immediato dello stato di funzionamento. É altresì possibile utilizzare tale sezione per configurare determinati parametri del dispositivo. Cliccando sul Menù Status si apriranno tutte le seguenti sottosezioni:

- **ARP Table**
- **DHCP Table**
- **PPTP Status**
- **IPSec Status**
- **Email Status**
- **Event Log**
- **Error Log**
- **UpnP PortMap**

Accedendo a queste sottosezioni avrete un quadro dettagliato sullo stato di funzionamento della relativa funzionalità. Nella sezione Event Log vengono mostrate tutte le informazioni relative a tutto quello che riguarda la sicurezza. Vengono registrate qui infatti tutte le attività del Firewall. Ogni regola soddisfatta viene registrata qui assieme agli attacchi di hacker. In questo modo potrete conoscere chi vi ha attaccato (l'IP) e quando e come operano le regole di filtraggio. Quando nuove regole vengono applicate alla sezione Firewall la sezione viene svuotata. Nelle sezioni PPTP e IPSec invece potrete monitorare lo stato relativo alla VPN. É importante sottolineare che nessun settaggio potrà essere cambiato.
Cliccando invece su **Status** vedremo la seguente schermata:

Host Name	home.gateway		Set Host Name...
System Up-Time	2 days, 19 hours		
Current Time	Mon, 14 Jul 2003 - 12:01:58		Set Time...
Hardware Version	ADSL GE-A v1.00 / He100/2xx CSP v2.3		
Software Version	4.211		
MAC Address	00:04:ED:04:10:61		
Home URL	Hamlet		
LAN			
	IP Address:	192.168.1.1	LAN Settings...
	SubNetmask:	255.255.255.0	
	DHCP Server:	Yes	DHCP Server Settings...
WAN			
	QS_PPPoA		WAN Settings...
	VPI/VCI:	8 / 35	
	PPP Connection:	Connection established	Disconnect
	Connected time so far:	01:11:27s	
	IP Address:	151.38.242.142	
	SubNetmask:	255.0.0.0	
	Default Gateway:	0.0.0.0 (Interface:QS_PPPoA)	
	Primary DNS:	193.70.192.25	DNS Settings...
Port Status			
	Port **Type** **Connected** **Line State** Ethernet ethernet ✓ A1 adsl ✓		
Defined Interfaces			
	QS_WAN:	VPI/VCI:8/35	Ric: 6271D/0

Vediamo i parametri su cui possiamo agire:

Set Host Name
É possibile scegliere il nome con cui accedere al dispositivo.

Set Time
Serve per la configurazione dell'orario. Consultare la sezione opportune per maggiori dettagli.

LAN Settings
É possibile configurare l'indirizzo IP lato LAN del Router (ne può avere 2) ed i protocolli di RIP e Multicast. Per maggiori dettagli consultare la sezione opportuna.
DHCP Server Settings
É possibile selezionare la modalità operativa del DHCP. Il Router può essere infatti server DHCP oppure può effettuare il DHCP relay. É possibile inoltre disabilitare tale funzionalità. Per maggiori dettagli consultare la sezione opportuna.

WAN Settings
Permette il settaggio della connessione. Per maggiori dettagli consultare la sezione opportuna.

DNS
É possibile inserire i server DNS. Sono assolutamente da inserire nel caso di RFC1483/1577 con 1 indirizzo IP (dunque NAT abilitato) ed il Router che funge da server DHCP verso i PC della LAN che sono client. In caso di PPPoA/PPPoE vengono automaticamente forniti dall'ISP.

Port Status(Ethernet)
Informazioni sull' interfaccia Ethernet.

Port Status(A1)
É possibile forzare il tipo di modulazione e vedere la velocità della connessione.

Defined Interfaces
É possibile avere tutte le statistiche nonché informazioni sullo stato della connessione.

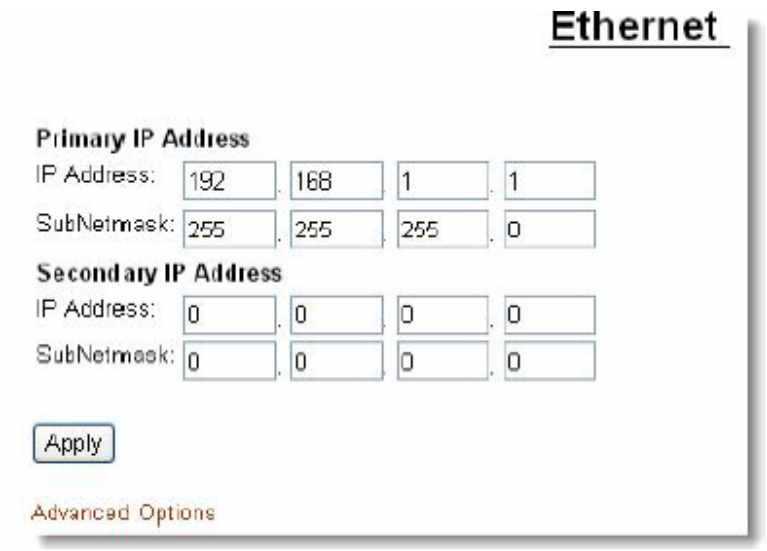
2.8.2 Configurare

In questa sezione del Router è possibile effettuare la configurazione di quasi tutti i parametri.
Ciccando sul Menù **Configuration** si apriranno tutti i seguenti sottomenù:
- **LAN**
- **WAN**
- **System**
- **Firewall**
- **VPN**
- **Virtual Server**
- **Advanced**

2.8.2.1 LAN

Questa sezione contiene i settaggi per la LAN interna. Selezionandola appariranno 3 nuove sottosezioni:**Ethernet, Port Settings e DHCP Server.**

2.8.2.1.1 Ethernet



Questo è l'indirizzo IP con cui il Router Hamlet ADSL Firewall è visto nella LAN (potrebbe essere un IP pubblico nel caso l'ISP vi fornisca una classe). É necessario, qualora si cambiasse IP con quello di un'altra subnet accertarsi che tutti i PC della LAN abbiano un indirizzo IP (se non sono settati come client DHCP) nella stessa subnet. Diversamente questo potrebbe impedire il corretto funzionamento della LAN e l'accesso al Router ADSL. IL Router supporta 2 indirizzi IP su 2 differenti subnet. In questa modalità i PC appartenenti a 2 sottoreti differenti possono contemporaneamente andare in Internet. Cliccando su **Advanced Options** è possibile configurare la versione di protocollo RIP (V1 e V2) e Multicast utilizzata dal Router. Il Router ADSL usa il protocollo dinamico RIP per aggiornare le proprie tabelle di routine facendo il broadcasting di queste informazioni agli altri router che aggiustano le loro tabelle. É necessario scegliere tra RIP1, RIP2 oppure RIP1+RIP2 sia per la trasmissione che per la ricezione attraverso la rete.

IP Address: Il valore di default è:**192.168.1.254**
Subnet Mask: Il valore di default è:**255.255.255.0.**

Gli scenari possibili per la configurazione di una rete LAN privata (o pubblica) ed il Router ADSL potrebbero essere moltissimi, a titolo d'esempio vengono riportati i più comuni. Quando si implementa 23 il Nat si isola di fatto la propria LAN da Internet. La LAN locale, se privata, deve avere gli indirizzi IP appartenenti ai seguenti blocchi (riservati dall'ente IANA per reti private).

CLASSE	IP Partenza	IP Finale	Subnet Mask
A	10.0.0.0	10.255.255.255	255.0.0.0
B	172.16.0.0	172.31.255.255	255.255.0.0
C	192.168.0.0	192.168.255.255	255.255.255.0

É chiaramente raccomandato scegliere gli indirizzi della propria LAN appartenenti alla tabella di sopra (per ulteriori informazioni fare riferimento all'RFC 1597). Scegliendo dei blocchi pubblici potreste avere problemi di mancata visibilità di taluni siti internet.
Vediamo gli scenari più comuni:

• **PC con IP appartenenti ad una classe privata**, il cui default gateway è il Router ADSL che fa NAT. Può essere attivo o meno il DHCP (il Router prenderà sull'interfaccia WAN un indirizzo IP statico o dinamico, ma pubblico, ed avrà un suo default Gateway che può essergli dato in automatico o settato a mano su informazione dell'ISP). Il management del Router può essere fatto da un qualunque PC collegato ad Internet (abilitando l'apposita funzione sul Router Hamlet ADSL Firewall) oppure dai PC della LAN. Il collegamento con l'ISP può essere uno qualsiasi tra quelli supportati (il default gateway del Router ADSL sarà dato automaticamente come i DNS in caso di PPPoE e PPPoA, dovranno essere inseriti in caso di altri protocolli come RFC1483/1577). In questo caso dunque una possibile configurazione della LAN sarebbe la seguente:

Host	Indirizzo IP	Maschera	Gateway	DNS
Router Lan IP	192.168.1.254	255.255.255.0		
PC A	192.168.1.1	255.255.255.0	192.168.1.254	Forniti ISP
PC B	192.168.1.2	255.255.255.0	192.168.1.254	Forniti ISP
PC C	192.168.1.3	255.255.255.0	192.168.1.154	Forniti ISP
PC X	192.168.1.n	255.255.255.0	192.168.1.254	Forniti ISP

In questo caso si è scelto di mantenere la rete 192.168.1.x e l'indirizzo IP (per il Router Hamlet ADSL Firewall) di default. É possibile in questo caso abilitare il DHCP server del Router (per assegnare ulteriori indirizzi IP, magari a PC portatili) ma bisogna prestare attenzione nello scegliere un pool di indirizzi compatibile (in questo caso bisognerà settare come IP starting 192.168.1.n+1, dove n+1<254).
É comunque possibile cambiare la rete, avendo l'accortezza di sceglierla tra quelle riservata dallo IANA a tale utilizzo.

• **PC con IP appartenenti ad una classe pubblica**, in questo caso tutti i PC della LAN sono raggiungibili da Internet e l'interfaccia LAN del Router ha anch'essa un indirizzo IP pubblico.
Il default gateway dei PC è l'indirizzo IP della LAN del Router che avrà chiaramente il NAT disabilitato. L'interfaccia WAN del Router prenderà un IP che può essere pubblico o privato

(si ottiene per il fornitore del servizio un risparmio di indirizzi IP), l'ISP fornirà comunque l'indirizzo del default gateway del Router Hamlet ADSL Firewall assieme alla subnet mask.
Questo scenario è tipico, ma non esclusivo, con l'uso del protocollo RFC 1483 o RFC 1577.
Come già accennato è possibile che il Router ADSL sia collegato (per la parte WAN) con una punto-punto composta da indirizzi IP che possono essere pubblici o privati.

2.8.2.1.2 Port Settings

In questa sezione è possibile forzare il tipo di modalità di funzionamento su ognuna delle 4 porte. É possibile infatti scegliere (usando il combo box) tra **Auto**, **10Full Duplex**, **10Half Duplex**, **100Full Duplex** e **100Half Duplex**. Potrete scegliere la modalità di funzionamento per ogni porta, indipendentemente dalle altre.
Potete anche, sempre per porta, allocare la banda disponibile in multipli di 32Kbps. In questo modo potrete allocare le corrette risorse evitando che taluni utenti blocchino il lavoro degli altri. Per abilitare tale funzionalità è sufficiente, una volta scelta la porta, spuntare il bottone **Enable** e scegliere il valore cui limitare la porta in questione.
É inoltre possibile anche abilitare la funzionalità **IPV4 TOS priority control**. Tramite questa caratteristica il Router processerà con precedenza i pacchetti aventi il valore di TOS selezionati. In questo modo potrete dare priorità maggiore ad opportuni servizi ed evitare fastidiosi rallentamenti.
Questo renderà più fruibili particolari servizi. Si ricorda che i router in Internet ignorano il campo TOS.

2.8.2.1.3 DHCP Server

Sono disponibili 3 differenti opzioni:

- Disabile
- DHCP Server
- DHCP Relay

Vediamo nel dettaglio come configurare la sezione DHCP:

- **Disable:** Selezionare per NON usare il DHCP Server nel Router che dunque non distribuirà gli indirizzi IP ai vari clients DHCP. In questo caso bisogna assegnare a tutti

i PC della rete un indirizzo IP (diverso per ogni PC), la subnet mask, DNS e l'indirizzo del gateway (che, salvo casi particolari, dovrebbe essere quello del Router Hamlet ADSL Firewall).

• **DHCP Server:** Selezionare per usare il DHCP Server nel Router che dunque distribuirà gli indirizzi IP, subnet mask, gateway (l'indirizzo IP del Router) e DNS ai vari clients DHCP.

Appariranno, una volta premuto il tasto **Next**, i seguenti campi:

Starting IP Address: Introdurre l'indirizzo IP di partenza del pool che il server DHCP assegnerà ai vari client**.** Il valore di default è**: 192.168.1.100**.

Ending IP Address: Introdurre l'indirizzo IP finale del pool che il server DHCP assegnerà ai vari client**.** Il valore di default è**: 192.168.1.199**.

Default Lease Time: Valore che esprime in secondi il tempo di validità dell'indirizzo assegnato.

Maximum Lease Time: Valore che esprime in secondi il tempo di validità massimo dell'indirizzo assegnato.

Use Router as DNS Server: Se selezionato tutte le richieste DNS saranno inviate al Router ADSL che provvederà a reindirizzarle.

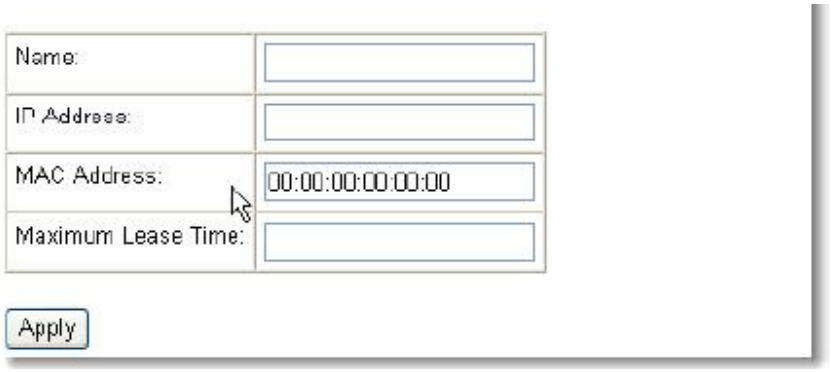
Primary/Secondary DNS Server Address:Potete introdurre gli indirizzi IP dei server DNS

che desiderate, questi saranno passati ai vari client.

Use Router as Default Gateway: Se selezionato l'indirizzo IP del Router verrà dat, ai client DHCP, come default Gateway

Qualora fosse già presenti nella LAN un server DHCP bisogna disabilitare tale funzionalità nel Router ADSL (o nel PC che opera dea server DHCP) per evitare possibili conflitti.

É inoltre disponibile la funzionalità Fixed Host:



É possibile infatti selezionare un PC come client DHCP ma fargli assegnare permanentemente sempre lo stesso IP. Immettendo infatti l'IP che si vuole assegnare e l'indirizzo MAC della scheda Ethernet il Router provvederà alla funzionalità di cui sopra.

• **DHCP Relay:**Selezionando questa funzionalità il servizio DHCP passa attraverso il Router Hamlet ADSL Firewall e raggiunge altri server che assegnano alla LAN i vari indirizzi IP. Se questa funzionalità non fosse disponibile questi PC sarebbero impossibilitati ad accedere al server DHCP. Al solito ogni PC che necessità di un

indirizzo IP si mette in contatto con un server DHCP (in questo caso fuori dalla LAN) e da questo riceve: IP, Subnet. DG, DNS.
Questi indirizzi IP sono dinamici, nel senso che hanno un tempo di validità. Scaduto questo termine il client DHCP ricontatterà il server per riottenere un nuovo IP.

2.8.2.2 WAN

Questa sezione contiene i settaggi per la WAN. Selezionandola appariranno 2 nuove sottosezioni:

- **ISP**
- **DNS**

Vediamo nel dettaglio come configurare la sezione WAN:

2.8.2.2.1 ISP

Sono disponibili cinque diverse soluzioni per la connessione con l'ISP (PPPoE, PPPoA, RFC1483 routed, IPoA, PPPoE Bridge). É necessario conoscere quale protocollo è adottato dal vostro provider. Vediamo i parametri necessari:

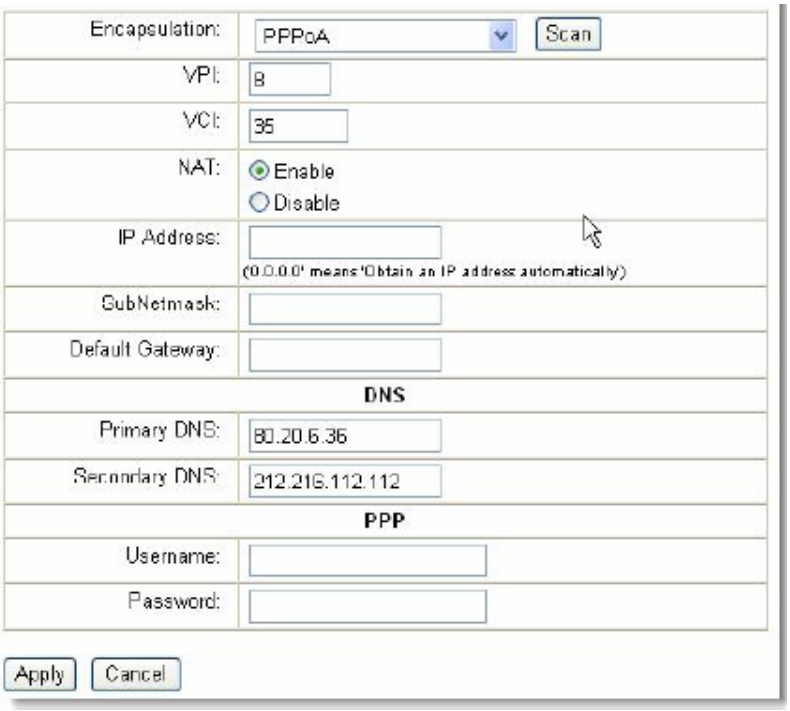
- **VPI/VCI:** Consultare il vostro ISP per conoscere i valori del Virtual Path Identifier (VPI) e del Virtual Channel Identifier (VCI). Il range valido per il VPI va da 0 a 255 e per il VCI da 32 a 65535. I valori di default per il **VPI =8** e per il **VCI =35**.
- **NAT:** Il NAT consente a più utenti di accedere ad Internet al costo di un singolo account IP. Se gli utenti della LAN dispongono di indirizzi IP pubblici e possono pertanto accedere direttamente ad Internet (e fungere da server per determinati servizi) tale funzionalità dovrebbe essere disabilitata. Il Nat inoltre è una sorta di primo firewall che migliora la sicurezza della LAN locale. Andrebbe usata quando il traffico indirizzato verso Internet è una parte di quello che circola nella LAN locale, altrimenti tale funzionalità potrebbe degradare leggermente le prestazioni della connessione ad Internet. Tale funzionalità coesiste con la funzionalità Virtual Server, DMZ e DHCP. Il Nat manipola i pacchetti IP uscenti e ne cambia il campo "IP provenienza" sostituendo il mittente del pacchetto (in questo caso l'indirizzo IP il PC della LAN, che è un IP privato non valido in Internet) con l'IP pubblico del Router Hamlet ADSL Firewall. In questo modo tutti i pacchetti uscenti dal Router avranno nel campo mittente l'indirizzo IP pubblico del Router. Quando poi i pacchetti torneranno al Router (perché sono a lui indirizzati) questo in base a tabelle memorizzate provvederà al processo contrario e li spedirà al PC interessato nella LAN.
- **Encapsulation Method:** Assicurarsi di usare lo stesso metodo di incapsulamento usato dall'ISP (LLC/SNAP or VC MUX).

Qualora si disabilitasse la funzionalità NAT il Virtual Server e VPN saranno disabilitate.

Passiamo adesso alla configurazione vera e propria dell'interfaccia WAN (ricordiamo per l'ennesima volta che dovreste avere già chiesto al vostro ISP tutti i dati relativi alla vostra connessione ADSL). Individuato il tipo di protocollo seguire la sezione opportuna.
Evidenziare la sezione **Configuration**, poi **WAN** e poi **ISP**. Apparirà la seguente immagine:

• **QUICK START**

Cliccare su **Quick Start**, apparirà la procedura automatica per selezionare la connessione.

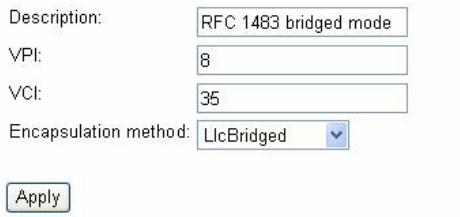


Cliccare su **SCAN** (e poi su **Start**) per ottenere le informazioni sul tipo di protocollo ed i valori di VCI/VPI. Qualora conosciate già questi valori potrete procedere inserendoli immediatamente, passando alla sezione opportuna. Dopo aver premuto il tasto **SCAN** otterrete i parametri caratteristici della vostra linea ADSL.

A questo punto evidenziare (qualora siano state rilevate più configurazioni possibili) la configurazione e premere su **Apply**. Non vi resta che inserire i parametri restanti (Username e Password nel caso di PPPoA/PPPoE o indirizzo IP/Subnet/Default Gateway nel caso di RFC1483/1577). Terminata la configurazione premere su **Save Config to FLASH** per rendere i settaggi permanenti.

• RFC1483 Bridge

In questa particolare modalità il Router funziona appunto da Bridge e dunque ruota l'indirizzo IP pubblico che il provider gli assegna (l'abbonamente sottoscritto deve essere di tipo PPPoE) al client sul PC che lo controlla. Quando viene fatto funzionare in modalità bridge molte funzionalità (Virtual Server) vengono disabilitate. Tale funzionalità potrebbe rendersi necessaria per il funzionamento di alcune particolari applicazioni internet.

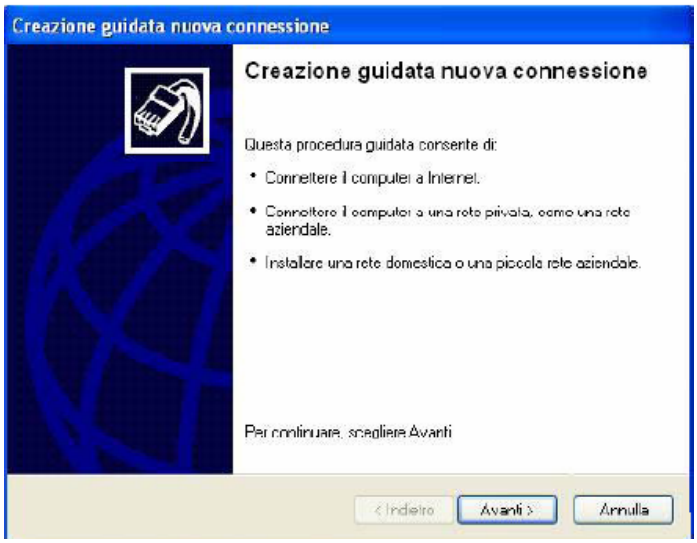


É sufficiente inserire il tipo di incapsulamento (sceglibile tra **LLC** e **VCMux**) per terminare la configurazione del router.

Vediamo adesso la configurazione del client **PPPoE su Windows XP** (le altre piattaforme Microsoft richiedono l'installazione di stack PPPoE opzionali quali RasPPPoE, Enternet o WinPoET). Per creare la connessione basta seguire i seguenti passaggi:

Dal Pannello di Controllo ciccare due volte sull'icona Connessioni di Rete.

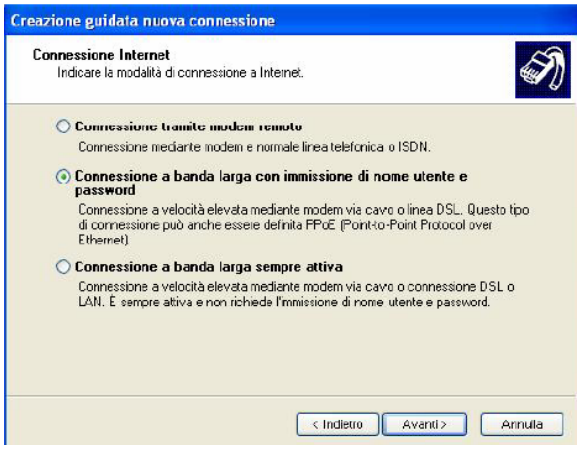
Cliccare due volte su **Crea Nuova Connessione** e poi cliccare su **Avanti**.



Entreremo nel Wizard di Windows XP, sarà , a questo punto sufficiente, selezionare la voce: **Connessione ad Internet** e poi cliccare su **Avanti.**

Al menù successivo scegliere **Imposta Connessione Manualmente** e cliccare sempre su **Avanti**.

Alla nuova richiesta, selezioniamo la seconda voce: **Connessione a Banda Larga utilizzando Nome Utente e Password** e cliccare su **Avanti**.



Indichiamo ora il nome dell'ISP e poi clicchiamo su **Avanti**.

Inserire Nome Utente e Password forniteci dall'ISP e poi cliccare su **Avanti**.

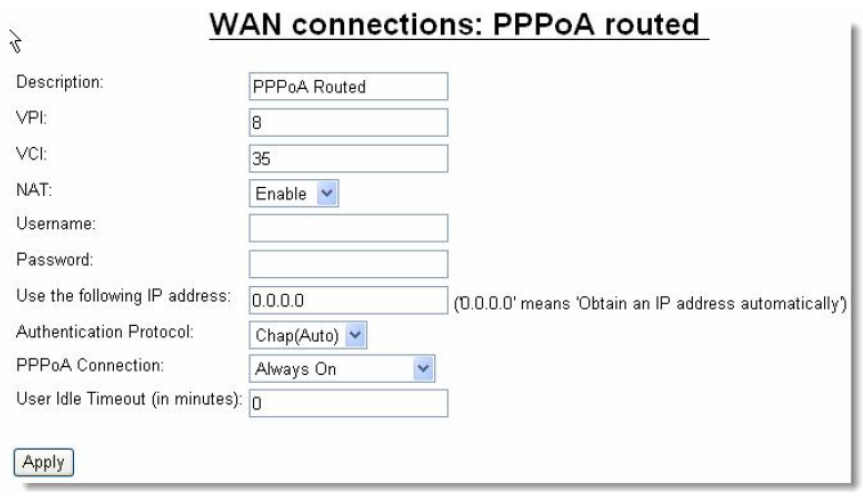
Cliccare poi su **Fine** per terminare la connessione. A questo punto cliccando sulla nuova connessione potremo navigare in Internet con IP pubblico. Resta inteso che un solo PC alla volta potrà navigare con questa particolare modalità.

Nota bene:

Mac OS X al pari di Windows XP incorpora già il client PPPoE. Si rimanda al Capitolo 3 per dettagli sulla configurazione. Per sistemi con Mac OS 9è invece necessario utilizzare un client PPPoE di terze parti, si rimanda sempre al Capitolo 3 per ulteriori informazioni.
Windows 95, 98, ME, 2000 ed NT4.0 contrariamente a Windows XP non incorporano il client PPPoE. Si rimanda al Capitolo 3 per ulteriori informazioni.

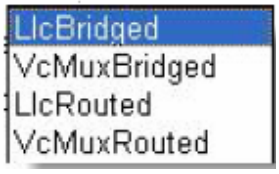
• **PPPoA Routed**

PPPoE/PPPoA sono connessioni ADSL conosciute come dial-up DSL. Sono state concepite per integrare servizi a banda larga con un'attenzione particolare alla facilità di configurazione. L'utente può beneficiare di una grande velocità di accesso senza cambiare l'idea di funzionamento, condividere lo stesso account con l'ISP.



Vediamo i parametri da configurare:
1. **VPI**=8
2. **VCI**=35
3. **NAT**: Il NAT consente a più utenti di accedere ad Internet al costo di un singolo account IP. Se gli utenti della LAN dispongono di indirizzi IP pubblici e possono pertanto accedere direttamente ad Internet (e fungere da server per determinati servizi) tale funzionalità dovrebbe essere disabilitata. Se invece l'abbonamento prevede un solo IP pubblico il NAT deve essere abilitato.

Encapsulation Method(presente solo in caso di RFC1577): Scegliere il metodo di incapsulazione utilizzato dal vostro provider. Sono disponibili:LLC Bridged, VCMux Bridged, VCMux Routed, LLC Routed.



Non vi resta che selezionare la voce **Use the following IP address ed introdurre**:
1. **IP Address**:Introdurre il vostro IP pubblico.
2. **Netmask**:Introdurre la Netmask fornitavi dall'ISP.
3. **Gateway**: Introdurre il Defaukt Gateway del Router.

Qualora invece questi dati siano forniti dal server dall'ISP in maniera automatica potete spuntare la voce **Obtain an IP address automatically via DHCP client**.
Premere **Apply** per rendere operativa la nuova configurazione. Terminata la configurazione premere su **Save Config to FLASH** (e poi su **Save**) per rendere i settaggi permanenti. Il Led PPP resterà spento.

2.8.2.2.2 DNS

Un Domain Name System (DNS) contiene una tabella di corrispondenze tra nomi di domini ed indirizzi IP pubblici. In Internet un certo sito ha un unico nome come www.yahoo.com ed un indirizzo IP. L'indirizzo IP è difficile da ricordare (però è assolutamente il modo più efficiente), certamente molto più del nome. Questo compito è svolto appunto dal DNS che grazie alla tabella incorporata riesce a fornire al PC che ne fa richiesta l'indirizzo IP corrispondente al nome del sito (e qualora non l'avesse la richiederà ad altri server DNS di

cui conosce l'IP). Gli indirizzi IP dei DNS sono forniti dall'ISP al momento in cui si effettua il LogOn (in caso si usi il PPPoA/PPPoE o RFC1483 Bridge).
Se il protocollo è RFC 1483 Routed o IpoA(RFC 1577) è necessario introdurre manualmente gli indirizzi IP dei DNS dell'ISP.

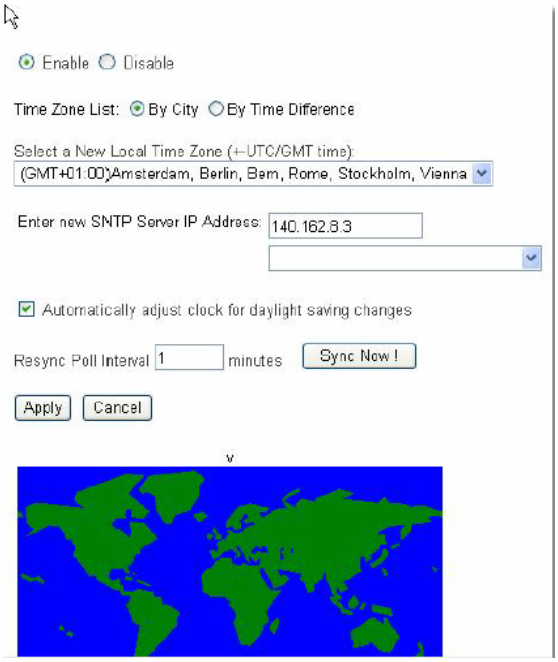
2.8.3 SYSTEM

Ciccando sul menù **Configuration** e si apriranno tutti i seguenti sottomenù:

- **TimeZone**
- **Remote Access**
- **Firmware Upgrade**
- **Backup/Restore**
- **Restart Router**
- **User Management**

2.8.3.1 Time Zone

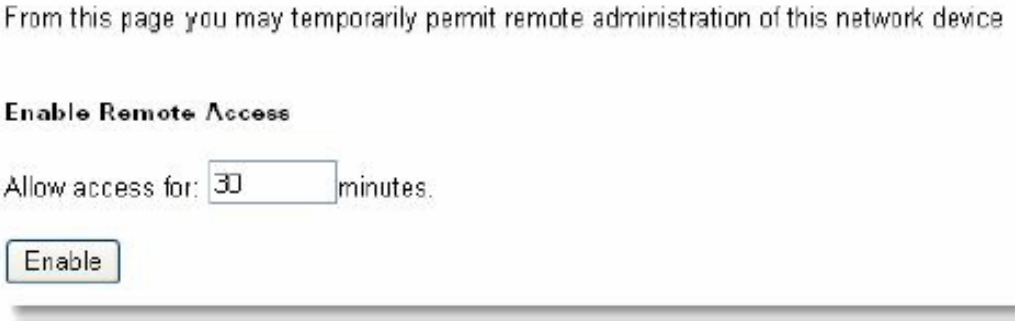
Il Router non ha un orologio al suo interno, usa il protocollo SNTP per risolvere tale inconveniente.



Anzitutto attivare tale funzionalità spuntando la scelta **Enable**. Per scegliere la zona di appartenenza sarà sufficiente selezionare il fuso di appropriato (dopo aver scelto By City o Time Difference) e scegliere nella combo box un server SNTP. Le opzioni di **Resync** permettono di stabilire l'intervallo di tempo di sincronizzazione. Premere poi il tasto **Apply** per endere effettive le scelte. É possibile ricevere, pertanto, l'ora corretta solo dopo che il collegamento ad Internet è attivo.
. É possibile controllare l'ora segnata dal Router ADSL accedendo, sotto il menù **Status** (nel Menù principale).
Cliccare sul tasto **Refresh** per aggiornare la tabella mostrata.

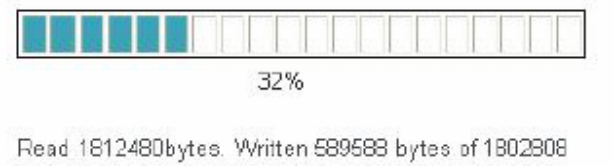
2.8.3.2 Remote Access

Attivando tale funzionalità è possibile attivare la configurazione remota dell'apparato via http:



2.8.3.3 Firmware Upgrade

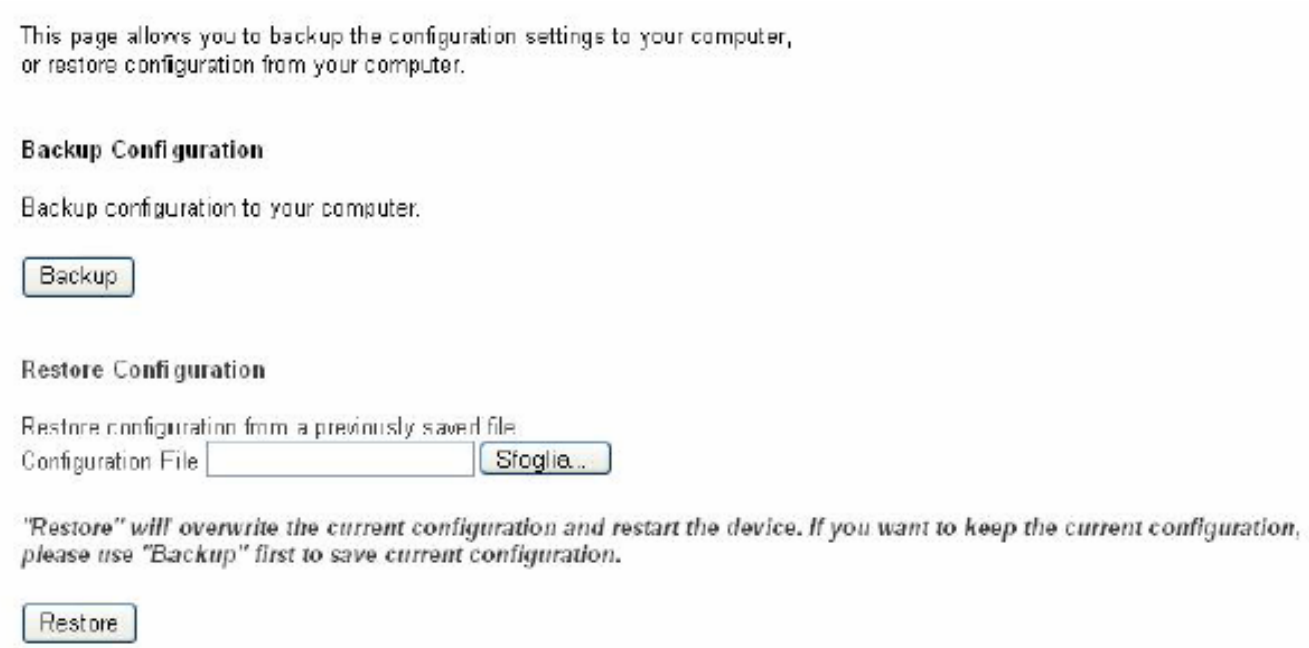
Per effettuare l'upgrade del firmware del Router ADSL è necessario anzitutto scaricare dal sito www.hamletcom.com (nella sezione opportuna) un nuovo firmware (se disponibile). Aprire il file compresso in una directory. Accedere a questo punto, sotto il menù **Configuration** e poi **System** , alla voce **Firmware Upgrade** e premere poi il tasto **Sfoglia** ed indicare la path dove si è messo il file del firmware decompresso. Premere poi sul tasto **Upgrade** per terminare l'aggiornamento. **É opportuno non staccare, durante la fase di upgrade, il Router ADSL dalla presa elettrica**.
Durante la fase di upgrade il Router indicherà lo stato di completamento della riscrittura del firmware mostrandovi un indicatore percentuale.



Completata la procedura il Router ADSL si resetterà automaticamente e inizierà a funzionare col nuovo firmware. Tutti i settaggi precedenti del Router ADSL dovrebbero essere conservati, si invita comunque ad effettuare un salvataggio della configurazione prima di procedere con l'upgrade del firmware.

2.8.3.4 Backup/Restore

Il Router Hamlet ADSL Firewall consente di effettuare un backup (ripristino) sul (dal) disco fisso del vostro PC. Grazie a questa comoda funzionalità potrete salvare complesse configurazioni e rendere nuovamente operativo il Router in pochi veloci passaggi.



Per effettuare il Backup cliccare sul bottone **Backup** (in caso venisse visualizzata una finestra di errore premere su **OK** e poi ciccare su **Here**). Non vi resta che selezionare il percorso in cui salvare i dati sulla configurazione (verrà generato un file con estensione ICF).
Per effettuare il Ripristino cliccare sul bottone **Sfoglia**, indicando il percorso dove è contenuto il file contenente la configurazione, e cliccare poi su **Restore**.

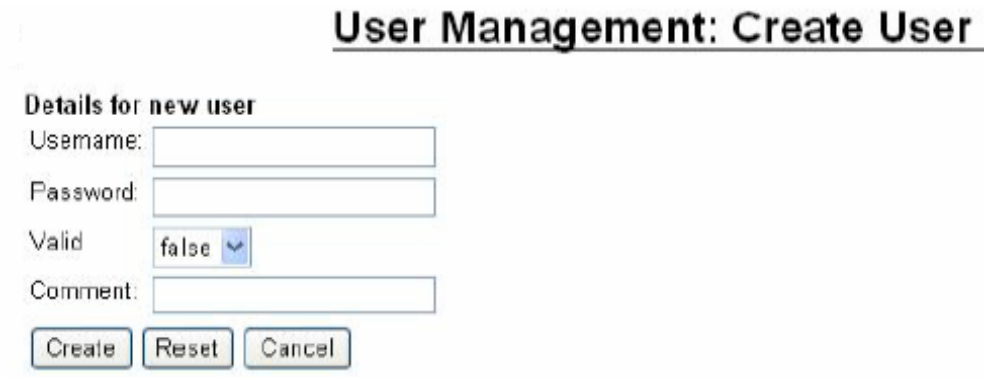
2.8.3.5 Restart Router

Se per necessità si desidera reimpostare il router ADSL con la configurazione di default (perdendo tutti i settaggi inseriti) sarà sufficiente accedere, sotto il menù **Configuration-System** alla voce **Restart Router** e spuntare la voce **Reset to factory default settings**. Premere poi il tasto **Restart Router.** Il Router effettuerà un reboot e caricherà i settaggi di default. Premendo invece il solo tasto **Restart** il router effettuerà un reboot caricando la configurazione attuale. Dopo ogni cambiamento si invita a cliccare sul bottone **Save config to Flash** per rendere permanente (e dunque salvare su eprom) il cambiamento.

2.8.3.6 User Management

É possibile creare differenti utenti che possono accedere alla configurazione del Router. Andare nel menù **Configuration-System** alla voce **User Management**, apparirà la schermata sottostante:

É possibile vedere tutti i profili abilitati o meno alla configurazione del Router. Per creare un nuovo utente premere su **Create,** apparirà la schermata sottostante in cui potrete immettere **Username** e **Password** e tramite il campo **Valid** rendere attivo o meno il nuovo utente.



Qualora non ricordaste la password di accesso è possibile riportare il Router alle condizioni iniziali eseguendo la procedura sotto riportata(si ricorda che è meglio creare un nuovo utente, provarne la password e solo adesso cancellare il vecchio utente):

Dopo che il dispositivo è acceso, premere per effettuare il reset o il restore. Le operazioni sono le seguenti:

• **0-3 secondi**: per resettare il dispositivo (ma ne conserva il contenuto salvato sulla eprom)

• **3-6 secondi**: nessuna azione

• **6 secondi o più:** effettua un ritorno alle condizioni di default

2.8.3.4 Firewall

Questa funzionalità offerta dal Router ADSL è un firewall che consente una prima valida difesa nei confronti di qualche malintenzionato di cui Internet è piena. Come già detto le funzionalità offerte, pur essendo varie ed efficaci, non sono da ritenersi “sicure” sempre e comunque. Certamente potrebbero essere considerate ampiamente soddisfacenti in molte circostanze, ma data la varietà degli attacchi e la velocità con cui questi si evolvono, si consiglia sempre di non considerarsi inattaccabili.

Qualora le informazioni custodite siano particolarmente importanti consigliamo un’attenta configurazione del firewall e magari l’uso di prodotti, a supporto, più adatti al caso.

Un utente può decidere di abilitare il firewall del Router composto sostanzialmente dalle seguenti sottosezioni:

• **General Settings/Packet Filter**

• **Intrusion Detection**

• **Mac Filter**

• **URL Filter**

Il firewall presente nel Router opera su 2 differenti livelli:

1. Anzitutto previene dagli accessi indesiderati dall’esterno della LAN. Questo è fatto su 3 livelli:

• **NAT**: quando abilitato (sempre, escluso il caso di classe pubblica) tutti i PC della LAN sono visti dall’esterno come un unico indirizzo IP. É molto più difficile pertanto per un hacker accedere alla singola macchina.

• **General Settings/Packet Filter**: É possibile filtrare per pacchetto e protocollo tutto quello che entra verso la LAN e far effettivamente passare solo il traffico ritenuto sicuro.

• **Intrusion Detection:** questa sezione si occupa di effettuare una difesa attiva contro ogni tipo di attacco DoS, Port Scan utilizzando, al fine di ridurre l'efficacia di questi attacchi, una blacklist dinamica. Ogni tentativo di attacco è memorizzato in un file di Log.

2. Previene inoltre gli accessi dalla LAN locale.
   • **General Settings/Packet Filter:** É possibile filtrare per pacchetto e protocollo tutto quello che esce verso Internet e far effettivamente passare solo il traffico ritenuto sicuro.
   • **MAC Filter rules:** consente l'accesso verso Internet di tutti e soli i MAC address desiderati (o impedisce l'accesso ad una lista)
   • **URL Filter**: permette di bloccare l'accesso a determinati siti É consigliabile visitare periodicamente il sito (www.hamletcom.com) al fine di reperire l'ultimo Firmware che potrebbe migliorare le caratteristiche del firewall.

2.8.3.4.1 General Settingf/Packet /Filter

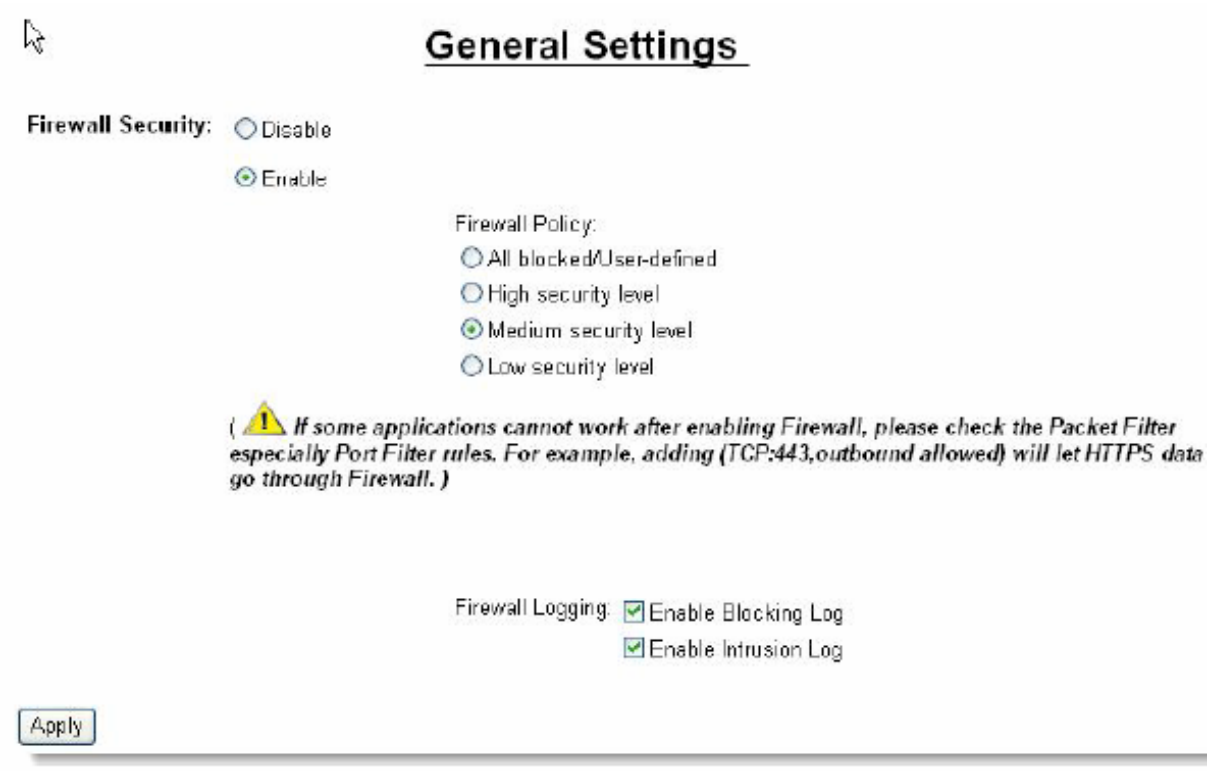
Queste funzioni di filtraggio dei pacchetti IP sono in buona sostanza una serie di regole che il Router ADSL applicherà ai pacchetti IP che lo attraversano e stabilirà o meno il soddisfacimento di queste regole, pacchetto per pacchetto. É utile comunque sapere che il solo filtraggio sui pacchetti non elimina i problemi legati a livello di applicazioni o altri livelli. Le politiche con cui organizzare un filtraggio sono essenzialmente riassumibili in **due posizioni**:

1. **Blocco ciò che conosco come pericoloso e consento il passaggio del resto:** Tale posizione dovrebbe essere applicata da coloro che possiedono una discreta conoscenza di Internet.
   Richiede la conoscenza dei pericoli da filtrare opportunamente e consente, nella maggior parte dei casi, di non imbattersi in decine di applicazioni che hanno problemi perché mal configurate (con questa filosofia si blocca solo il pericolo).
2. **Passa solo quello che ritengo sicuro il resto è bloccato:**Tale posizione dovrebbe essere applicata da coloro che possiedono una buona conoscenza di Internet in quanto è necessario creare una regola per ogni "servizio" che si vuole usare. É certamente più sicura ma richiede una maggiore conoscenza delle problematiche ed una più lunga preparazione delle regole dei filtri (che possono essere moltissimi).

Una volta realizzate le regole che determinano il modo in cui avviene il filtraggio dei pacchetti IP è opportuno **verificare la sicurezza del sistema**. Questo è realizzabile in diverse modalità:

• **Sito specializzato**:In questo caso è possibile ottenere un primo risultato visitando il sito http://www.dslreports.com (ve ne sono ovviamente moltissimi altri) e accedendo alla sezione DSLR Tools ed infine scegliere Port-Scan. I risultati possibili, per ogni porta controllata, possono essere 3 (open:la porta è in ascolto e dietro c'è un servizio che accetta le connessioni, closed:la porta rifiuta la connessione e non è dato sapere se c'è un servizio dietro, stealth: la porta non risponde alla richiesta di connessione)
• **PC esterno alla vostra LAN**:In questo modo potete provare i vostri filtri.

Vediamo nel dettaglio come configurare la sezione General Settings/Packet Filter.



Anzitutto è necessario abilitare il Firewall spuntando Enable.
É possibile scegliere tra 4 possibili selezioni:

- **All blocked/User-defined**: non è definito nulla. Tutto il traffico sia entrante che uscente è bloccato. L'utente deve configurare le proprie regole nella sezione **Packet Filter**.
- **High/Medium/Low security level**: sono definiti tutta una serie di impostazioni preconfigurate modificabili che permettono un uso immediato. A seconda del grado di protezione scelto determinati servizi saranno o meno abilitati.

Selezionando le voci **Enable Blocking Log** e **Enable Intrusion Log** è possibile avere dei Log dettagliati di ciò che il firewall sta facendo. É possibile controllare questi Log nella sezione **Status- Event Log**.

Vediamo nel dettaglio le impostazioni preconfigurate.
Come già detto scegliendo il livello di sicurezza tra **High/medium e Low** non facciamo altro che caricare una matrice di regole di volta in volta meno stringente.

Application	Protocol	Port Number	Firewall (High)	Firewall(Medium)	Firewall (Low)

		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	53	53	NO	YES	NO	YES	YES	YES
DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	YES	YES
FTP(21)	TCP(6)	21	21	NO	NO	NO	YES	NO	YES
Telnet(23)	TCP(6)	23	23	NO	NO	NO	YES	NO	YES
SMTP(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS(119)	TCP(6)	119	119	NO	NO	NO	YES	NO	YES
RealAudio (7070)	UDP(17)	7070	7070	NO	NO	YES	YES	YES	YES
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	NO	NO	NO	YES	YES	YES
T.120(1503)	TCP(6)	1503	1503	NO	NO	NO	YES	YES	YES
SSH(22)	TCP(6)	22	22	NO	NO	NO	YES	YES	YES
NTP(123)	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTPS(443)	TCP(6)	443	443	NO	NO	NO	YES	NO	YES

Si ricorda che tutto il traffico non contemplato nel set di regole viene scartato. É comunque possibile aggiungere o modificare le regole al fine di ottenere un firewall che soddisfi particolari esigenze. Per esempio dopo aver scelto il firewall con impostazione di sicurezza HIGH, tra le altre cose il Router non risponderà ai Ping provenienti dall'esterno nè consente lo scaricamento via FTP di file dalla rete. Per modificare questa situazione è sufficiente accedere alla sezione **Configuration, Firewall, Racket Filter.** Apparirà l'immagine sottostante.

Type	Configuration		Note
external < > internal	Port Filters...	Address Filters...	1. By default, all protocol types and TCP/UDP ports are blocked. 2. Only the listed IP addresses are blocked

A questo punto cliccare su **Address Filters** per bloccare determinati IP o **Port Filters** per entrare nel dettaglio delle regole.

Port Filters

Type	Start Port	End Port	Inbound	Outbound		
TCP	80	80	Block	Allow	Edit...	Delete...
UDP	53	53	Block	Allow	Edit...	Delete...
TCP	53	53	Block	Allow	Edit...	Delete...
TCP	21	21	Block	Block	Edit...	Delete...
TCP	23	23	Block	Block	Edit...	Delete...
TCP	25	25	Block	Allow	Edit...	Delete...
TCP	110	110	Block	Allow	Edit...	Delete...
TCP	119	119	Block	Block	Edit...	Delete...
UDP	7070	7070	Block	Block	Edit...	Delete...
ICMP	N/A	N/A	Block	Allow	Edit...	Delete...
TCP	1720	1720	Block	Block	Edit...	Delete...
TCP	1503	1503	Block	Block	Edit...	Delete...
TCP	22	22	Block	Block	Edit...	Delete...
UDP	123	123	Block	Allow	Edit...	Delete...

Non resta che modificare (premendo **Edit**) la regola in questione. Nel nostro caso, per la regola ICMP, è sufficiente rendere possibile il traffico in ingresso per consentire al router di rispondere (dato che il traffico ICMP in uscita è già consentito). In maniera identica per l'FTP sceglieremo la regola opportuna e renderemo il traffico in uscita possibile.
In figura è possibile osservare adesso il nuovo insieme di regole.

Port Filters

Type	Start Port	End Port	Inbound	Outbound		
TCP	80	80	Block	Allow	Edit...	Delete...
UDP	53	53	Block	Allow	Edit...	Delete...
TCP	53	53	Block	Allow	Edit...	Delete...
TCP	21	21	Block	Allow	Edit...	Delete...
TCP	23	23	Block	Block	Edit...	Delete...
TCP	25	25	Block	Allow	Edit...	Delete...
TCP	110	110	Block	Allow	Edit...	Delete...
TCP	119	119	Block	Block	Edit...	Delete...
UDP	7070	7070	Block	Block	Edit...	Delete...
ICMP	N/A	N/A	Allow	Allow	Edit...	Delete...
TCP	1720	1720	Block	Block	Edit...	Delete...
TCP	1503	1503	Block	Block	Edit...	Delete...
TCP	22	22	Block	Block	Edit...	Delete...
UDP	123	123	Block	Allow	Edit...	Delete...

Cliccando su **Delete** invece l'intera regola viene eliminata e tutto il traffico che la riguarda viene scartato. Per aggiungere invece regole nuove è possibile cliccare sulle voci opportune (sotto la tabella) :

Add TCP Filter...

Add UDP Filter...

Add Raw IP Filter...

Scegliendo **Add TCP Filter** è possibile aggiungere regole che utilizzino il protocollo TCP (Scegliendo **Add UDP Filter** è possibile aggiungere regole che utilizzino il protocollo UDP, Scegliendo **Add RAW IP Filter** è possibile aggiungere protocolli). Vediamo alcuni protocolli contenuti nel pacchetto IP:

- **TCP** (Transmission Control Protocol) Tale protocollo fornisce un servizio di comunicazione basato sulla connessione (al contrario dell'IP e UDP). Tale servizio è affidabile. Vengono utilizzate le porte di origine e destinazione (interi di 16 bit). É usato moltissimo specie per Telnet (porta 23), FTP (porta 20 e 21), http (porta 80), SMTP e POP3 (porta 25 e 110).
- **UDP** (User Datagram Protocol) Tale protocollo fornisce un servizio di comunicazione non basato sulla connessione (come dell'IP). Tale servizio è più veloce del TCP sebbene meno sicuro. Vengono utilizzate le porte di origine e destinazione (interi di 16 bit). É utilizzato per interrogare i DNS.
- **ICMP** (Internet Control Message Protocol) Viene usato per notificare al mittente eventuali problemi legati ai datagrammi IP. I principali messaggi dell'ICMP sono: **Destination Unreachable** (l'host non è raggiungibile e pertanto il pacchetto non sarà consegnato), **Echo Reply ed Echo Request** (usati per verificare la raggiungibilità di alcuni host nella rete), **Parameter Problem** (indica che un Router che ha esaminato il pacchetto ha rilevato un qualche problema nell'intestazione), **Redirect** (usato da un

host o un Router per avvisare il mittente che i pacchetti dovrebbero essere inviati ad un altro indirizzo), **Source Quench** (inviato da un Router congestionato al mittente per informarlo dello stato), **Timestamp e Timestamp Reply** (simili ai messaggi di Echo, ma aggiungono l'orario) **TTL Exceeded** (il campo TTL è sceso a zero, dunque il pacchetto è stato scartato e ne viene informato il mittente).

Scegliendo invece **All blocked/User-defined** dovrete necessariamente creare un set di regole ex novo, infatti con questa selezione tutto il traffico, tanto entrante che uscente, viene scartato.

2.8.4.2 Intrusion Detection

Il Router può automaticamente riconoscere e bloccare un attacco di tipo DoS (Denial of Service) o Port Scan se la funzione di Intrusion Detection è attiva. Lo scopo di attacchi appartenenti a questa tipologia non è quello di cogliere informazioni particolari dalla vostra rete quanto piuttosto renderla inutilizzabile per un certo periodo di tempo. Il Firewall inoltre supporta la funzionalità Blacklist per minimizzare l'efficacia degli attacchi. La Blacklist è vuota nel momento dell'attivazione del Firewall. Quando il router si accorge di essere stato attaccato memorizza nella blacklist l'IP da cui proviene l'attacco. L'IP di ogni pacchetto ricevuto dal router, prima di essere processato, viene confrontato con quelli presenti nella blacklist (e se presente viene scartato). A seconda del tipo di attacco, l'IP verrà mantenuto « inattivo » per un determinato periodo di tempo (scaduto il quale verrà cancellato dalla Blacklist).

Vediamo nel dettaglio le tipologie di attacchi DoS.

- Attacchi che mirano all'esaurimento della banda, sono realizzabili in due modalità diverse a seconda di quanta banda abbia l'attaccante. Qualora la banda sia maggiore dell'attaccato può saturarlo diversamente, altrimenti può usare altri host che di fatto amplificano l'attacco.
- Attacchi che mirano all'esaurimento delle risorse.
- Attacchi contro difetti di programmazione, che mirano a sfruttare bug software o hardware.
- Attacchi DoS generici.

Vengono riconosciuti diversi tipi diversi di patterns tra i quali:

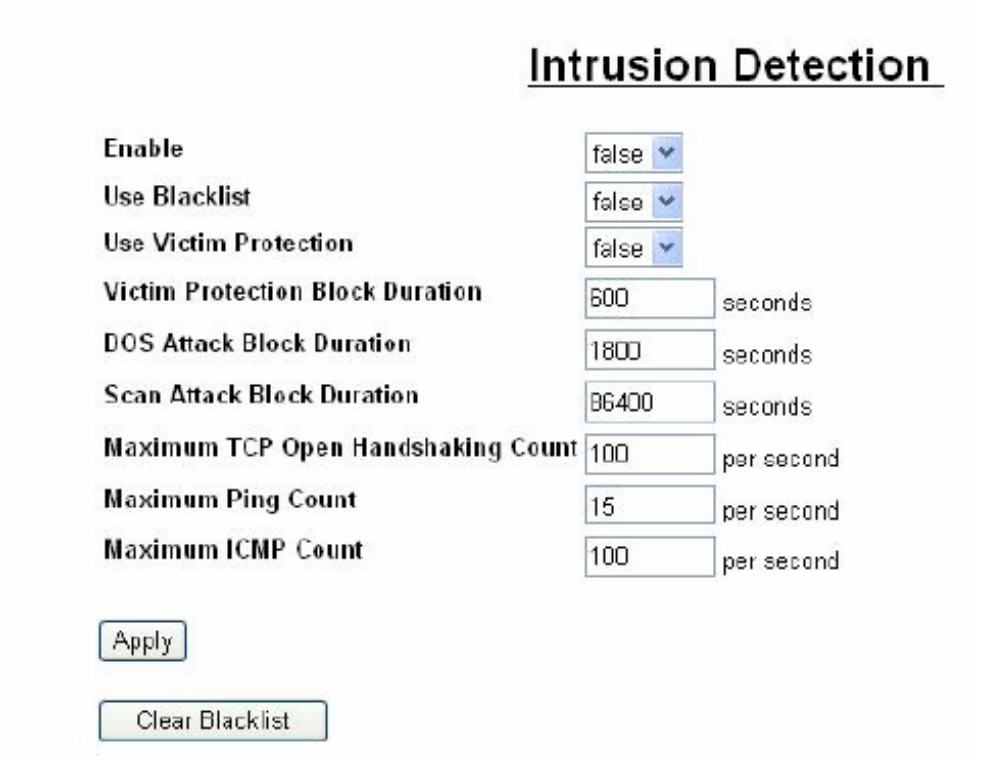
- IP Spoofing
- Ping of Death (Length > 65535)
- Land Attack (Same source / destination IP address)
- IP with zero length
- Sync flooding
- Smurf Attack (ICMP Echo with x.x.x.0 or x.x.x.255)
- Snork Attack
- UDP port loop-back
- TCP NULL scan
- TCP XMAS Scan
- WinNuke Attack
- TCP SYN Flooding
- Ascend Kill
- IMAP SYN/FIN scan
- Net Bus scan
- Back Orifice scan

Segue una breve descrizione del funzionamento degli attacchi più comuni.

- **IP Spoofing** è un attacco particolare in cui l'attaccante cerca di intromettersi in una connessione con lo scopo di abbatterla o di prenderne il controllo. Può essere fatto sia dall'interno della propria LAN (con possibilità più alte di successo se si dispone di LAN con HUB) che da Internet con possibilità di successo infinitamente inferiori. Grazie al SPI il Router esamina a fondo i pacchetti che lo attraversano e confrontando molti parametri coi pacchetti precedenti della stessa connessione riesce a stabilire con efficacia se un pacchetto in arrivo è "spoofato" o meno.
- **Sync Flood**, come già accennato è un attacco che mira a esaurire le risorse del sistema che lo subisce. All'atto dell'instaurazione di una connessione viene spedito un pacchetto (dall'attaccante) col quale si avvisa che si vuole costruire la connessione. Il ricevente, cioè l'attaccato, alloca delle risorse e risponde con un pacchetto per proseguire la creazione della connessione. L'attaccato aspetta pazientemente il pacchetto di risposta (che non arriverà mai poiché l'attaccante avrà scelto o un IP di un host spento oppure starà attaccando l'host in questione impedendogli di rispondere). Le risorse allocate saranno bloccate sino a che non scade il timer associato. Nel frattempo l'attaccante ripeterà quest'attacco finendo col bloccare tutte le risorse disponibili nell'attaccato. Il firewall integrato nel Router Hamlet ADSL Firewall riconosce il tentativo di apertura di diverse connessioni provenienti dallo stesso IP e non allocherà le risorse. Certamente, a meno di trovarsi con sprovveduti, l'IP che verrà registrato nella tabella del sicurity logs non apparterrà all'attaccante.
- **Smurf Attack**, tenta invece di esaurire l'intera banda dell'host vittima, per fare questo può (a seconda della velocità della sua connessione) sfruttare anche delle sottoreti che fungono da amplificatore. Infatti l'indirizzo di broadcast di queste sottoreti vieni sfruttato e così tutti gli host di questa sottorete rispondono all'Echo Request richiesto dall'attaccante che avrà sostituito l'IP del mittente con quello dell'attaccato. All'attaccato tutti gli host risponderanno col pacchetto di Echo Reply generando un traffico intensissimo. Il Router Hamlet ADSL Firewall filtra i pacchetti di Echo Reply in uscita trattandolo come un attacco.
- **Ping of Death**, quest'attacco particolare e dalle conseguenze variabili (anche a seconda del carico della macchina) viene generato creando un pacchetto ICMP di Echo Request fuori standard. Il pacchetto IP può infatti essere lungo, dalle spefiche RFC, al massimo 65536 bytes di cui 20 sono riservati per l'header. Entro il Payload vengono inseriti i pacchetti di livello superiore, in questo caso l'ICMP (oppure TCP, UDP) che ha un header lungo 8 bytes. La lunghezza massima per il Payload del pacchetto ICMP è dunque 65535-20-8=60507 bytes. Sebbene un pacchetto del genere sia fuori specifica è comunque realizzabile, inoltre arriva frammentato alla destinazione (l'attaccato) dove verrà ricomposto (non verificandolo prima) ma a questo punto potrebbe generare un overflow dello stato di alcune variabili. Il firewall integrato si accorge di questo tipo di attacco e scarta il pacchetto in questione, aggiornando la tabella del security logs.
- **LANd Attack**, sfrutta un errore presente in molti Sistemi operativi o Router che quando ricevono un particolare pacchetto (il cui IP di provenienza è uguale a quello di destinazione, cioè l'attaccato) di richiesta di connessione tentano di stabilirla ma vanno incontro ai più diversi blocchi. In pratica l'attaccato cerca di colloquiare con se stesso. Il Router Hamlet ADSL Firewall elimina tutti i pacchetti con questa caratteristica.

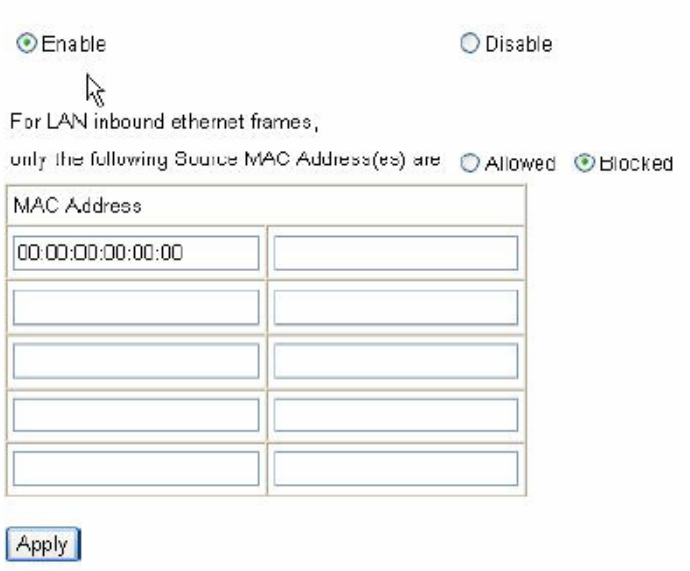
Vediamo come attivare e configurare la funzionalità di **Intrusion Detection**.

- **Enable**: selezionare True per rendere attiva l'Intrusion Detection.
- **Use Blacklist**: selezionare True per rendere attiva la Blacklist. Se abilitata tutti gli IP di provenienza degli attacchi vengono memorizzati.
- **Use Victim Protection**: selezionare True per utilizzare la funzionalità Victim Protection. Il Router proteggerà gli host interni da attacchi sospetti.
- **Victim Protection Duration**: una volta che il Router stabilisce che un host è stato attaccato, blocca ogni tipo di accesso all'host (nel tentativo di proteggerlo) per il tempo stabilito.
- **DoS Attack Block Duration**: dopo che un attacco di tipo DoS è stato rilevato, il router blocca il traffico dall'host esterno (il cui IP èstato inserito nella blacklist) per un intervallo di tempo stabilito.
- **Scan Attack Block Duration:** una volta determinato un attacco di tipo Scan, il router blocca il traffico dall'host esterno (il cui IP èstato inserito nella blacklist) per un intervallo di tempo stabilito.
- **Maximum TCP Open Handshaking Count**: stabilisce il massimo numero si sessioni TCP aperte (in fase di handshaking) per secondo. Qualora questo numero venga raggiunto il router considera questo come un attacco **SYN Flood**.
- **Maximum Ping Count:** stabilisce il massimo numero pacchetti tipo PING per secondo. Qualora questo numero venga raggiunto il router considera questo come un attacco **ECHO Storm.**
- **Maximum ICMP Count:** stabilisce il massimo numero pacchetti tipo ICMP per secondo. Qualora questo numero venga raggiunto il router considera questo come un attacco **ICMP Flood.**



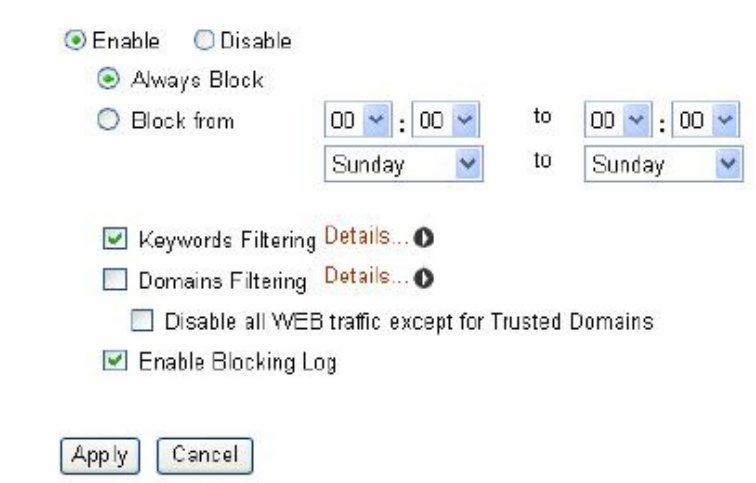
2.8.4.3 MAC Address Filter

Tramite questa funzionalità è possibile filtrare ulteriormente il traffico limitando l'accesso in base all'indirizzo MAC degli apparati di rete. Sarà possibile bloccare l'accesso ad una lista di MAC Address oppure consentire l'accesso solo ad una listadi MAC Address.
Per attivare questa funzionalità anzitutto spuntare la voce **Enable** (come da figura), scegliere la modalità operativa:
Allowed=per consentire solo ai MAC appartenenti alla lista l'accesso
Blocked=per consentire l'accesso a tutti esclusi i MAC appartenente alla lista



2.8.4.4 URL Filter

Tramite questa funzionalità è possibile filtrare ulteriormente il traffico in uscita limitando tale traffico in base all'ora e/o giorno ed al tipo di URL. Sarà possibile bloccare l'accesso ad alcuni siti oppure consentire l'accesso solo ad una lista opportuna di siti. É inoltre possibile impedire l'accesso ad alcuni URL che hanno una determinata sequenza di caratteri.
Per attivare questa funzionalità anzitutto spuntare la voce **Enable** (come da figura).



Scegliendo l'opzione **Always Block** le regole di filtraggio verranno applicate sempre, nel caso invece si scelga **Block From** è possibile limitare, in base al giorno e all'ora l'utilizzo dei filtraggi. Spuntando la voce Enable Blocking Log è possibile avere un LOG aggiornato di tutte le azioni del Firewall (nella sezione **Status- Event Log**).
Selezionando **Keywords Filtering** (e premendo poi **Details**) è possibile limitare l'accesso a tutti gli URL contenenti la parola specificata. Ad esempio immettendo "**.it**" è possibile bloccare tutti e soli i siti con estensione it.
Selezionando **Domains Filtering** (e premendo poi **Details**) è possibile limitare l'accesso a tutti e soli gli URL specificati o creare una lista vietata. É possibile infatti creare una lista di siti vietati (da mettere in **Forbidden Domain**), oppure consentire l'accesso a solo un limitato numero di siti (da mettere in **Trusted Domain** e spuntare la voce **Disabile all Web traffic except for Trusted Domain**). In questo modo potrete limitare l'accesso ai soli siti che ritenete opportuni e controllare comunque in **Status Event Log** tutti i tentativi di violazione dell'URL **Filtering**.

2.8.5 VPN

Le Virtual Private Network consentono di mettere in comunicazione due o più LAN fisicamente distinte attraverso Internet, garantendo la riservatezza delle informazioni tramite meccanismi di autenticazione e crittografia. Questo è reso possibile da un insieme di tecnologie che permettono la creazione di un "Tunnel" tra le sedi remote. Il "Tunneling" è il processo di incapsulamento dei pacchetti provenienti dalla rete locale in altri pacchetti, che attraversano la rete pubblica, in grado di nasconderne le informazioni contenute. Il router A02-RA3 integra due differenti tipologie di VPN in grado di garantire la massima versatilità di utilizzo di tale tecnologia:

PPTP
Il protocollo PPTP è stato progettato per consentire comunicazioni autenticate e crittografate tra due host, presenta come caratterisiche principali semplicità di installazione e di gestione. Il protocollo PPTP (Point-to-Point Tunneling Protocol) utilizza una connessione TCP per la gestione del tunnel e frame PPP incapsulati GRE (Generic Routing Encapsulation) per i dati sottoposti a tunneling, fornendo la possibilità di crittare e comprimere il *payload* dei pacchetti. Il router A02-RA3 permette utilizzare questo protocollo in due differenti modalita:

- **REMOTE ACCESS:** permette di avere accesso alla rete locale da una postazione remota tramite un client PPTP software (Dial-In) oppure di accedere ad un server PPTP tramite il client contenuto nel router (Dial-Out)
- **LAN-TO-LAN:** permette di mettere in comunicazione due LAN distinte tramite due router creando una VPN basata su protocollo PPTP

IPSec
L' IPSec è un insieme di protocolli basati su avanzate tecnologie di criptazione per fornire servizi di autenticazione e confidenzialità tra host che comunicano attraverso una rete pubblica consentendo la creazione di VPN. I protocolli principali che costituiscono IPSec sono tre:

- ***AH*** **(Authentication Header):** utilizzato per fornire autenticazione e integrità ai pacchetti
- ***ESP*** **(Encapsulating Security Payload):** fornisce integrità e segretezza
- ***IKE*** **(Internet Key Exchange):** gestisce lo scambio delle chiavi

Questi protocolli operano sotto le indicazioni di una SA (Security Association) ossia una sorta di tabella che contiene le informazioni sugli algoritmi e le chiavi utilizzati per proteggere il traffico che attraversa la VPN. Le SA sono unidirezionali, ogni host che partecipa alla VPN deve averne una impostata. Lo standard IPSec supporta due modalità operative differenti:

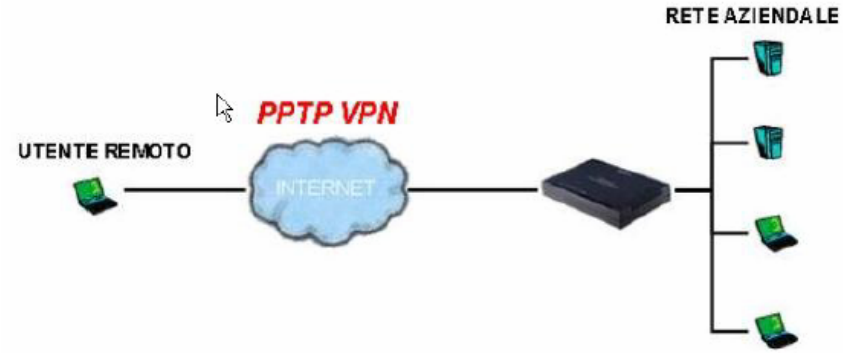
- **TRANSPORT MODE:** L'header del pacchetto IP viene lasciato inalterato, viene quindi preso in considerazione dagli algoritmi di criptaggio solo il payload del pacchetto stesso. Questo garantisce un livello di protezione minima delle informazioni perché è possibile scoprire mittente e destinatario dei dati.
- **TUNNELL MODE:** L'intero pacchetto IP viene criptato divenendo a sua volta il payload di un nuovo pacchetto dotato di un nuovo header che conterrà nei campi IP sorgente e IP di destinazione gli indirizzi dei due estremi della VPN.

ESEMPI DI CONFIGURAZIONE

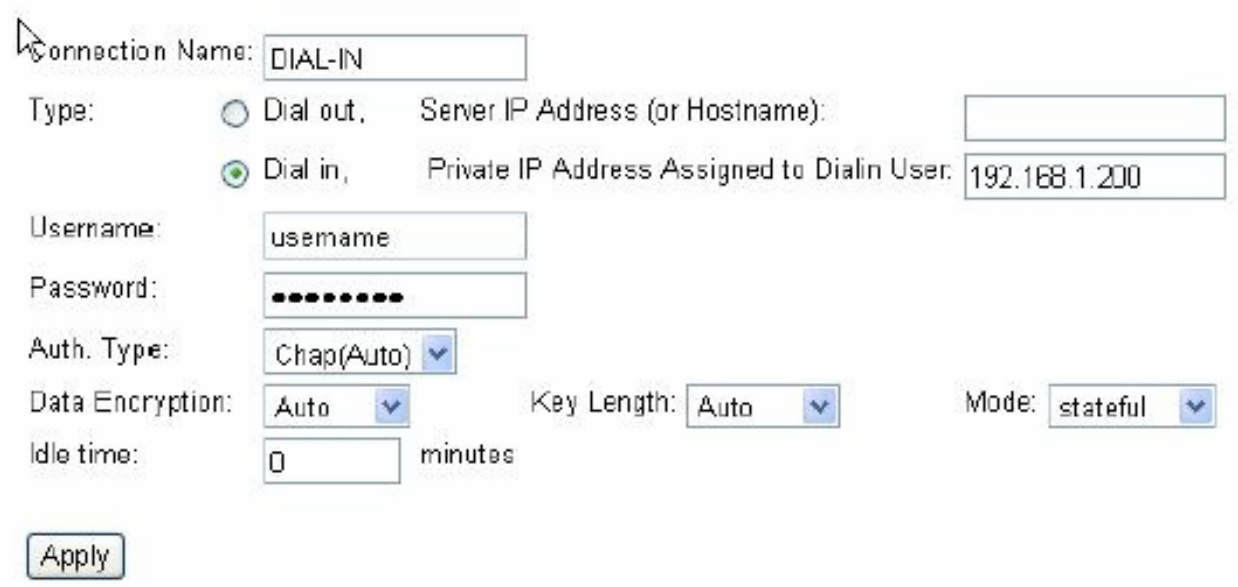
In questa sezione verranno descritti alcuni scenari comuni di implementazioni VPN PPTP/IPSec

2.8.5.1 PPTP VPN – Remote Access (Dial-In)

In questo scenario un utente remoto deve accedere alla rete aziendale utilizzando un PC collegato ad internet per mezzo di un modem. Verrà quindi configurato un account VPN PPTP – Remote Access (Dial-In), l'utente si connetterà al router utilizzando il client VPN-PPTP contenuto in tutti i sistemi operativi Microsoft attualmente in commercio (l'esempio riporta una configurazione con sistema operativo XP). Alla postazione remota verrà assegnato un indirizzo IP come se si trattasse di una macchina interna alla rete, potrà quindi attingere dalle risorse della rete aziendale e condividere a sua volta servizi e risorse. La figura che segue riassume quanto detto.

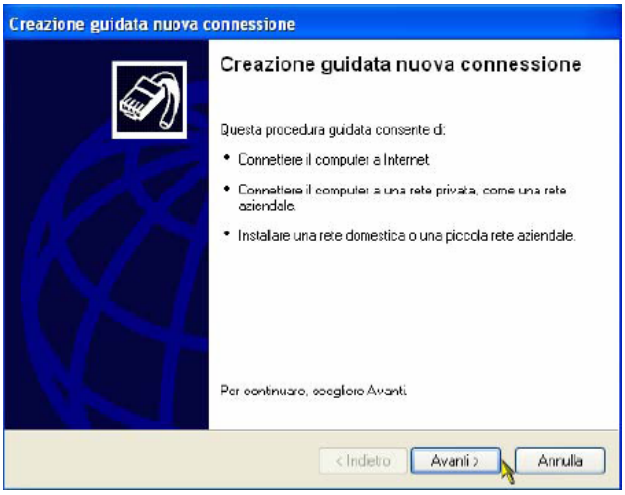


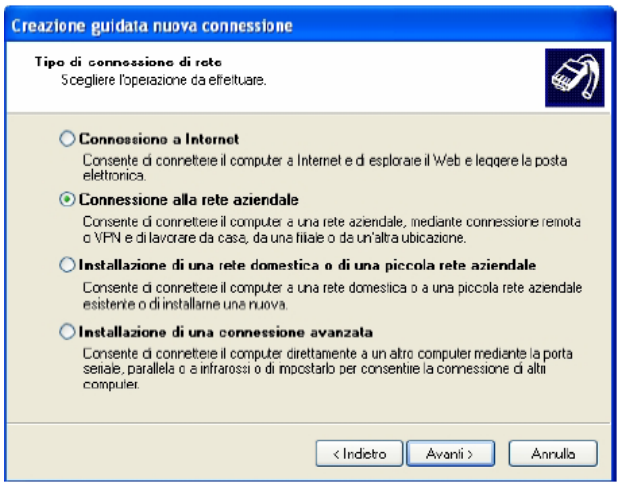
Per configurare il router per la modalità VPN PPTP – Remote Access (Dial-In) è necessario accedere all'interfaccia web di configurazione, cliccare sulla voce **Configuration** del menù, poi sulla voce **VPN** e selezionare quindi la voce **PPTP**. Nella parte destra della pagina di configurazione cliccare sulla voce **Create** e alla successiva schermata su **Remote Access**. Cliccare quindi sul pulsante **NEXT** per accedere alla pagina **PPTP Remote Access Connection**.

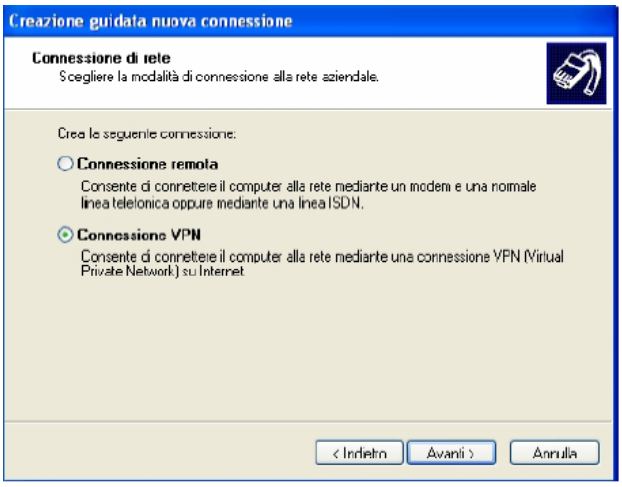


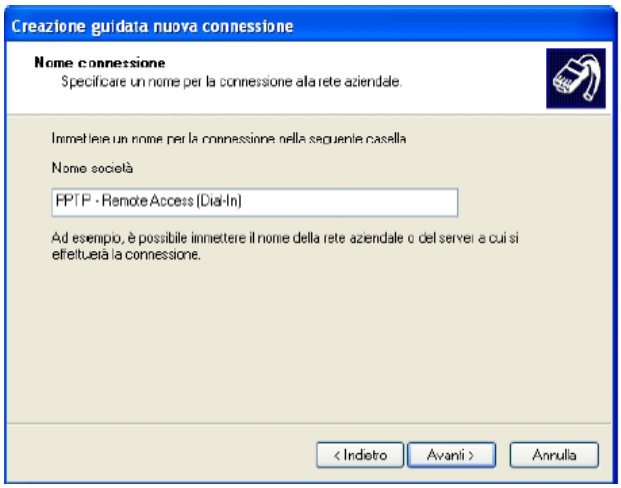
Inserire nel campo **Connection Name** una nome che identifichi la connessione, selezionare **Dial-In** come tipologia di connessione e inserire l'IP che verrà assegnato all'host remoto una volta proiettato nella LAN. Inserire quindi **Username** e **Password** con i quali l'utente remoto accederà al servizio e cliccare sul pulsante **Apply** per applicare le modifiche. La nuova connessione viene automaticamente impostata come **Disable** selezionare quindi la voce **Enable** cliccare sul pulsante **Apply** e salvarla cliccando sulla voce del menù **Save config to flash** seguito da lpulsante **Save**. Per modificare la nuova connessione è necessario spostare lo stato da **Enable** a **Disable** e cliccare su **Apply**, il comando **Edit** sarà quindi attivato.

Vediamo ora come configurare il PC in modo da accedere alla rete aziendale tramite PPTP. Anzitutto cliccare sull'icona Connessione di rete contenuta nel pannello di controllo. Poi scegliere la voce "Crea nuova connessione", premere poi avanti ed effettuare le scelte come nelle figure che seguono.

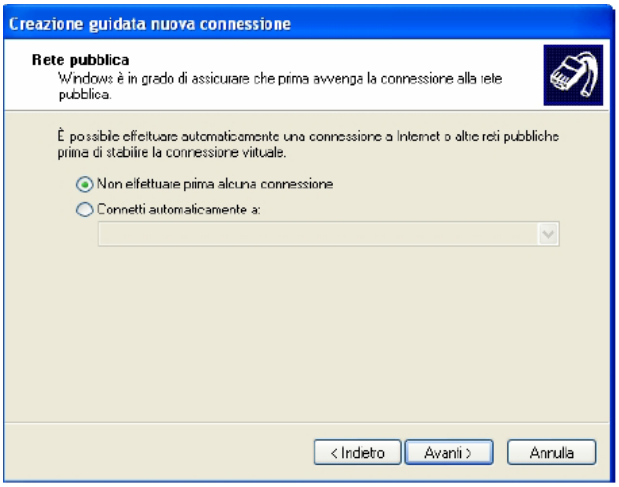


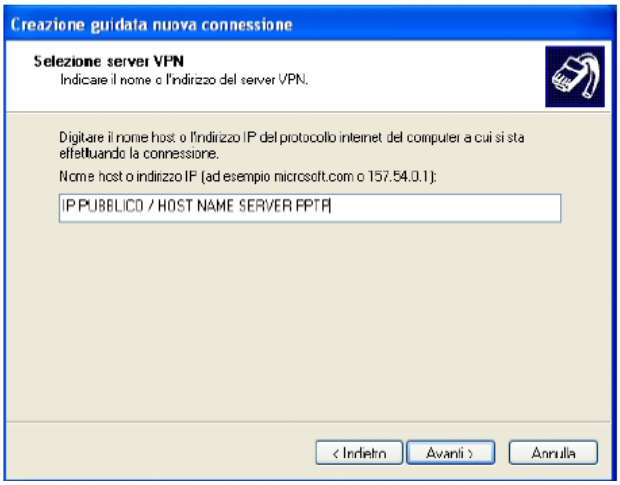




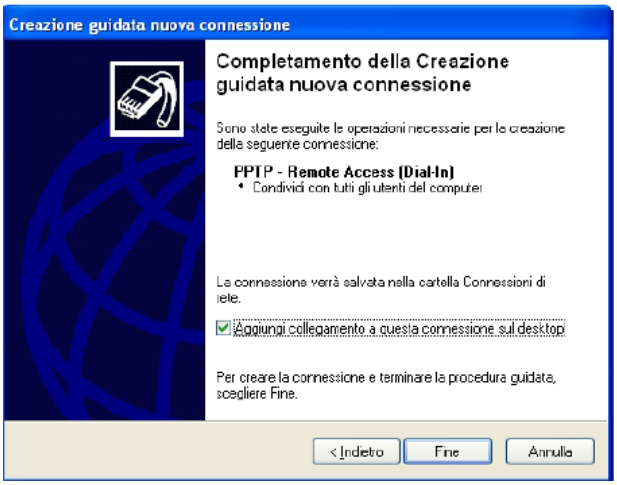


Se non si dispone di una connessione ad Internet sempre attiva sarà necessario selezionare quale connessione lanciare per raggiungere il router remoto.





Se il router remoto non dovesse disporre di un indirizzo IP statico è possibile ottenere un “Nome Host” tramite il servizio **Dynamic DNS**. Per ulteriori dettagli sul servizio fare riferimento alla “Dynami DNS” di questo manuale.



Verrà quindi creata sul desktop un'icona che permette di lanciare la connessione PPTP verso il router A02-RA3, cliccare sull'icona. Inserire **Nome Utente** e **Password** precedentemente impostati nella configurazione VPN PPTP del router e cliccare su **Connetti**. Ora il PC è all'interno della LAN aziendale.
É possibile **verificare lo stato della connessione PPTP cliccando sulla voce Status del menù e poi sulla voce PPTP Status**, la figura che segue ne riporta un esempio.

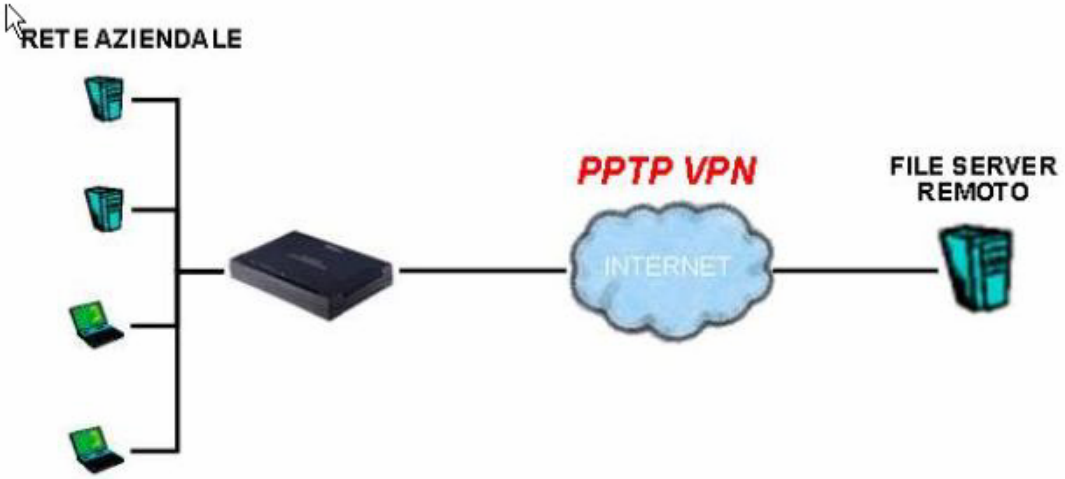
VPN/PPTP for Remote Access Application

Name	Type	Enable	Active	Session Connected	Call Connected	Encryption
PPTP	dialin	✓	✓	✓	✓	encryption enabled mppe 128bits stateful mode

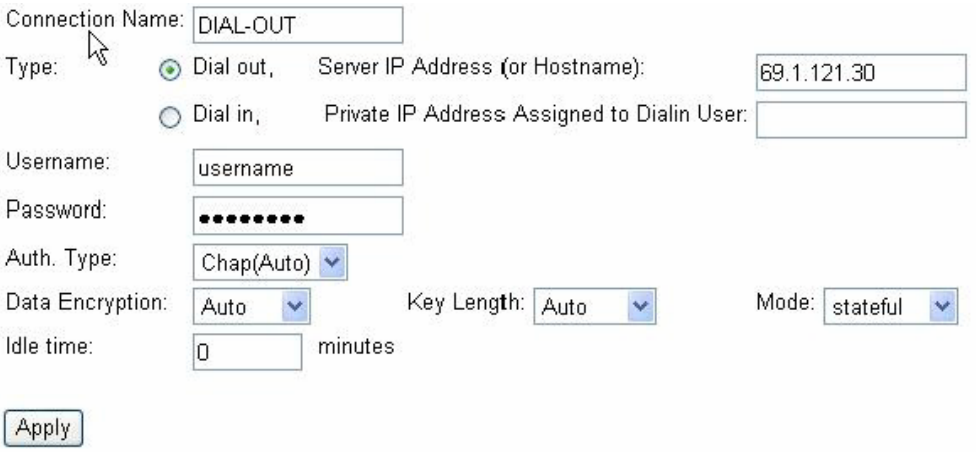
Qualora si dovessero verificare problemi durante la creazione della sessione VPN con il router, verificare nelle proprietà della connessione PPTP sotto la voce **Rete** che il campo **Tipo di VPN** sia impostato sul valore **PPTP VPN**.

2.8.5.2 PPTP VPN – Remote Access (Dial-Out)

In questo scenario gli utenti di una LAN devono accedere ai dati contenuti in un File Server remoto il quale integra un PPTP Server per la trasmissione crittata dei dati alle sedi remote. La figura che segue riassume quanto detto.



Per configurare il router per la modalità VPN PPTP – Remote Access (Dial-Out) è necessario accedere all'interfaccia web di configurazione, cliccare sulla voce **Configuration** del menù, poi sulla voce **VPN** e selezionare quindi la voce **PPTP**. Nella parte destra della pagina di configurazione cliccare sulla voce **Create** e alla successiva schermata su **Remote Access**. Cliccare quindi sul pulsante **NEXT** per accedere alla pagina.



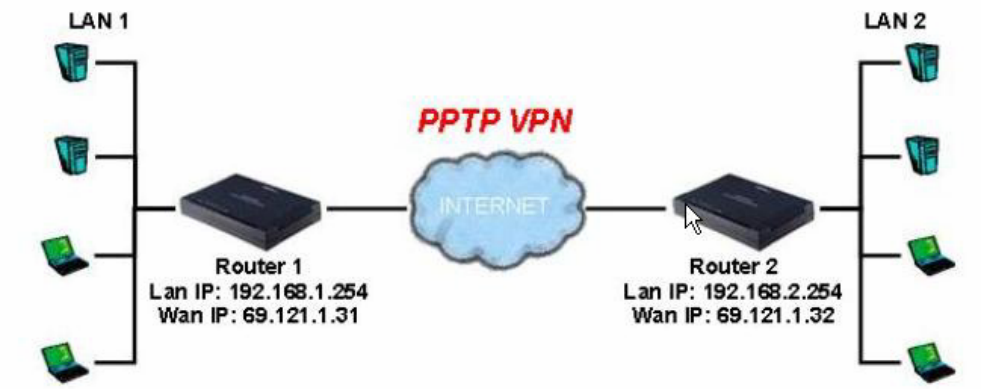
Inserire nel campo **Connection Name** un nome che identifichi la connessione, selezionare **Dial-Out** come tipologia di connessione e inserire l'IP o il Nome Host del PPTP Server remoto. Inserire quindi **Username** e **Password** con i quali il router accederà al servizio e cliccare sul pulsante **Apply** per applicare le modifiche. La nuova connessione viene automaticamente impostata come **Disabile** selezionare quindi la voce **Enable** cliccare sul pulsante **Apply** e salvarle cliccando sulla voce del menù **Save config to flash** seguito dal pulsante **Save**. Per modificare la nuova connessione è necessario spostare lo stato da **Enable** a **Disable** e cliccare su **Apply**, il comando **Edit** sarà quindi attivato.
Ora la LAN connessa al File Server remoto, è possibile verificare lo stato della connessione PPTP cliccando sulla voce **Status** del menù e poi sulla voce **PPTP Status**, la figura che segue ne riporta un esempio.

VPN/PPTP for Remote Access Application

Name	Type	Enable	Active	Session Connected	Call Connected	Encryption
PPTP	dialout	✓	✓	✓	✓	encryption enabled mppe 128bits stateful mode

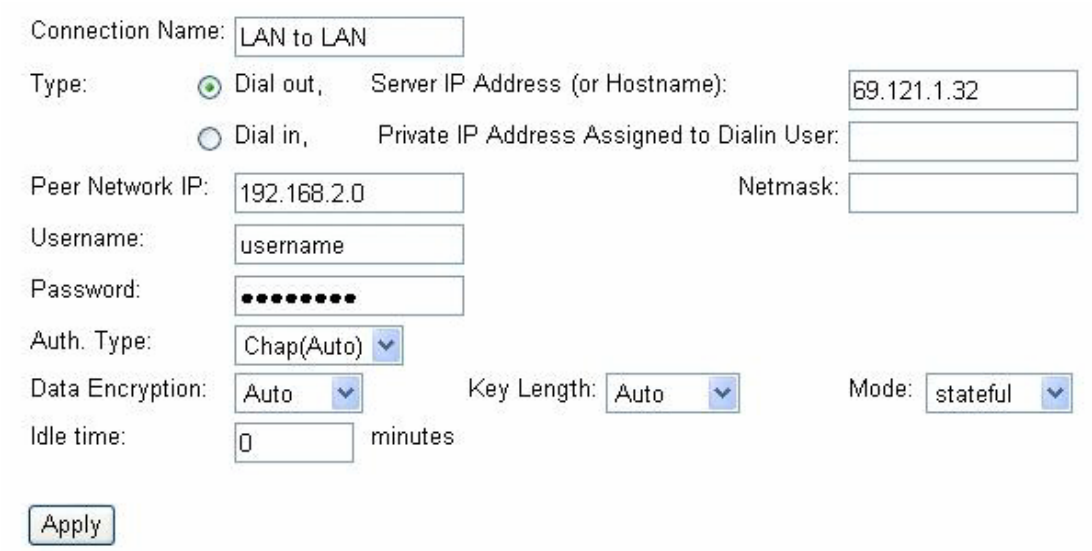
2.8.5.3 PPTP VPN – LAN to LAN

In questo scenario due sedi remote verranno connesse tramite una VPN PPTP, gli utenti della LAN 1 devo condividere risorse e servizi con la LAN 2. La figura che segue riassume quanto detto.



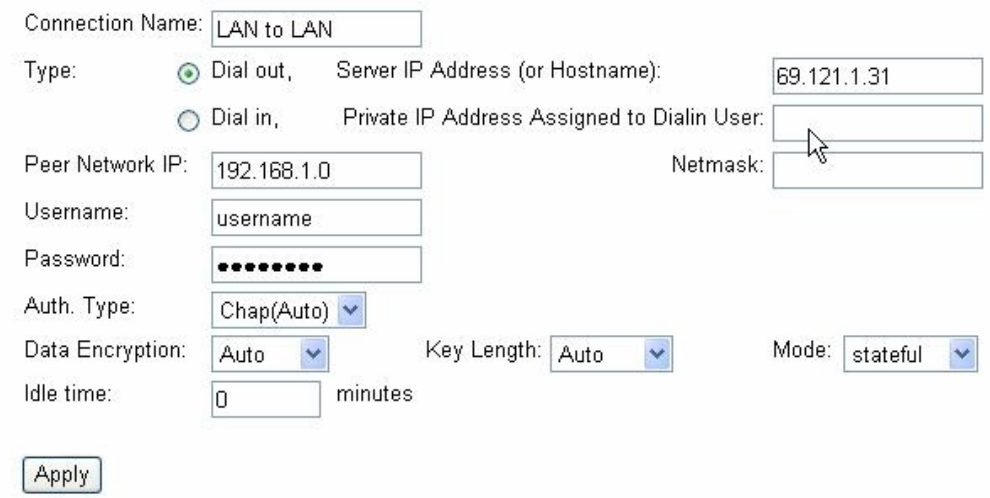
Vediamo quindi come configurare i due router A02-RA3 per mettere in comunicazione le due sedi:

• **ROUTER 1:** Per configurare il router per la modalità **VPN PPTP – LAN to LAN** è necessario accedere all'interfaccia web di configurazione, cliccare sulla voce **Configuration** del menù, poi sulla voce **VPN** e selezionare quindi la voce **PPTP**. Nella parte destra della pagina di configurazione cliccare sulla voce **Create** e alla successiva schermata su **LAN to LAN**. Cliccare quindi sul pulsante **NEXT** per accedere alla pagina **PPTP LAN to LAN**.



Inserire nel campo **Connection Name** una nome che identifichi la connessione, selezionare **Dial-Out** come tipologia di connessione e inserire l'IP o il "Nome Host" del PPTP Server remoto. Inserire ora l'indirizzo di rete della LAN remota, inserire quindi **Username** e **Password** con i quali il router accederà al servizio e cliccare sul pulsante **Apply** per applicare le modifiche. La nuova connessione viene automaticamente impostata come **Disable** selezionare quindi la voce **Enable** cliccare sul pulsante **Apply** e salvarle cliccando sulla voce del menù **Save config to flash** seguito dal pulsante **Save**. Per modificare la nuova connessione è necessario spostare lo stato da **Enable** a **Disable** e cliccare su **Apply**, il comando **Edit** sarà quindi attivato.

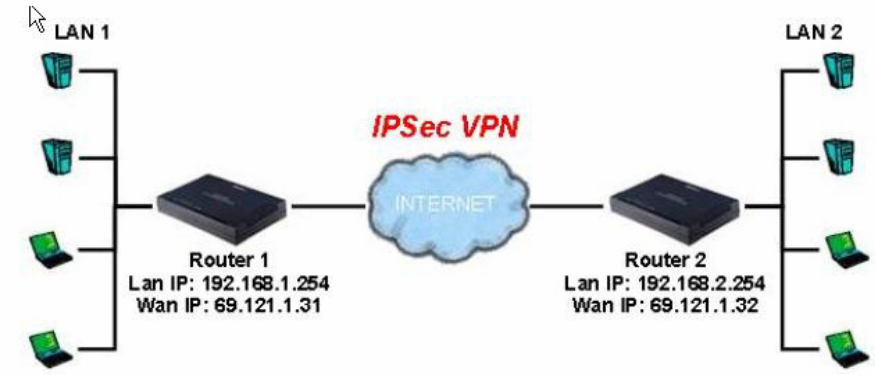
• **ROUTER 2:** Per configurare il router per la modalità VPN PPTP – LAN to LAN è necessario accedere all'interfaccia web di configurazione, cliccare sulla voce **Configuration** del menù, poi sulla voce **VPN** e selezionare quindi la voce **PPTP**. Nella parte destra della pagina di configurazione cliccare sulla voce **Create** e alla successiva schermata su **LAN to LAN**. Cliccare quindi sul pulsante **NEXT** per accedere alla pagina **PPTP LAN to LAN**.



Inserire nel campo **Connection Name** una nome che identifichi la connessione, selezionare **Dial-Out** come tipologia di connessione e inserire l'IP o il "Nome Host" del PPTP Server remoto. Inserire ora l'indirizzo di rete della LAN remota, inserire quindi **Username** e **Password** con i quali il router accederà al servizio e cliccare sul pulsante **Apply** per applicare le modifiche. La nuova connessione viene automaticamente impostata come **Disable** selezionare quindi la voce **Enable** cliccare sul pulsante **Apply** e salvarle cliccando sulla voce del menù **Save config to flash** seguito dal pulsante **Save**. Per modificare la nuova connessione è necessario spostare lo stato da **Enable** a **Disable** e cliccare su **Apply**, il comando **Edit** sarà quindi attivato. Ora le due reti potranno possono scambiare informazioni criptate. **É importante che le due LAN appartengano a due subnet differenti, la configurazione mostrata sopra utilizza infatti una rete 192.168.1.0 e una 192.168.2.0.**
É possibile verificare il corretto funzionamento della VPN PPTP cliccando sulla voce **Status** del menù e poi sulla voce **PPTP Status**.

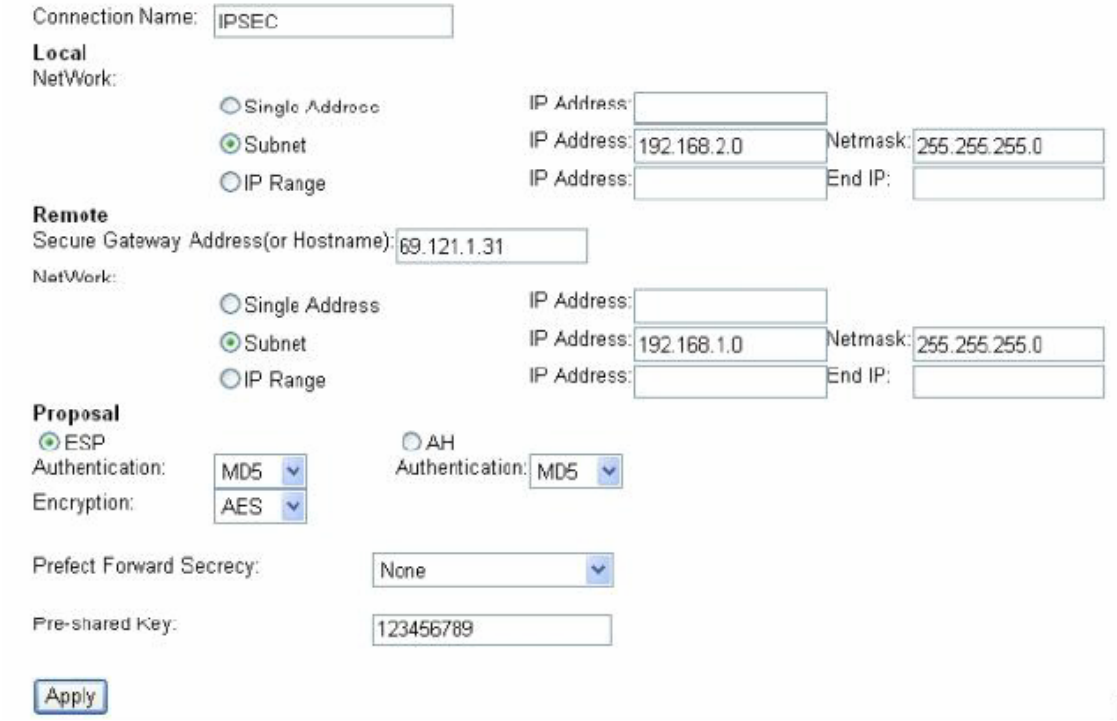
2.8.5.4 IPsec VPN

In questo scenario due sedi remote verranno connesse tramite una VPN IPSec, gli utenti della LAN 1 devo condividere risorse e servizi con la LAN 2. La figura che segue riassume quanto detto.



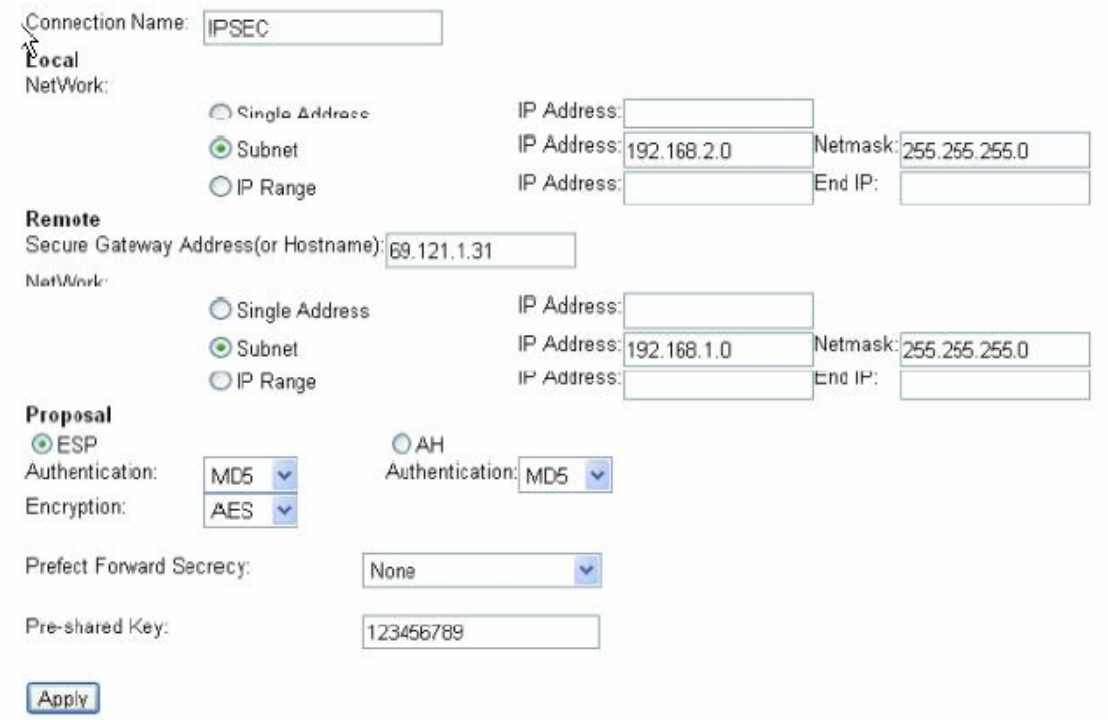
Vediamo quindi come configurare i due router A02-RA3 per mettere in comunicazione le due sedi:

• **ROUTER 1:** Per configurare il router per la modalità VPN IPSec è necessario accedere all'interfaccia web di configurazione, cliccare sulla voce **Configuration** del menù, poi sulla voce **VPN** e selezionare quindi la voce **IPSec**. Nella parte destra della pagina di configurazione cliccare sulla voce **Create** e poi sul pulsante **Apply**.

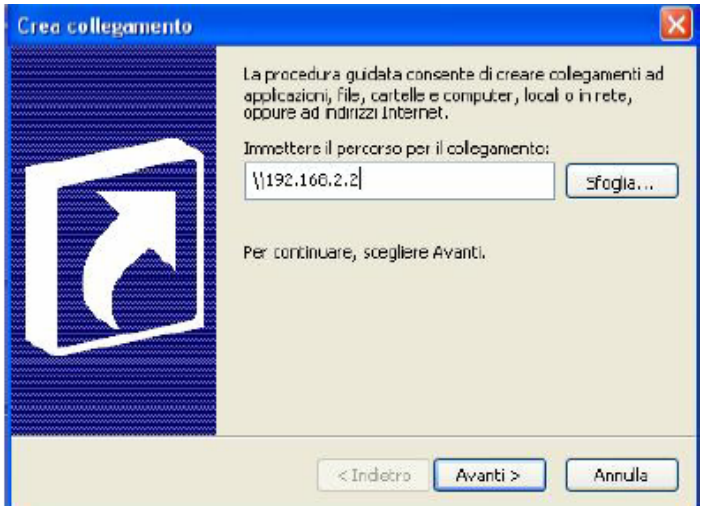


Inserire nel campo **Connection Name** una nome che identifichi la connessione. Nella sezione **Local** selezionare la voce **Subnet**, inserire quindi indirizzo di rete e netmask della LAN locale. Nella sezione **Remote** inserire l'indirizzo IP pubblico del router remoto nel campo **Secure Gateway Address**, selezionare la voce **Subnet** e inserire indirizzo di rete e netmask della LAN remota. La sezione **Proposal** contiene le informazioni relative alla modalità di crittazione, selezionare quindi la tipologia desiderata ed inserire una stringa numerica, alfabetica o alfanumerica nel campo **Pre-shared Key**. É necessario che la sezione **Proposal** contenga le medesime informazione in entrambi i router. Cliccare sul pulsante **Apply** per confermare i valori impostati e salvarle cliccando sulla voce del menù **Save config to flash** seguito dal pulsante **Save**.

• **ROUTER 2:** Per configurare il router per la modalità VPN IPSec è necessario accedere all'interfaccia web di configurazione, cliccare sulla voce **Configuration** del menù, poi sulla voce **VPN** e selezionare quindi la voce **IPSec**. Nella parte destra della pagina di configurazione cliccare sulla voce **Create** e poi sul pulsante **Apply**.



Inserire nel campo **Connection Name** una nome che identifichi la connessione. Nella sezione **Local** selezionare la voce **Subnet**, inserire quindi indirizzo di rete e netmask della LAN locale. Nella sezione **Remote** inserire l'indirizzo IP pubblico del router remoto nel campo **Secure Gateway Address**, selezionare la voce **Subnet** e inserire indirizzo di rete e netmask della LAN remota. Selezionare quindi nella sezione **Proposal** la modalità di crittazione ed inserire una stringa numerica, alfabetica o alfanumerica nel campo **Pre-shared Key**.É necessario che la sezione **Proposal** contenga le medesime informazione in entrambi i router. Cliccare sul pulsante **Apply** per confermare i valori impostati e salvarle cliccando sulla voce del menù **Save config to flash** seguito dal pulsante **Save**.



Ora le due reti potranno possono scambiare informazioni criptate. É importante che le due LAN appartengano a due subnet differenti, la configurazione mostrata sopra utilizza infatti una rete 192.168.1.0 e una 192.168.2.0.
É possibile verificare il corretto funzionamento della VPN IPSec cliccando sulla voce **Status** del menù e poi sulla voce **IPSec Status**, la figura che segue riporta un esempio di corretto funzionamento della VPN.
Dopo qualche minuto, se tutto è stato fatto correttamente avrete realizzato una VPN in IPSec tra le 2 LAN. Per verificare questo provate a pingare da un PC della LAN un PC dell'altra (settando opportunamente la sezione Firewall del Router affinché non tagli l'ICMP).

É possibile condividere, ad esempio, le risorse dei PC creando un collegamento e mettendo l'indirizzo IP (privato) del PC. Su Windows XP cliccare il tasto destro,sul Desktop, scegliere **Nuovo** e poi **collegamento**. Vi apparirà la schermata sotto riportata.
Inserire nel campo vuoto l'indirizzo IP di un PC nella LAN remota per poter accedere alle risorse condivise.

2.8.6 Virtual Server

Il firewall del Router ADSL consente la protezione della LAN locale da parte di accessi indesiderati. Può essere necessario, consentire ad utenti esterni l'accesso ad un PC specifico della LAN (per esempio verso un PC fa da server Web o FTP). La funzionalità di Virtual Server consente di reindirizzare un particolare servizio, che avviene su una determinata porta (si ricorda che Web =80 FTP =20/21, Telnet =23, SMTP =25, POP3 =110, DNS =53, ECHO =7, NNTP =119) , su un PC della LAN interna. É possibile scegliere l'intervallo (o la singola porta) di porte ed il protocollo (tra TCP,UDP o entrambi) che si intende rigirare sull'indirizzo IP.

Nota bene:

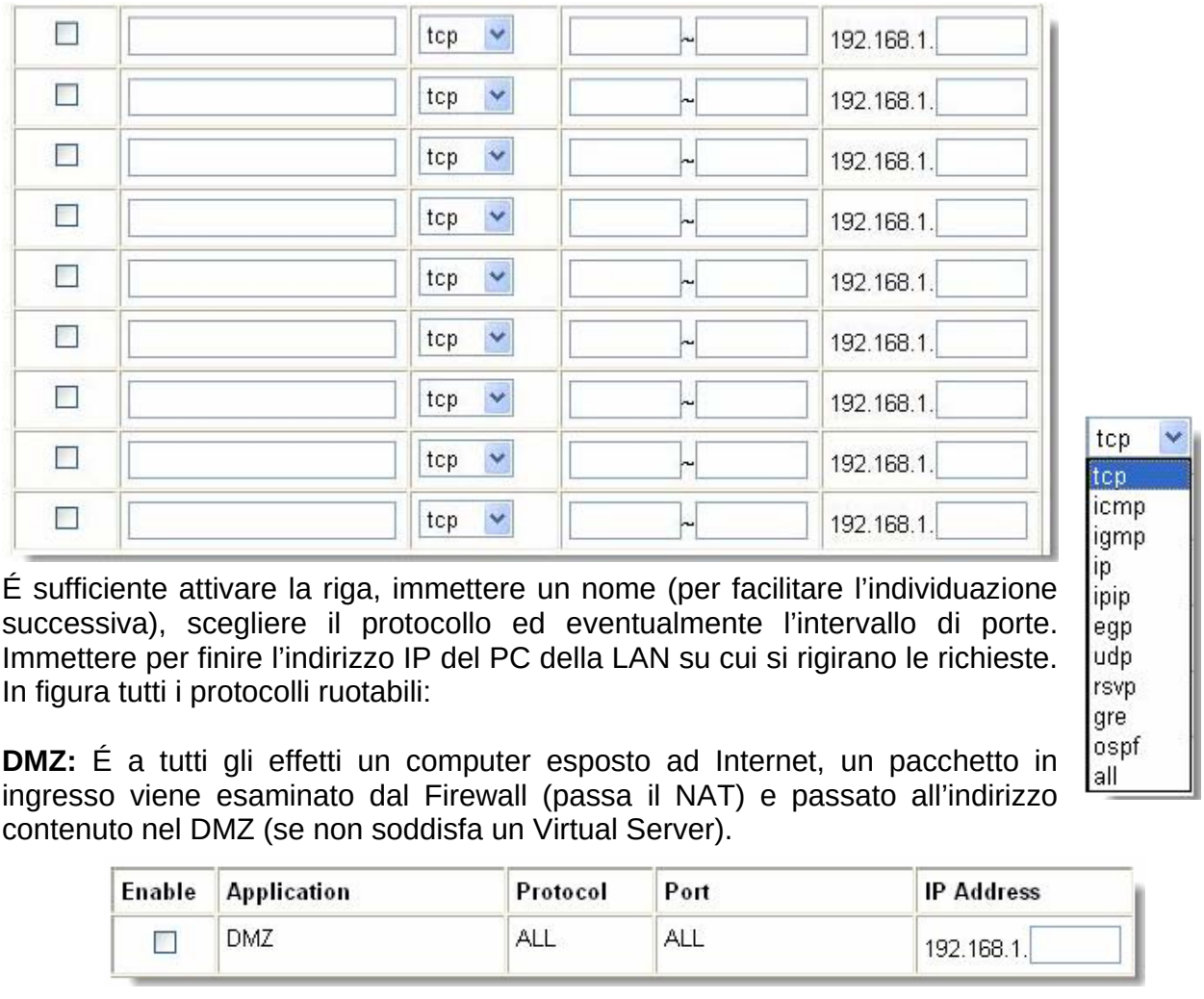
La sezione Firewall viene prima di quella del Virtual Server, assicurarsi che le porte/protocolli ruotati non siano bloccati dal Firewall.

Accedendo alla sezione Confi**guration-Virtual Server** avrete accesso alla seguente immagine:

Enable	Application	Protocol	Port	IP Address
☐	FTP	TCP	21	192.168.1.
☐	Telnet	TCP	23	192.168.1.
☐	SMTP	TCP	25	192.168.1.
☐	HTTP	TCP	80	192.168.1.
☐	POP3	TCP	110	192.168.1.
☐	NNTP	TCP	119	192.168.1.
☐	NTP	UDP	123	192.168.1.
☐	HTTPS	TCP	443	192.168.1.
☐	IKE	UDP	500	192.168.1.
☐	T.120	TCP	1503	192.168.1.
☐	H.323	TCP	1720	192.168.1.
☐	PPTP	TCP	1723	192.168.1.
☐	SIP	TCP/UDP	5060	192.168.1.

Se per esempio il server WEB (che riceverà chiamate sulla porta 80) della LAN ha indirizzo IP privato 192.168.1.2 dovremo editare la regola che consenta questo servizio, che verrà fatta come in figura.

É chiaro che in questo caso non dovremo utilizzare il DHCP client sul PC poichè in tal caso non conosceremo l'IP che il server Web potrebbe prendere (benchè la funzionalità Fixed Host permettere di risolvere questo problema).
É importante capire che il Router Hamlet ADSL esegue, in ordine di numerazione crescente, le associazioni richieste dai vari Virtual Server e solo alla fine (qualora fosse presente) rigira il tutto alla DMZ. Pertanto se la porta (20)21 è mappata su un certo PC della rete tramite Virtual Server, il PC il cui indirizzo è indicato nel DMZ non potrà funzionare come server FTP.
Sono anche presenti 10 Virtual Server non preconfigurati, come da figura:



É sufficiente attivare la riga, immettere un nome (per facilitare l'individuazione successiva), scegliere il protocollo ed eventualmente l'intervallo di porte. Immettere per finire l'indirizzo IP del PC della LAN su cui si rigirano le richieste. In figura tutti i protocolli ruotabili:

DMZ: É a tutti gli effetti un computer esposto ad Internet, un pacchetto in ingresso viene esaminato dal Firewall (passa il NAT) e passato all'indirizzo contenuto nel DMZ (se non soddisfa un Virtual Server).

Nota bene:

Qualora l'opzione di NAT sia disabilitata nella sezione WAN-ISP, la funzionalità di Virtual Server non è utilizzabile.

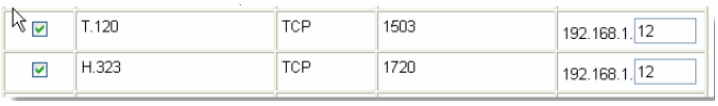
Se sul Router è abilitato il DHCP bisogna prestare particolare attenzione ad assegnare l'indirizzo IP dei Virtual Server per evitare conflitti. In questo caso è sufficiente assegnare al Virtual Server (Tale PC non sarà client DHCP ed avrà oltre all'indirizzo IP, la subnet mask, il gateway (cioè l'IP privato del Router ADSL) ed i server DNS) un indirizzo IP che sia nella stessa subnet del Router ma fuori dal range di indirizzi IP assegnabili dal server DHCP attivo sul Router ADSL.

Qualora abbiate problemi con un server FTP, creare un Virtual Server che ruoti anche la porta 20. Selezionare inoltre in IE la modalità FTP passiva.

Alcune applicazioni Internet ormai oggi diffusissime necessitano, per essere usate pienamente, di una configurazione particolare della sezione Virtual Server del Router ADSL. Nella lista seguente sono presenti questi settaggi. La lista non vuole essere esaustiva ma solo un punto d'inizio, invitiamo a consultare eventuali aggiornamenti di questo manuale (scaricabile dal sito www.hamletcom.com poi sezioni prodotti, si sceglie il Router ADSL e da qui è possibile scaricare il manuale)

Applicazione	Connessioni Uscenti	Connessioni Entranti
ICQ 98, 99a	Nessuno	Nessuno
NetMeeting 2.1 a 3.01	Nessuno	1503 TCP, 1720 TCP
VDO Live	Nessuno	Nessuno
mIRC	Nessuno	Nessuno
Cu-SeeMe	7648 TCP &UDP, 24032 UDP	7648 TCP &UDP, 24032 UDP
PC AnyWhere	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP
Edonkey/Emule	Nessuno	principalmente 4660-4662 TCP , 4665 UDP
MSN Messanger	Nessuno	TCP da 6891-6900 TCP 1863 TCP 6901 UDP 1863 UDP 6901 UDP 5190

Usando NetMeeting (Versione3.0), ad esempio, quando la chiamata generata è uscente da un PC dietro al Router verso un PC esterno non ci sono problemi. Il contrario non è realizzabile. Rigirando invece le porte 1503 e 1720 è possibile ricevere anche chiamate in ingresso con video (h.323 e T.120). In figura è presente una configurazione di VS per ricevere chiamate in ingresso in Netmeeting (vengono rigirate al PC con IP 192.168.1.12).



Nota bene:

Attenzione il Router può gestire un numero non infinito di connessioni entranti, pertanto per grandi range (o centinaia di connessioni contemporanee) potrebbero sorgere problemi.

Sono allegate tutta una serie di porte notevoli (da utilizzarsi per il VS ed il Firewall):

Servizio	Numero di Porta / Protocollo
File Transfer Protocol (FTP) Data	20/tcp
FTP Commands	21/tcp
Telnet	23/tcp
Simple Mail Transfer Protocol (SMTP) Email	25/tcp
Domain Name Server (DNS)	53/tcp and 53/udp
Trivial File Transfer Protocol (TFTP)	69/udp
finger	79/tcp
World Wide Web (HTTP)	80/tcp
POP3 Email	110/tcp
SUN Remote Procedure Call (RPC)	111/udp
Network News Transfer Protocol (NNTP)	119/tcp
Network Time Protocol (NTP)	123/tcp and 123/udp
News	144/tcp
Simple Management Network Protocol (SNMP)	161/udp
SNMP (traps)	162/udp
Border Gateway Protocol (BGP)	179/tcp
Secure HTTP (HTTPS)	443/tcp
rlogin	513/tcp
rexec	514/tcp
talk	517/tcp and 517/udp
ntalk	518/tcp and 518/udp
Open Windows	2000/tcp and 2000/udp
Network File System (NFS)	2049/tcp
X11	6000/tcp and 6000/udp
Routing Information Protocol (RIP)	520/udp
Layer 2 Tunnelling Protocol (L2TP)	1701/udp

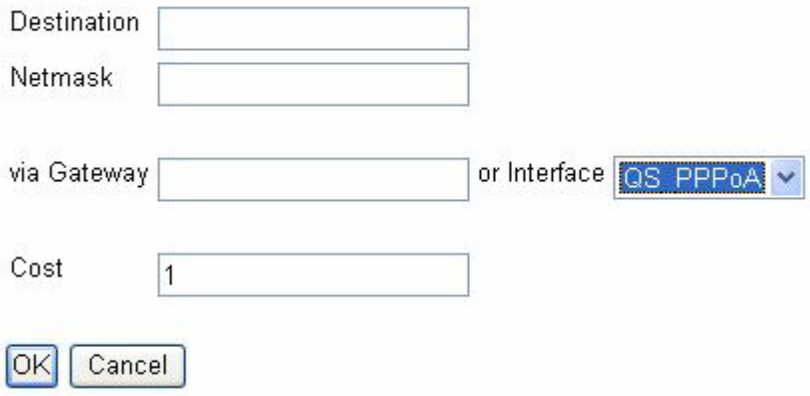
2.8.7 Advanced

Sono disponibili le seguenti sottosezioni:

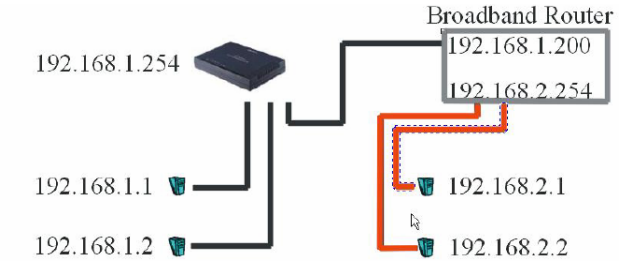
- **Routing Table**
- **Dynamic DNS**
- **Check Emails**
- **Device Management**

2.8.7.1 Routing Table

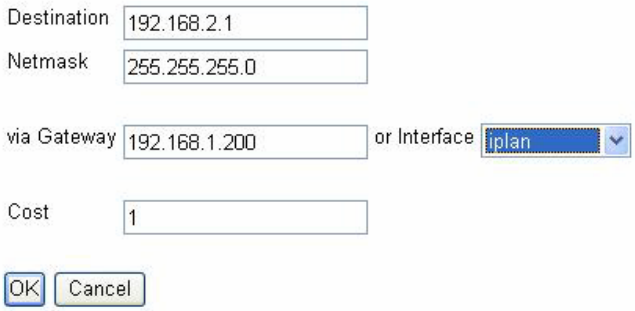
Grazie a tale funzionalità è possibile creare delle tabelle di Routing statiche.



Destination: Introdurre l'IP di destinazione.
Netmask: Introdurre la Subnet.
Gateway: Introdurre l'IP della macchina che fa Nat sulla classe indirizzata **Cost:** Introdurre il costo in Hop. Usualmente 1. Mettere tale valore in funzione del numero di Router che bisogna attraversare per arrivare alla rete desiderata.
Interface: Selezionare il tipo di interfaccia (iplan, per l'interfaccia LAN)
Nel caso in cui si abbia il Router con la classe LAN 192.168.1.X ed un Router Broadband che effettua NAT sulla classe 192.168.2X è necessario effettuare la configurazione di una route statica.



In questo caso nel Router ADSL dovremo indicare che tutti i pacchetti diretti alla classe 192.168.2.X andranno indirizzati verso il Router Broadband avente IP 192.168.1.200.



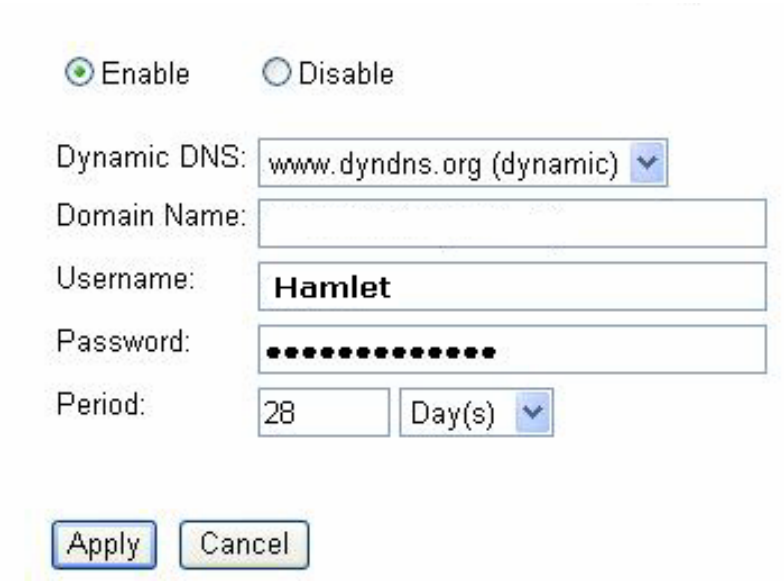
Abbiamo scelto poi l'interfaccia su cui avviene il forwarding del pacchetto. In questo caso si è lasciato come **Cost** valore 1 poiché vi è un solo Router fra l'Hamlet e la classe 192.168.2.X. In caso di differenti Router Broadband (per restare al caso di sopra) è necessario indicare il corretto valore nel campo **Cost**.

2.8.7.2 Dynamics DNS

Tramite questa funzionalità è possibile registrare un dominio ed associarlo ad un IP dinamico. Ogni qual volta il Router si riconnetterà, tramite il client incorporato, comunicherà al server DNS il nuovo indirizzo IP. Associando tale funzionalità con il Virtual Server è possibile :

- Ospitare un sito WEB sul proprio PC
- Effettuare configurazioni remote
- Accedere tramite VPN PPTP

I passaggi da seguire sono i seguenti:



Tramite questa funzionalità è possibile registrare un dominio ed associarlo ad un IP dinamico. Ogni qual volta il Router si riconnetterà, tramite il client incorporato, comunicherà al server DNS il nuovo indirizzo IP. Associando tale funzionalità con il Virtual Server è possibile ospitare un sito WEB sul proprio PC. I passaggi da seguire sono i seguenti:

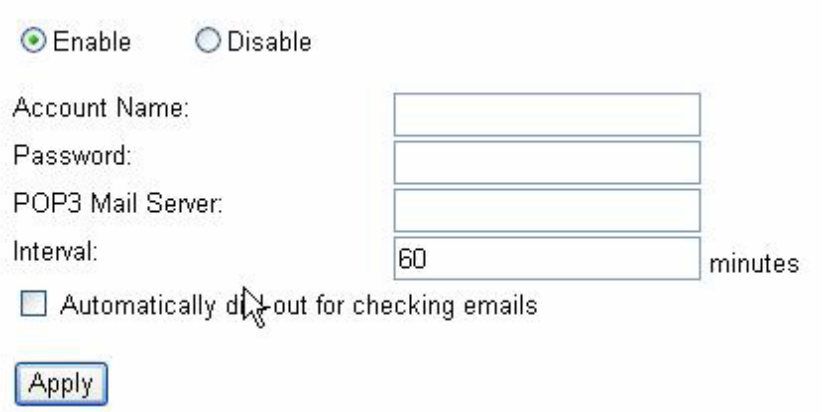
- Registrare il proprio dominio gratuitamente e istantaneamente su **www.dyndns.org**, **www.zoneedit.com.**
- Configurare il client sul Router Hamlet ADSL inserendo i campi appropriati (**Domain Name**, **Username** e **Password**)
- Impostare il campo **Period**. Il Router infatti aggiornerà il DDNS ogni qualvolta ottiene un nuovo IP dalla sfida PPP oppure ogni volta che il tempo contenuto nel campo Period è stato superato.

A questo punto il Router è sempre e comunque raggiungibile dall'esterno. É possibile ospitare un sito WEB o FTP (ruotando le opportune porte), accedere al servizio Server VPN o alla configurazione remota del Router.
In questo modo ogni utente esterno interrogherà il server DNS che gli restituirà di volta in volta l'indirizzo IP assegnatovi dall'ISP. Usando la funzionalità di riconnessione (disponibile in PPPoA e PPPoE), qualora la connessione dovesse cadere, il Router la rialzerà immediatamente.

Nota bene:
Qualora dovreste incontrare problemi quali la sospensione del servizio vi invitiamo a prendere nota delle condizioni praticate dal vostro fornitore di servizio Dynamic DNS e aumentare il campo **Period** in modo rispettare le politiche.

2.8.7.3 Check Emails

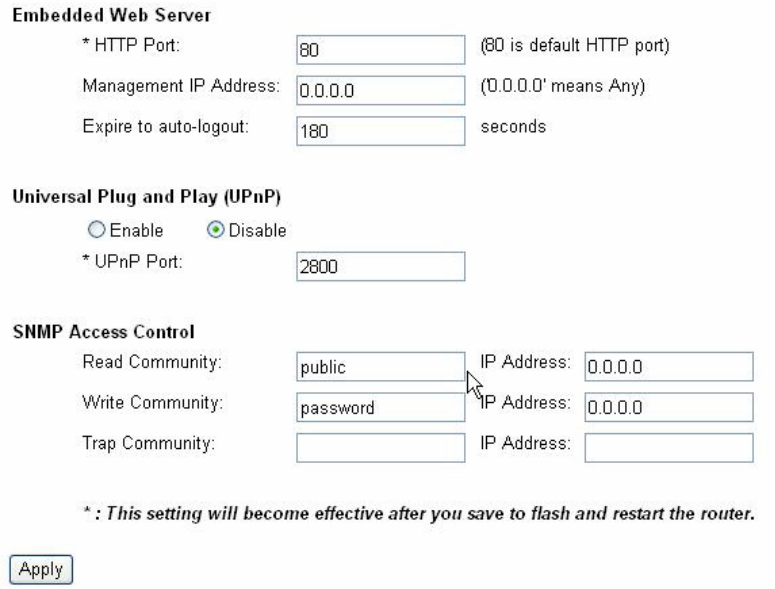
Questa funzionalità permette al Router di controllare se nell'account di posta preconfigurato è arrivata una nuova mail. In caso affermativo accenderà il LED mail. In questo modo, semplicemente guardando il Router, potrete sapere se vi sono state inviate nuove mail.



Per la configurazione è sufficiente spuntare **Enable** e configurare l'account da controllare, scegliere l'intervallo di controllo. Abilitando la voce **Automatically dial out for checking emails** il Router in caso di connessioni PPPoA/PPPoE alzerà la connessione per controllare l'account di posta. Prestare particolare attenzione nel caso di abbonamenti di tipo non FLAT.

2.8.7.4 Device Management

É possibile spostare la porta tramite cui si effettua la configurazione remota del Router, bloccare tale possibilità per un determinato periodo di tempo ed ad un preciso indirizzo IP (lasciando invece 0.0.0.0 è possibile configurare il Router da qualsiasi IP).
É inoltre possibile Abilitare/Disabilitare la funzionalità Universal Plug and Play e stabilire la porta. Infine è possibile configurare il protocollo SNMP.



2.8.3 Save Config. to FLASH

Ogni volta che si effettua un cambiamento alla configurazione del dispositivo, questo cambiamento viene (salvo rare eccezioni) immediatamente reso attivo. Per rendere tale

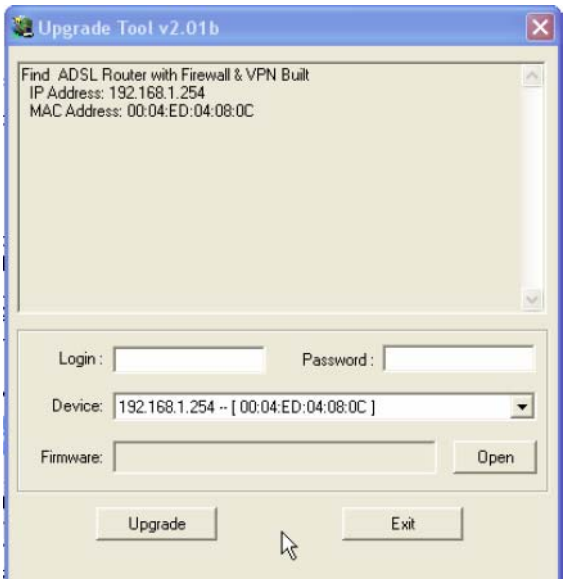
cambiamento permanente è sufficiente ciccare su Save Config to FLASH e poi su Save. In questo modo verrà scritto su eprom e dunque caricato ad ogni boot del dispositivo.

2.8.4 Logout

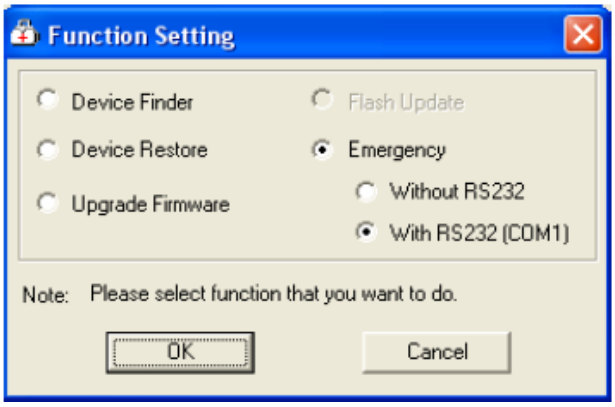
Per uscire dalla configurazione del Router ADSL si consiglia di non chiudere il browser semplicemente ma di effettuare il **Logout**, ciccando sull'apposita voce (l'ultima verso il basso).

2.9 Ripristino del Firmware

Questa procedura consente il ripristino del firmware del Router qualora qualcosa sia andato male durante la procedura di update o qualora si sia sprogrammata la memoria flash a causa di scariche elettriche provenienti, in massima misura (sono meno probabili quelle sul cavo LAN), tanto dalla rete elettrica quanto da quella telefonica. A tal fine vi invitiamo di dotarvi degli apparati adeguati per evitare eventuali guasti (**i fulmini e/o scariche elettriche non sono coperte da garanzia**).
Lanciare il software Upgrade Tool presente nella cartella Recovery del CDRom(D:\A02-RA3\Recovery). Vi apparirà l'immagine di sotto:



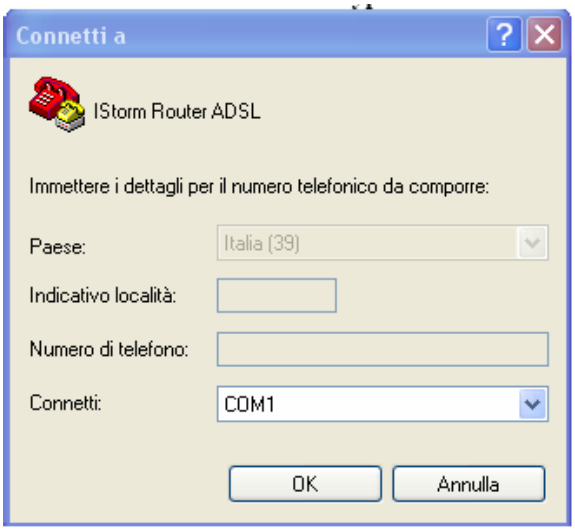
Premere **Alt + F**, vi apparirà la seguente immagine:



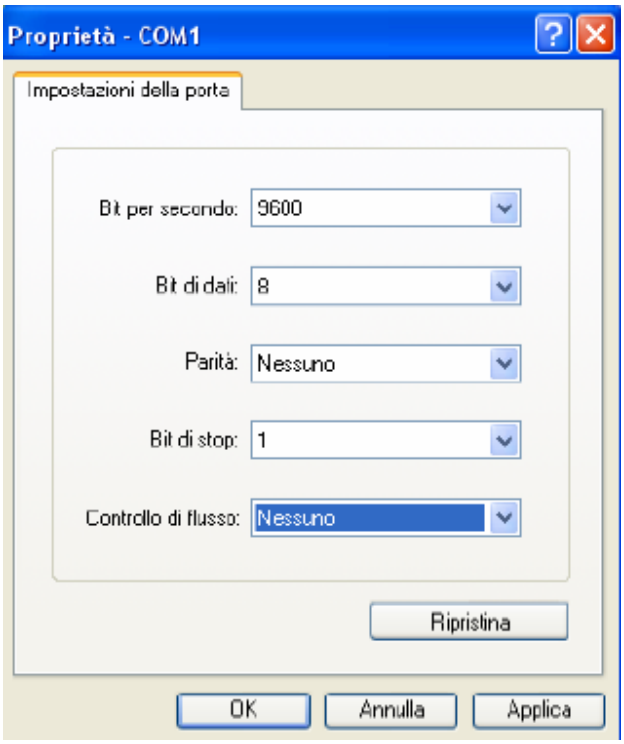
Spuntate, come da figura, **Emergency** e poi **With RS232(COM1).** Premete poi **OK.**
A questo punto seguite le istruzioni a schermo:
• Spegnete il dispositivo
• Accertatevi del collegamento tramite la COM1
• Inserite Username e Password
• Tramite **Open** selezionate il percorso del firmware (è un file con estensione AHE)
• Cliccate su **Emergency** ed accendete il Router
Partirà la procedura di ripristino forzato che vi permetterà di riutilizzare il Router.

2.10 Console e/o Telnet

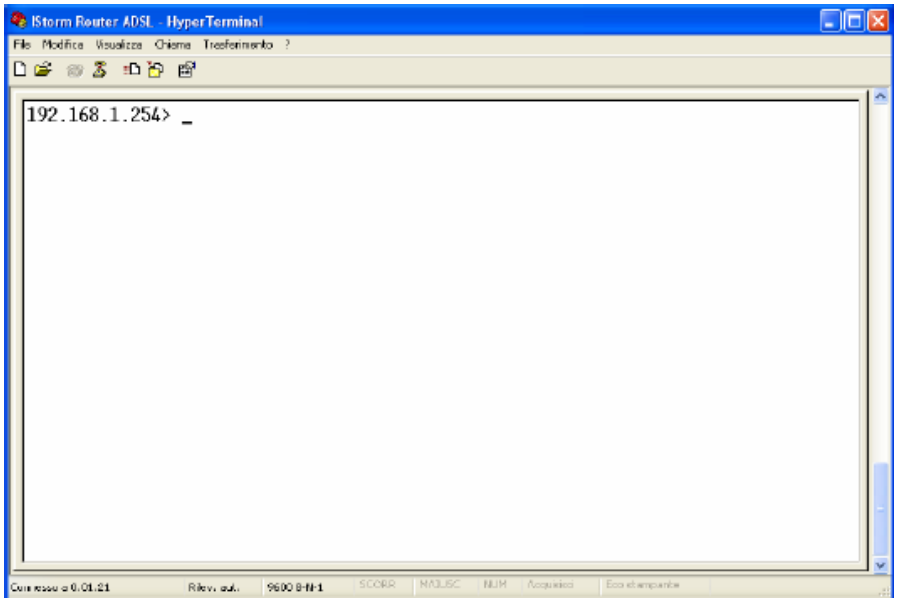
É possibile configurare il Router ADSL sia tramite Telnet (username = **admin** e la password = **Hamlet**)
che tramite Console. Per la configurazione tramite Telnet andare nel prompt dei comandi e digitare **telnet <indirizzo Lan IP>** e premere invio.
Vediamo adesso la configurazione tramite Hyperterminal:
Lanciare Hyperterminal o qualsiasi altro programma di emulazione terminale (le istruzioni seguenti si riferiscono a hyperterminal).
In XP, ad esempio, andare su **Start-tutti programmi-accessori-comunicazioni-hyperterminal**



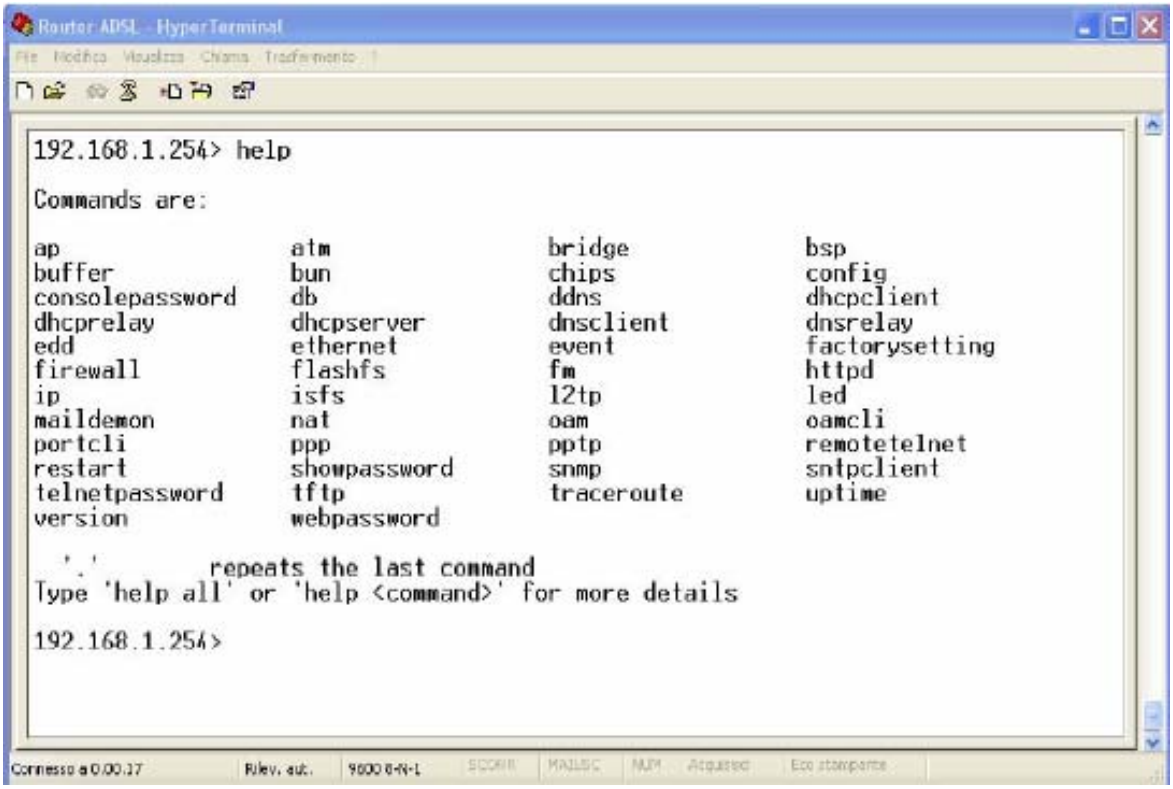
Introdurre il nome da dare alla connessione e premere **OK**.
Scegliere la porta **COM** cui è collegato il Router Hamlet ADSL
Inserire i settagli come da figura (bit per secondo=9600, Bit di dati=8, Parità=Nessuno, Bit di Stop=1, controllo di flusso=Nessuno):



Premere su **Applica** e poi **OK**.
Vi troverete a questo punto dopo aver premuto **INVIO** di fronte alla seguente schermata in cui vi si chiede di introdurre username e password.
Digitando **Console Enable** seguito da **INVIO** passerete in modalità console. Dovreste vedere l'immagine sotto:



A questo punto apparirà l'indirizzo LAN del Router ed un cursore lampeggiante. Utilizzando il comando **help** seguito dal tasto invio è possibile vedere la lista di tutti i comandi disponibili. Vi apparirà il seguente elenco (può variare a seconda del firmware installato):



Digitando il nome del comando (se riferito ad un processo) seguito da invio e poi digitando **help all** potremo vedere tutti i comandi relativi all'opportuno processo. Per tornare alla root sarà sufficiente digitare **home** seguito da invio. Alcuni comandi invece (quelli non riferiti ad un processo) eseguono immediatamente un'azione. Di questa categoria fanno parte (tra gli altri):

restart (effettua il restart del Router)

uptime (mostra il tempo dall'ultima accensione o restart)

version (fornisce informazione sul firmwaree installato nel dispositivo)

Capitolo 3

Troubleshooting

Qualora il Router ADSL non funzionasse propriamente, prima di rivolgersi all'ISP, consultare questo capitolo.

Problemi alla partenza del Router Hamlet ADSL

Problema	Azioni correttive
Nessun LED è acceso quando si collega il Router ADSL alla rete elettrica.	Controllare la connessione tra l'alimentatore ed il Router ADSL. Accertarsi che il Power Switch posto nel retro sia premuto. Qualora il problema persistesse potrebbe essere un problema hardware. Rivolgersi, in questo caso, al supporto tecnico

Ho dimenticato la Password

Problema	Azioni correttive
Qualora abbiate dimenticato la password per entrare nel Router Firewall ADSL Hamlet oppure non ricordate più l'IP che gli avevate assegnato.	Potete, perdendo la configurazione del dispositivo, resettarlo premendo l'apposito bottone (per almeno 6 secondi) posto sul retro.

Non riesco ad entrare nel Router via WEB

Problema	Azioni correttive
Pur digitando l'IP del Router (192.168.1.254) non ottengo risposta, cosa posso fare?	Il problema potrebbe essere dovuto o ad un cablaggio errato oppure a causa di indirizzo IP del PC "inconsistente. Verificare il cablaggio (non dovrebbero esserci problemi nel caso di connessione diretta tra il PC ed il Router in quanto quest'ultimo grazie alla funzionalità di autopolarità può funzionare tanto con cavi dritti che incrociati. Potrebbero esserci problemi nel caso si usino Switch). A questo punto si è pronti per configurare il Router digitando il suo IP che di default è 192.168.1.254. Qualora non si riuscisse ancora ad entrare, è opportuno controllare l'indirizzo IP del PC e spostarlo sulla classe 192.168.1.x (ad esempio 192.168.1.1, subnet=255.255.255.0 e default gatewy quello del Router).

Problemi con l'interfaccia WAN

Problema	Azioni correttive
Fallisce l'inizializzazione della connessione PVC.	Assicurarsi che il cavo RJ11 sia connesso propriamente alla linea telefonica ed al Router ADSL. Il LED ADSL dovrebbe essere acceso fisso. Qualora lampeggiasse attendere che smetta, la connessione non è altrimenti realizzabile. Controllare i valori di VPI e VCI, il tipo di incapsulazione ed il tipo di modulazione (valori forniti dall'ISP). Effettuare il Reboot del Router ADSL. Andare (se si è in modalità Router) in System e poi nella sottosezione System status e qui sotto la sezione WAN controllare lo stato della connessione (il bottone deve essere sullo stato DISCONNECT, qualora così non fosse cliccarci sopra). Qualora il problema persistesse contattare l'ISP e verificare tali parametri.

Problemi con l'interfaccia LAN

Problema	Azioni correttive
Non posso fare il ping con alcun PC della LAN.	Controllare i LED LAN, nel pannello frontale. Tale LED dovrebbe essere acceso(almeno uno dei 4). Se così non fosse controllare il cablaggio.
	Verificare, nel caso in cui il LED sia acceso, che l'indirizzo IP e la subnet mask tra il Router ed i PC siano consistenti.

Problemi di Connessione ad un Remote Node oppure ad un ISP

Problema	Azioni correttive
Non riesce a connettersi ad un remote node o ad un ISP.	Fare riferimento alla *sezione Status* per verificare lo stato della linea.
	Verificare Login e Password per la connessione col remote node (nel caso di PPPoA/PPPoE). Controllare l'indirizzo IP nel caso di RFC1483/1577.
	Controllare il tipo di Incapsulamento utilizzato ed i valori di VCI/VPI (in caso di dubbi, cancellare la connessione ed utilizzare la procedura di Quick Start).

Conflitto di indirizzi IP

Problema	Azioni correttive
Il PC visualizza un messaggio che informa sul conflitto dell'indirizzo IP.	La causa può essere un reboot del Router ADSL (se impostato come server DHCP) oppure da due o più PC che hanno lo stesso indirizzo. E' possibile lanciando l'utilità "**winipcfg**" controllare tutti i parametri (IP, Subnet, DG) ed eventualmente rinnovarli (se il PC è un client DHCP ed il Router funge da server DHCP). L'utilità "winipcfg.exe" è disponibile per Win95, 98 e ME. Per WinNT, Win2000 e WinXP utilizzare l'utility "**ipconfig**".

Il Router non riesce ad allinearsi?

Problema	Azioni correttive
Il Led ADSL continua a lampeggiare ed il Router non riesce ad allinearsi. Cosa posso fare?	Il Router, grazie al supporto del protocollo G.994.1 (G.hs) riesce a scegliere il tipo di modulazione automaticamente. Potrebbe rendersi necessario forzare un tipo di modulazione in questo caso scegliere quella opportuna (**glite, gdmt, multi, ansi etc**). Andare su **Status** e poi premere su **Al** ed impostare tremite la combo box di **Connect Mode** la modulazione più adatta. Cliccare su **Save config to Flash** e poi su save per rendere permanenti le modifiche.

Cos'è il NAT?

Quesito	Risposta
Cosa fa esattamente il NAT?	Nat significa Network Address Traslation (traslazione degli indirizzi di rete locale). E' stato proposto e descritto nell'RFC-1631 ed aveva, almeno originariamente, il compito di permettere uno sfruttamento intensivo degli indirizzi IP. Ogni strumento che realizzi il NAT è composto da una tabella costruita da coppie di indirizzi IP, uno della rete privata ed uno pubblico. Dunque c'è una traslazione dagli IP della rete

segue

Cosa fa esattamente il NAT?	privata a quelli pubblici ed il contrario. Il Router ADSL supporta il NAT, pertanto con un'opportuna configurazione più utenti possono accedere ad Internet usando un singolo account (e un singolo IP pubblico). Il NAT consente a più utenti di accedere ad Internet al costo di un singolo account IP. Se gli utenti della LAN dispongono di indirizzi IP pubblici e possono pertanto accedere direttamente ad Internet (e fungere da server per determinati servizi) tale funzionalità dovrebbe essere disabilitata. Il Nat inoltre è una sorta di primo firewall che migliora la sicurezza della Lan locale. Andrebbe usata quando il traffico indirizzato verso Internet è una parte di quello che circola nella Lan locale, altrimenti tale funzionalità potrebbe degradare leggermente le prestazioni della connessione ad Internet. Tale funzionalità coesiste con la funzionalità Virtual Server, DMZ e DHCP. Il Nat manipola i pacchetti IP uscenti e ne cambia il campo **IP provenienza** sostituendo il mittente del pacchetto (in questo caso l'indirizzo IP il PC della Lan, che è un IP privato non valido in Internet) con l'IP pubblico dell'I-Storm ADSL Router. In questo modo tutti i pacchetti uscenti dal Router avranno nel campo mittente l'indirizzo IP pubblico del Router. Quando poi i pacchetti torneranno al Router (perché sono a lui indirizzati) questo in base a tabelle memorizzate provvederà al processo contrario e li spedirà al PC interessato nella Lan.

Percorso dei pacchetti

Problema	Azioni correttive
Non funziona il Server che ho settato su un PC.	Il Router ADSL applica, ad ogni pacchetto, nell'ordine: Firewall, Virtual Server e DMZ. Affichè il Server funzioni bisogna accertarsi che nessun blocco antecedente al VS (Firewall) o DMZ (Firewall e VS) non operi in conformità. Settare il PC che funge da Server con un indirizzo IP privato fisso (o usare la modalità Fixed Host nel DHCP).

Non funziona correttamente un'applicazione Internet

Problema	Azioni correttive
Alcune applicazioni, quando il Router fa NAT oppure è attivo il firewall, potrebbero non funzionare propriamente.	Il Router, tramite il NAT e/o il firewall, protegge la LAN isolandola dall'esterno e rifiutando tutti i tentativi di connessione generati dall'esterno. In Internet ogni servizio è associato ad una porta. Queste porte potrebbero essere chiuse per evitare che malintenzionati possano accedere alla LAN. Tuttavia può essere necessario, per il funzionamento di determinate applicazioni (ad esempio NetMeeting), che i tentativi di connessione generati dall'esterno su determinate porte siano rigirati ad un PC della LAN su cui il programma in questione sia in "ascolto". Consultare la sezione Virtual Server per avere maggiori dettagli. Le applicazioni che tipicamente dovranno essere configurate sono: Alcuni Programmi di Email Alcuni Giochi Multi-Players Alcune Applicazioni Phone/Video Conferenza Per trovare le porte da aprire per il corretto funzionamento dell'applicazioni solitamente la strada più breve è quella di consultare il sito web del produttore dell'applicazione. Resta inteso che in questo modo un solo PC della LAN (quello su cui saranno girate le opportune porte) potrà usare l'applicazione in questione.

Perché nonostante il VS alcune applicazioni non vanno?

Problema	Azioni correttive
Ho effettuato la rotazione delle porte col VS ma l'applicazione ancora non va, cosa posso fare?	Potrebbe rendersi necessario effettuare una DMZ verso il PC su cui si vuole far girare una particolare applicazione. Se ad esempio il PC in questione viene "chiamato" dall'esterno per la costruzione di una VPN bisogna necessariamente effettuare verso il suo IP privato una DMZ.

Perché nonostante la DMZ alcune applicazioni non vanno?

Problema	Azioni correttive
Pur utilizzando la DMZ l'applicazione non funziona ancora, cosa posso fare?	Nonostante le caratteristiche del Router alcune applicazioni potrebbero non funzionare perché non trasparenti al NAT (nemmeno effettuando una DMZ). In questo caso è possibile utilizzare il Router in modalità Bridge. Così facendo l'indirizzo IP pubblico del Router viene "dato" al PC che dunque potrà far funzionare tutte le applicazioni (come se il Router fosse un modem ADSL). Anzitutto dovete chiedere al vostro ISP il protocollo PPPoE e poi configurare il Router secondo il protocollo RFC1483 Bridge. In questo modo però solo un singolo PC (dotato di client PPPoE) può accedere ad Internet.

RFC 1483 Bridge su MAC OS 9

Problema	Soluzione
Avendo un abbonamento di tipo PPPoE voglio utilizzare il Router in modalità RFC 1483 Bridge con una macchina con MacOS9. Come posso fare?	Il **MacPoet** è un software PPPoverEthernet, compatibile con tutti i MacOS dal 7.0. Una volta scaricato il file, faremo partire l'installazione, che è del tutto automatica; una volta conclusa, dal menù mela andremo in TCP/IP a controllare che nel campo Connetti Via ci sia selezionato Ethernet Built-in; fatto ciò, clicchiamo sull'icona del MacPoeT presente nella cartella sull'hard disk dove è stato installato il software. Si aprirà una finestra in cui basterà inserire username e password forniti dal provider e cliccare su **Connect**. Per lanciare la connessione appena aperto MacPoet ci basterà mettere la spunta su **Connect at Startup**.

RFC 1483 Bridge su MAC OS X

Problema	Soluzione
Avendo un abbonamento di tipo PPPoE voglio utilizzare il Router in modalità RFC 1483 Bridge con una macchina con MAC OS X. Come posso fare?	Al pari di Windows XP della Microsoft, il MacOSX, ha un'interessantissima potenzialità che consente di creare una connessione ad Internet mediante protocollo PPP over Ethernet senza la necessità di dover installare componenti esterni al SO stesso. La configurazione della connessione è molto semplice ed immediata: Innanzitutto, dal menù mela, cliccheremo sulla voce **Preferenze di sistema**. Nella cartella **Preferenze di sistema** clicchiamo su **Network**. Nella finestra **Network,** alla voce **Configura** selezioniamo **ETHERNET INTEGRATA**; poi, cliccando su **PPPoE**, inseriamo i dati forniti dal Provider: Se necessario, cliccando su "TCP/IP" potremo inserire i DNS del nostro Provider: A questo punto clicchiamo su **Registra** per salvare le modifiche. La nostra connessione in PPPoE è stata creata! Per lanciare la connessione sarà sufficiente andare, dal menù **VAI**, nella cartella Applicazioni. Qui clicchiamo su **Internet Connect**, selezioniamo di nuovo, alla voce Configurazione, **Ethernet Integrata**, e clicchiamo su **COLLEGAMENTO** per connetterci ad Internet.

RFC 1483 Bridge su macchine Windows 95, 98, ME

Problema	Soluzione
Avendo un abbonamento di tipo PPPoE voglio utilizzare il Router in modalità RFC 1483 Bridge con una macchina con Windows 95, 98, ME. Come posso fare?	E' possibile usare un qualunque software (Enthernet, Win PoET, RasPPPoE). Alleghiamo le istruzioni per RasPPPoE(freeware). Scompattare il file **RASPPPOE.ZIP** in una cartella (prendetene nota). Doppio click sull'icona **pannello di controllo** e poi doppio click su **rete**. Selezionare la voce **aggiungi** , poi scegliere **protocollo** e cliccare su **aggiungi**. Selezionare a questo punto **Disco Driver**. Selezionare la cartella dove precedentemente sono stati scompattati i driver e quindi scegliere uno qualsiasi dei 3 file.inf. A questo punto potremo cliccare su **OK** e far riavviare la macchina. Al riavvio sarà necessario creare la connessione remota. A tal fine seguire i seguenti passaggi: Aprire la cartella **C:\Windows\System** e cliccare due volte sul file **raspppoe.exe**. Apparirà una schermata nella quale è necessario selezionare la scheda di rete cui è connesso l'I-Storm; a questo punto cliccare una volta su **Create a Dial-Up connection for the selected Adapter** ed infine scegliamo **exit**. Il processo è terminato, in Accesso Remoto è stata creata un'icona che basterà cliccare per azionare il collegamento ad internet.

RFC 1483 Bridge su macchine Windows 2000

Problema	Soluzione
Avendo un abbonamento di tipo PPPoE voglio utilizzare il Router in modalità RFC 1483 Bridge con una macchina con Windows2000. Come posso fare?	E' possibile usare un qualunque software (Enthernet, Win PoET, RasPPPoE). Alleghiamo le istruzioni per RasPPPoE(freeware). Doppio click sull'icona pannello di controllo e poi doppio click su rete e connessione remote. Selezionare la voce Connessione alla rete locale (LAN) premere il tasto destro e poi proprietà. Selezionare la voce installa, poi scegliere protocollo e cliccare su aggiungi. Selezionare a questo punto Disco Driver ed indicare il percorso C:\raspppoe (dove al solito C: è l'unità Hard Disk e la directory raspppoe contiene i file scompattati). Vi verrà proposto di installare il PPP over Ethernet protocol. Rispondere affermativamente alle successive richieste (relative alla firma digitale assente). Cliccare su chiudi. Aprire la cartella C:\Windows2000\System32 e cliccare due volte sul file raspppoe.exe. Apparirà una schermata nella quale è necessario selezionare la scheda di rete cui è connesso l'I-Storm; a questo punto cliccare una volta su Create a Dial-Up connection for the selected Adapter ed infine scegliamo exit. Il processo è terminato ed è stata creata un'icona che basterà cliccare per azionare il collegamento ad internet.

RFC 1483 Bridge su macchine LINUX

Problema	Soluzione
Avendo un abbonamento di tipo PPPoE voglio utilizzare il Router in modalità RFC 1483 Bridge con una macchina Linux. Come posso fare?	Per Linux è necessario installare un software chiamato Roaming's Pinguins.

Le performance del Router non sono brillanti?

Problema	Azioni correttive
Le performance in download o in upload non sono allineate col tipo di contratto offerto dall'ISP.	Assicurarsi che il cavo ADSL sia (in ogni suo punto) ad almeno 30cm da qualsiasi alimentatore. Allontanare il Router da qualsiasi apparecchio che possa generare campi elettromagnetici (case con lo chassis aperto, monitor CRT, cellulari) ed interferire. Qualora non si ottenesse il risultato sperato controllare il proprio contratto (vedere la banda minima garantita) ed eventualmente contattare l'ISP. Se i problemi continuassero, contattare l'assistenza tecnica

Come posso abilitare la funzionalità SPI?

Quesito	Risposta
Voglio accrescere la sicurezza dle Router abilitando la funzionalità SPI?	Tale funzionalità consente, utilizzando l'hardware del Router, di impedire ogni tipo di accesso indesiderato. Per abilitarla è sufficiente entrare nel router e configurare la sezione Intrusion Detection del Firewall. Con questa funzionalità attiva l'interà Lan sarà ulteriormente protetta poiché ogni pacchetto in transito viene esaminato a fondo e tutti i pacchetti di risposta vengono confrontati ed esaminati prima di essere inoltrati (di ogni pacchetto viene fatto una sorta di hash particolare che ne certifica l'autenticità). **Nota Bene:** Alcune applicazioni internet potrebbero non funzionare correttamente con tale funzionalità attivata.

Cos'è il DHCP Relay?

Quesito	Risposta
Cos'è il DHCP Relay ed a cosa mi serve?	Settando questa funzionalità il servizio DHCP passa attraverso il Router I-Storm e raggiunge altri server che assegnano alla Lan i vari indirizzi IP. Se questa funzionalità non fosse disponibile questi PC sarebbero impossibilitati ad accedere al server DHCP. Al solito ogni PC che necessità di un indirizzo IP si mette in contatto con un server DHCP (in questo caso fuori dalla LAN) e da questo riceve: IP, Subnet. DG, DNS. Questi indirizzi IP sono dinamici, nel senso che hanno un tempo di validità. Scaduto questo termine il client DHCP ricontatterà il server per riottenere un nuovo IP.

Cos'è l'IDLE Time?

Quesito	Risposta
A cosa serve l'IDLE Time?	Il router ADSL stacca la connessione se non c'è traffico sulla connessione per un intervallo stabilito espresso in minuti (il che significa che nessun pacchetto, di alcun genere, è stato indirizzato dal Router verso Internet). E' possibile scegliere **Always On** per mantenere sempre alta la connessione (in PPPoA e PPPoE se tale modalità è abilitata il Routert ADSL alzerà nuovamente la connessione se questa dovesse cadere). Consigliamo di non utilizzare l'IDLE Time e mantenere il Router su Always ON a meno che non abbiate un abbonamento a tempo (attenzione in quel caso a monitorare la connessione che verrà rialzata non appena un pacchetto sarà indirizzato, da un qualsiasi PC, verso un indirizzo diverso dalla subnet di appartenenza). Fate attenzione, nel caso di abbonamenti a tempo, anche alla sezione Check Emails.

Perché il Router si connette automaticamente all'ISP?

Quesito	Risposta
Perché il Router si connette automaticamente all'ISP?	Il Router ADSL genera una connessione quando un PC della Lan invia un pacchetto (funzione di Dial on Demand) indirizzato ad un indirizzo IP differente da quello della sua (sue nel caso usaste il doppio IP) classe di appartenenza (che è poi la subnet della Lan). Questo fenomeno deve essere controllato in caso di abbonamento non Flat.

Cos'è un attacco Denial of Service?

Quesito	Risposta
Che caratteristiche ha un attacco Denial of Service?	Lo scopo di attacchi di questo tipo non è quello di cogliere informazioni particolari dalla vostra rete quanto piuttosto renderla inutilizzabile per un certo periodo di tempo. Più precisamente esistono 4 specifici tipologie di attacchi DoS. **1**-Attacchi che mirano all'esaurimento della banda, sono realizzabili in due modalità diverse a seconda di quanta banda abbia l'attaccante. Qualora la banda sia maggiore dell'attaccato può saturarlo diversamente può usare altri host che di fatto amplificano l'attacco. **2**-Attacchi che mirano all'esaurimento delle risorse. **3**-Attacchi contro difetti di programmazione, che mirano a sfruttare bug software o hardware. **4**-Attacchi DoS generici. Il Router può automaticamente accorgersi e bloccare un attacco di tipo DoS (Denial of Service) se questa funzione è attiva. Vengono riconosciuti oltre 15 tipi diversi di patterns tra i quali: IP Spoofing, IP with zero length, Ping of Death(Length>65535),Land Attack (Same source / destination IP address), Sync flooding ,Smurf Attack (ICMP Echo with x.x.x.0 or x.x.x.255), Snork Attack, UDP port loop-back, TCP NULL scan, Back Orifice Scan, Net Bus Scan TCP XMAS Scan, WinNuke Attack, IMAP SYN/FIN scan.

Come posso impedire ad un gruppo di utenti di andare in Internet?

Quesito	Risposta
Come posso impedire ad un gruppo di utenti di andare in Internet mentre altri hanno completo accesso?	Vi sono 2 possibili alternative: Utilizzare il MAC Filter, è però necessario conoscere l'indirizzo MAC dei PC in questione (o di tutti gli altri cui è consentito, dipende dal numero dei 2 gruppi). Anzitutto è necessario assegnare ai PC che si vogliono limitare degli indirizzi IP fissi e disabilitare così, qualora fosse attivo, il client DHCP (benché potreste utilizzare la funzionalità Fixed Host, ma dovreste conoscere i vari Mac address). In questo modo, avendo sempre i medesimi indirizzi IP potremo operare correttamente (si ricorda che invece se fossero client DHCP l'indirizzo IP potrebbe mutare). L'idea da seguire sono le seguenti: Utenti appartenenti al **gruppo A** saranno filtrati ed Utenti appartenenti al **gruppo B** avranno invece accesso senza alcuna limitazione a tutti i servizi internet (compatibili con il livello di sicurezza impostato). Per ottenere questo sceglieremo (creeremo) nel firewall dell'**Hamlet** il livello di sicurezza opportuno (tutta una serie di regole che consentiranno il passaggio dei servizi ritenuti necessari) . Andremo poi nella sezione racket Filter-Address Filter e metteremo gli IP da bloccare. Volendo è possibile mettere un indirizzo IP e la sua subnet.

segue:

	Scelta dei gruppi (opzionale per evitare di introdurre tutti gli IP uno per uno). E' opportuno per evitare errori scrivere gli indirizzi IP in modalità binaria così come la subnet mask. Facciamo un esempio il numere decimale **44** in binario diviene **00101100** (il valore più a sinistra rappresenta 2 elevato alla zero, il secondo 2 elevato alla 1. In questo esempio avremo 2 elevato alla seconda cui sommare due elevato alla 3 più due elevato alla 5). La subnet mask **248** è **11111000**. Quindi mettere come IP=192.168.1.44 e subnet mask=255.255.255.248 significa indicare in binario tutti quegli IP che cambiano nei soli ultimi 3 bit (000,001....111). Quando infatti la subnet mask ha valore 1 (255 in decimale corrisponde ad una sequenza di 8 uni in binario) il corrispondente bit dell'indirizzo IP non deve mutare. Cioè da 192.168.1.40 sino 192.168.1.47. Se avessimo usato come subnet 252 (11111100) avremmo potuto cambiare solo gli ultimi 2 bit pertano avremmo avuto da 192.168.1.44 a 192.168.1.47. Resta inteso che i gruppi, per via delle subnet, sono solo nei seguenti multipli:2,4,8,16,32,64,128 o 255. Nel caso, ad esempio, con 3 utenti si può mettere 192.168.1.1 e mettere subnet 255.255.255.252 in questo modo si settano i primi 4 (192.168.1.1, 192.168.1.2, 192.168.1.3) oppure mettendo 255.255.255.248 si arriva sino al 192.168.1.7. Tutti gli altri IP (sino 253) non saranno filtrati e potranno essere assegnati ai PC che non hanno limitazioni.

Cos'è il DDNS?

Quesito	Risposta
A cosa serve il DDNS?	Tramite questa funzionalità è possibile registrare un dominio ed associarlo ad un IP dinamico. Ogni qual volta il Router si riconnettera, tramite il client incorporato, comunicherà al server DNS il nuovo indirizzo IP. Associando tale funzionalità con il Virtual Server è possibile (ad esempio) ospitare un sito WEB sul proprio PC, effettuare configurazioni da remoto e utilizzare il Router come server VPN. I passaggi da seguire sono i seguenti: 1-Registrare il proprio dominio(ad esempio) gratuitamente www.dyndns.org, www.zoneedit.com. L'operazione richiederà qualche minuto. 2-Configurare il client sull'I-Storm Router ADSL inserendo i campi appropriati (Domain Name, Username e Password). Attenzione alla configurazione del campo Period (il Router aggiorna il server DDNS usando come parametro il campo Period, olte che ogni volta che riceve dalla sfida PPP un nuovo indirizzo IP) nel rispetto delle policy del gestore DDNS. 3-Predisporre il PC che deve fungere da Server Web o configuare il Router affinché sia gestibile da remoto o configurarlo come server VPN. 4-Configurare il Virtual Server affinché rigiri sull'indirizzo IP del PC (di sopra) predisposto le connessioni provenienti dall'esterno In questo modo ogni utente che voglia connettersi al vostro dominio interrogherà il server DDNS che gli restituirà di volta in volta l'indirizzo IP assegnatovi dall'ISP. Usando la funzionalità di riconnessione (disponibile in PPPoA e PPPoE), qualora la connessione dovesse cadere, il Router la rialzerà immediatamente. In questo modo se il PC resta sempre acceso il server WEB è di fatto sempre raggiungibile (se si escludono problemi diversi).

Appendice A

Dynamic DNS

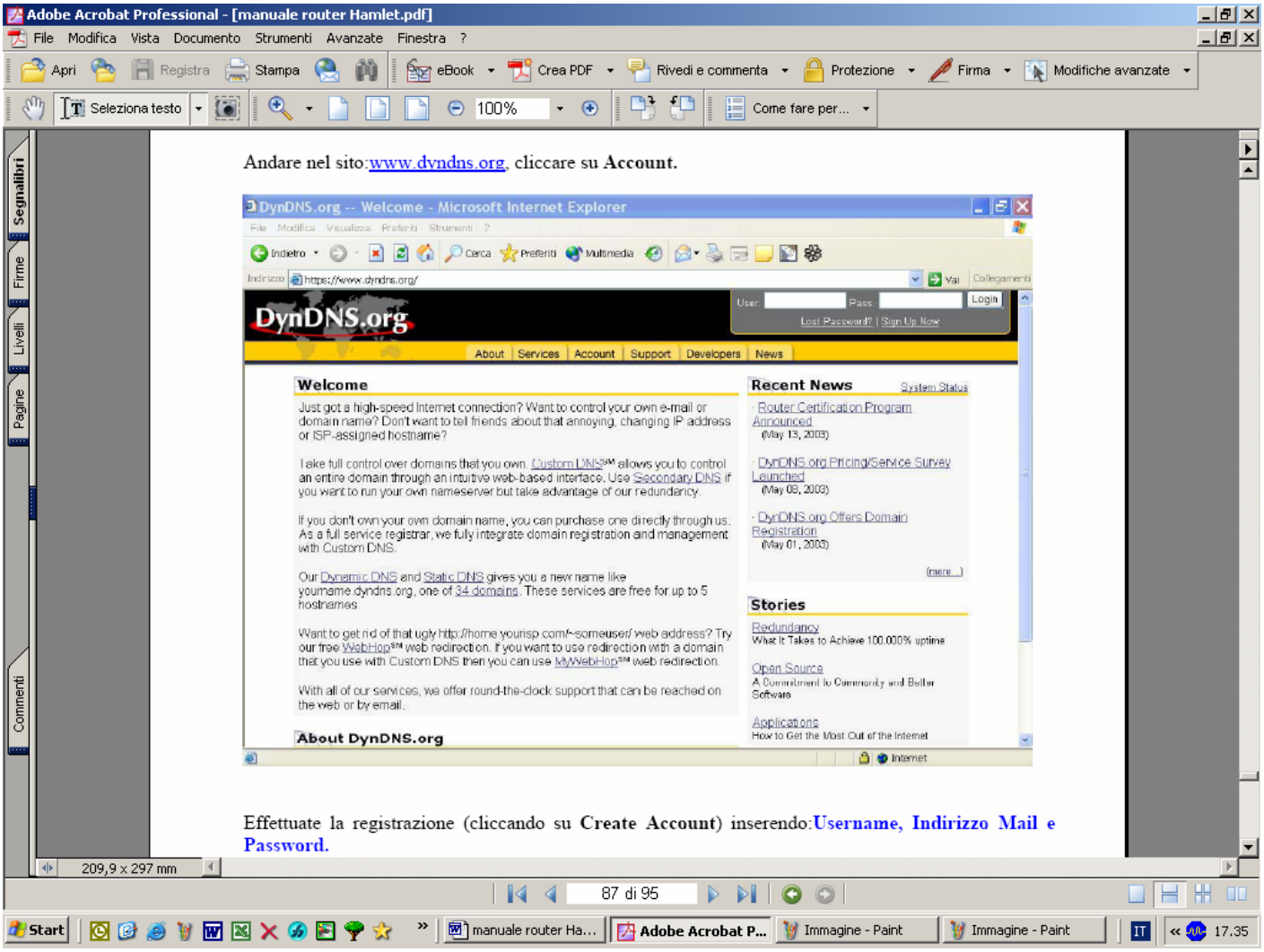
Grazie all'adozione di questa features è possibile registrare un dominio pur se associato ad un IP dinamico. Ci sono una moltitudine di server DDNS che offrono gratuitamente questo tipo di servizio.

Sarà sufficiente registrarsi per attivare in maniera gratuita ed immediata il servizio che vi consentirà di raggiungere (da remoto) sempre il Router. Potrete in questo modo effettuare facilmente configurazioni da remoto, ospitare il vostro sito WEB o utilizzare il Router come server VPN.

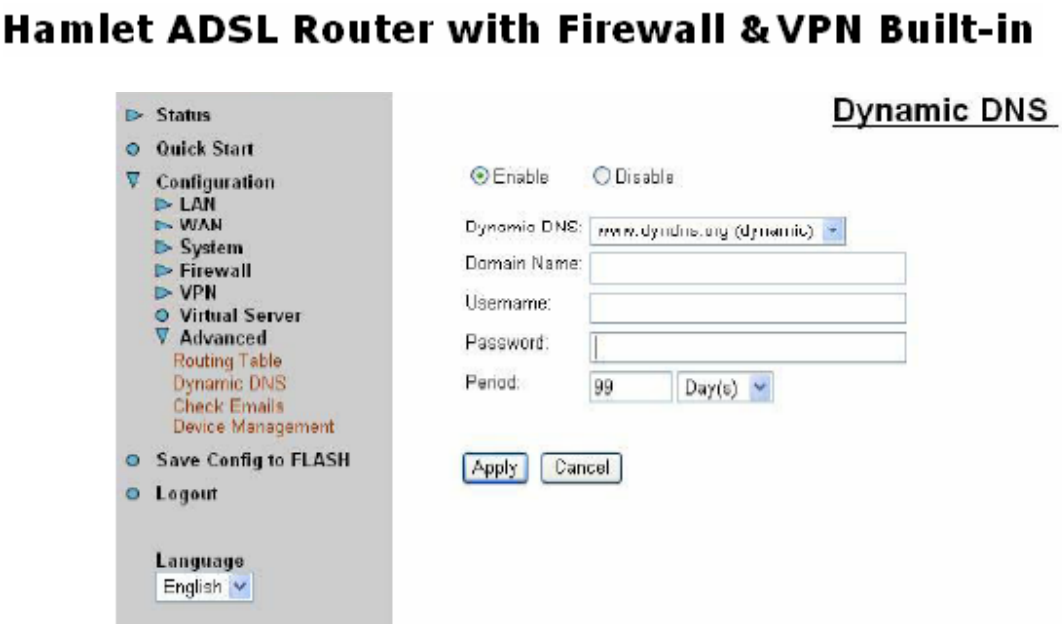
Ogni qual volta il Router si riconnetterà, tramite il client incorporato, comunicherà al server DDNS il nuovo indirizzo IP. In questo modo chiunque dall'esterno conoscendo l'URL saprà l'indirizzo IP che in quel momento è stato assegnato al Router.

Vediamo, nel dettaglio come effettuare una registrazione con il gestore DDNS forse più famoso.

Andare nel sito:www.dyndns.org, cliccare su **Account.**



Effettuate la registrazione (cliccando su **Create Account**) inserendo:**Username, Indirizzo Mail e Password.**
Vi verrà spedita immediatamente una mail, con le istruzioni per proseguire la registrazione e confermare così il tutto entro 48 ore. Seguite le istruzioni contenute e compilate il form per terminare la fase di registrazione.
A questo punto riloggatevi nel sito, andate su **Services**, evidenziate (nella parte sinistra) il menù **Dynamic DNS** e poi cliccate su **Add Host**.
Non vi resta che introdurre il **Nome dell'host** (evidenziare Enable WildCard) e scegliere il suffisso che più preferite e premere poi sul bottone **Add Host** per terminare.
Passiamo adesso alla configurazione del client nel Router (nella sezione **DynDNS**, **Configuration/Advanced**).



Spuntate il bottone **Enable.**

Alla voce Dynamic DNS scegliete, dalla combo box, **www.dyndns.org(dynamic**).
Compilate il campo **Domain Name** inserendo per esteso il dominio registrato e inserite poi **Username** e **Password**.
Impostate il campo **Period** su 99 Days (come da figura).
Non vi resta che premere su **Apply** e poi su **Save Config to FLASH** per rendere permanenti le modifiche.
Andando sul sito www.dyndns.org, (effettuare il LogIn ed andare nella sezione Account poi sotto Dynamic DNS al vostro URL) potrete controllare che l'IP sia stato aggiornato (alternativamente potrete effettuare un ping verso il vostro URL).

Appendice B

Packet Filter

Il Router dispone di un sofisticato Packet Filter col quale riesce ad esaminare tutto il traffico che lo attraversa. In questo modo è possibile, conoscendo le caratteristiche dei pacchetti IP associati ai più comuni servizi, effettuare i filtraggi in maniera corretta. In questa appendice vedremo come i pacchetti di un servizio possono cambiare.

Utilizzeremo le seguenti convenzioni:

• **BLU** per indicare una INVERSIONE

• Utilizzeremo il **ROSSO** per indicare un CAMBIAMENTO

Per cercare di comprendere a fondo come le modifiche che subisce un pacchetto IP immaginiamo di trovarci nelle seguenti condizioni:

- NAT attivo
- PCX della LAN con IP 192.168.1.X
- Router con LAN IP 192.168.1.254

Mettiamoci nel caso in cui il PCX voglia vedere un sito WEB. Vediamo nel dettaglio tutti i pacchetti nei vari stadi.

Vi sono 2 fasi:Risoluzione dell'URL (tale valore potrebbe essere recuperato in qualche cache o fornito da appositi programmi,ma per completezza immaginiamo il caso più comune) e costruzione della connessione TCP col sito WEB.

Il primo pacchetto è inviato dal PCX (con IP 192.168.1.X) verso il server DNS per chiedere la risoluzione dell'URL cercato.

	Direzione Pacchetto	PC-Router[Uscente]	
IP	IP Provenienza	192.168.1.X	
	IP Destinazione	IP del Server DNS	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	C	
	Porta Destinazione	53	

Questo pacchetto uscente arriva al Router che (essendo abilitato il NAT), ne cambia l'indirizzo di provenienza mettendovi il suo Pubblico e lo inoltra al server DNS)

	Direzione Pacchetto	Router-Internet[Uscente]	
IP	IP Provenienza	**IP lato WAN del Router**	
	IP Destinazione	IP del Server DNS	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	C	
	Porta Destinazione	53	

Arrivato al server DNS il pacchetto torna indietro, reindirizzato al Router (ricordate ne aveva cambiato prima l'IP di provenienza). Sono invertiti sia a livello IP i campi IP prov con IP dest e sia le porte nel livello UDP.

	Direzione Pacchetto	Internet-Router[Entrante]	
IP	IP Provenienza	**IP del Server DNS**	
	IP Destinazione	**IP lato WAN del Router**	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	**53**	
	Porta Destinazione	**C**	

Arrivato al Router il pacchetto viene riprocessato ed inviato all'IP di provenienza.

	Direzione Pacchetto	Internet-Router[Entrante]	
IP	IP Provenienza	IP del Server DNS	
	IP Destinazione	**192.168.1.X**	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	53	
	Porta Destinazione	C	

A questo punto, dal pacchetto UDP arrivato, il PCX (192.168.1.X) ha risolto l'URL e conosce l'indirizzo IP associato. Inizia dunque la fase della costruzione della connessione TCP (il protocollo TCP infatti richiede la costruzione della connessione, al contrario di quello UDP). Ci fermeremo solo fino a che il primo pacchetto non torna al nostro PC.

	Direzione Pacchetto	PC-Router[Uscente]	
IP	IP Provenienza	192.168.1.X	
	IP Destinazione	IP URL	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	K	
	Porta Destinazione	80	

Questo pacchetto uscente arriva al Router che (essendo abilitato il NAT), ne cambia l'indirizzo di provenienza mettendovi il suo Pubblico e lo inoltra al server WEB).

	Direzione Pacchetto	Router-Internet[Uscente]	
IP	IP Provenienza	**IP lato WAN del Router**	
	IP Destinazione	IP URL	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	K	
	Porta Destinazione	80	

Arrivato al server WEB il pacchetto torna indietro, reindirizzato al Router (che ne aveva cambiato prima l'IP di provenienza). Vengono invertiti sia a livello IP i campi IP prov con IP dest e sia le porte nel livello TCP.

	Direzione Pacchetto	Internet- Router [Entrante]	
IP	IP Provenienza	**IP URL**	
	IP Destinazione	**IP lato WAN del Router**	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	**80**	
	Porta Destinazione	**K**	

Arrivato al Router il pacchetto viene riprocessato ed inviato all'IP di provenienza.

	Direzione Pacchetto	Router-PC[Entrante]	
IP	IP Provenienza	IP URL	
	IP Destinazione	**192.168.1.X**	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	80	
	Porta Destinazione	K	

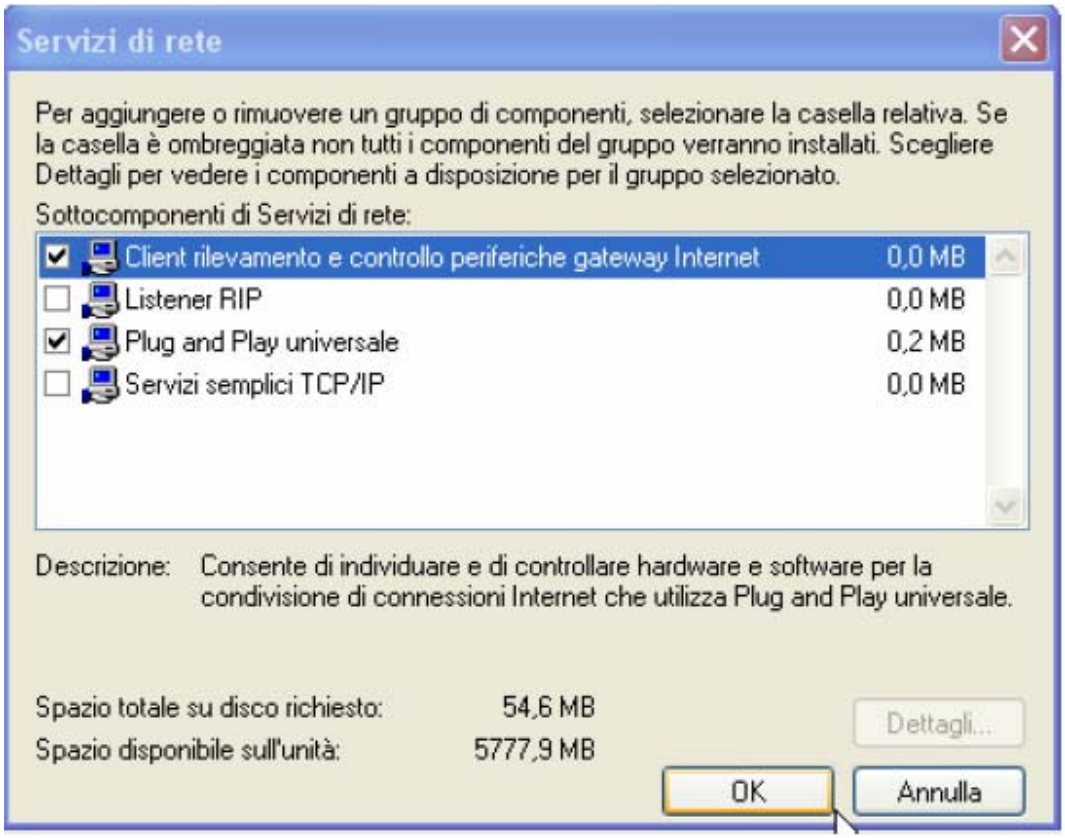
Abbiamo visto il percorso dei pacchetti e le loro trasformazioni. Nell'esempio di sopra si sono utilizzati dei parametri C e K. Sono dei numeri interi >1024. Nei protocolli per porta quali TCP/UDP infatti il mittente parla ad una porta di destinazione (su cui è in ascolto il server) ed indica una porta (la porta di provenienza appunto) dove aspetta la risposta. Il pacchetto una volta ricevuto dal server viene rinviato al mittente avendo e sulla porta su cui questo aspetta la risposta. A livello IP viene effettuato lo stesso percorso.

Appendice C

UPnP

Grazie alla funzionalità UpnP potrete configurare facilmente tutte quelle applicazioni che hanno problemi nell'attraversamento del NAT. L'utilizzo del NAT Trasversale renderà le applicazioni in grado di autoconfigurarsi automaticamente senza l'intervento dell'utente. Chiunque dunque sarà in grado, senza conoscere complicati concetti, di godere pienamente dei vantaggi del NAT e contemporaneamente utilizzare le più comuni applicazioni Internet senza il minimo problema.

Pannello di Controllo poi **Installa applicazioni**, scegliere **Installazione Componenti di Windows**. Selezionare **Servizi di Rete** e poi cliccare su **Dettagli**. Assicuratevi che siano spuntate le seguenti voci: **Plug and Play Universale** e **Client rilevamento e controllo periferiche Gateway Internet**.



Andando su **Risorse di Rete** dovreste trovare il nome del campo **Set Host Name**. Ciccandoci sopra entrerete nella configurazione del Router ADSL (alla stessa maniera di quando ne digitate l'IP nell'URL di IE). Cliccando il tasto destro e poi Proprietà avrete accesso ad informazioni supplementari. Andando su **Pannello di Controllo** e poi **Connessioni di rete** dovreste trovare l'icona **Connessione Internet**. Cliccandoci 2 volte vedrete l'immagine a fianco:

Scegliendo **proprietà** e poi **impostazioni** effettuerete le configurazioni necessarie all'uso dell'UpnP. Infatti vi basterà premere aggiungi per creare una sorta di Virtual Server per l'applicazione del caso.

Descrizione del Servizio=identificativo

Nome o Indirizzo IP=IP del PC su cui risiede il server

Numero di porta esterna del servizio=immettere la porta esterna (es 80 per http, 20-21 per FTP)

Numero di porta interna del servizio=immettere la porta interna

Scegliere il protocollo tra **UDP** o **TCP**.
Premendo OK il protocollo UpnP dialogherà col Router.

Andando sotto la sezione Status e poi UpnP Port Map potrete vedere questi nuovi settaggi.

UPnP Portmap

Name	Protocol	Start Port	End Port	IP Address
emwebigd1	tcp	80	80	192.168.1.1
emwebigd3	tcp	20	20	192.168.1.1
emwebigd5	tcp	21	21	192.168.1.1

In questa modalità potrete configurare una sorta di **Virtual Server** da ogni PC senza accedere al Router vero e proprio.
Alcune applicazioni sono da sole in grado di configurare in maniera autonoma il servizio UpnP.
Questo renderà tali applicazioni fruibili da chiunque.

N.B.:

É necessario configurare il Router Hamlet affinché utilizzi una porta superiore a 1024 (Windows XP altrimenti non funzionerebbe correttamente).