

# I-Storm Lan Router ADSL

with Firewall & VPN

A02-RA3+



## I-Storm Lan Router ADSL with Firewall & VPN

A02-RA3+

Manuale Completo  
V1.0



Company certified ISO 9001:2000



**AVVERTENZE**

Abbiamo fatto di tutto al fine di evitare che nel testo, nelle immagini e nelle tabelle presenti in questo manuale, nel software e nell'hardware fossero presenti degli errori. Tuttavia, non possiamo garantire che non siano presenti errori e/o omissioni e vi preghiamo di segnalarceli. Infine, non possiamo essere ritenuti responsabili per qualsiasi perdita, danno o incomprensione compiuti direttamente o indirettamente, come risulta dall'utilizzo del nostro manuale, software e/o hardware.

Il contenuto di questo manuale è fornito esclusivamente per uso informale, è soggetto a cambiamenti senza preavviso (a tal fine si invita a consultare il sito [www.atlantisland.it](http://www.atlantisland.it) o [www.atlantis-land.com](http://www.atlantis-land.com) per reperirne gli aggiornamenti) e non deve essere interpretato come un impegno da parte di Atlantis Land spa che non si assume responsabilità per qualsiasi errore o inesattezza che possa apparire in questo manuale. Nessuna parte di questa pubblicazione può essere riprodotta o trasmessa in altra forma o con qualsiasi mezzo, elettronicamente o meccanicamente, comprese fotocopie, riproduzioni, o registrazioni in un sistema di salvataggio, oppure tradotti in altra lingua e in altra forma senza un espresso permesso scritto da parte di Atlantis Land spa. Tutti i nomi di produttori e dei prodotti e qualsiasi marchio, registrato o meno, menzionati in questo manuale sono usati al solo scopo identificativo e rimangono proprietà esclusiva dei loro rispettivi proprietari.

**CE Mark Warning**

Questo dispositivo appartiene alla classe B. In un ambiente domestico il dispositivo può causare interferenze radio, in questo caso è opportuno prendere le adeguate contromisure.



# INDICE

## CAPITOLO 1 ..... 1

1.1 PANORAMICA DELL'I-STORM LAN ROUTER ADSL .....	1
1.2 CONTENUTO DELLA CONFEZIONE .....	2
1.3 CARATTERISTICHE DELL'I-STORM ADSL FIREWALL ROUTER .....	2
1.4 SCHEMA DI INSTALLAZIONE DELL'I-STORM ADSL FIREWALL ROUTER .....	4

## CAPITOLO 2 ..... 6

2.1 PRECAUZIONI NELL'USO DELL'I-STORM ADSL FIREWALL ROUTER .....	6
2.2 I LED FRONTALI .....	6
2.3 LE PORTE POSTERIORI .....	7
2.4 CABLAGGIO .....	7

## CAPITOLO 3 ..... 8

3.1 PRIMA DI INIZIARE .....	8
3.2 COLLEGARE L'I-STORM LAN ROUTER ADSL .....	8
3.3 CONFIGURAZIONE DEI PC .....	9
<i>Configurazione del PC in Windows 95/98/ME</i> .....	9
<i>Configurazione del PC in Windows NT4.0</i> .....	11
<i>Configurazione del PC in Windows 2000</i> .....	12
<i>Configurazione del PC in Windows XP</i> .....	14
<i>Configurazione in ambiente MAC</i> .....	16
3.4 VERIFICA .....	17
3.5 CONFIGURAZIONE DEL BROWSER .....	17
3.6 SETTAGGI DI DEFAULT .....	18
3.6.1 <i>Recupero Password</i> .....	18
3.6.2 <i>Porte LAN e WAN</i> .....	19
3.7 INFORMAZIONE SULL'ISP .....	19
3.8 CONFIGURAZIONE DEL ROUTER TRAMITE BROWSER .....	19
3.8.1 <i>STATUS</i> .....	21
Host Name .....	22
Current Time .....	22
IP Address .....	23
DHCP Server .....	23
WAN Settings .....	23
DNS .....	23
Port Status(Ethernet) .....	23
Port Status(ADSL) .....	23
Statistics .....	23
3.8.2 <i>CONFIGURATION</i> .....	23
3.8.2.1 LAN .....	23
3.8.2.1.1 Ethernet .....	24
3.8.2.1.2 Port Settings .....	25
3.8.2.1.3 DHCP Server .....	26
3.8.2.2 WAN .....	27
3.8.2.2.1 ISP .....	27



- 3.8.2.2.2 DNS..... 38
- 3.8.2.3 SYSTEM..... 39
  - 3.8.2.3.1 Time Zone..... 39
  - 3.8.2.3.2 Remote Access..... 40
  - 3.8.2.3.3 Firmware Upgrade..... 40
  - 3.8.2.3.4 Backup / Restore..... 41
  - 3.8.2.3.5 Restart Router..... 42
  - 3.8.2.3.6 User Management..... 42
- 3.8.2.4 Firewall..... 44
  - 3.8.2.4.1 General Settings/Packet Filter..... 44
  - 3.8.2.4.2 Intrusion Detection..... 48
  - 3.8.2.4.3 MAC Address Filter..... 51
  - 3.8.2.4.4 URL Filter..... 52
  - 3.8.2.4.5 Firewall Log..... 54
- 3.8.2.5 VPN..... 55
  - 3.8.2.5.1 PPTP VPN – Remote Access (Dial-In)..... 56
  - 3.8.2.5.2 PPTP VPN – Remote Access (Dial-Out)..... 63
  - 3.8.2.5.3 PPTP VPN – Lan to Lan..... 65
  - 3.8.2.5.4 IPsec VPN..... 68
- 3.8.2.6 QoS..... 73
  - 3.8.2.6.1 Prioritization..... 73
  - 3.8.2.6.2 IP Throttling..... 74
- 3.8.2.7 Virtual Server..... 75
- 3.8.2.8 Advanced..... 79
  - 3.8.2.8.1 Routing Table..... 79
  - 3.8.2.8.2 Dynamic DNS..... 80
  - 3.8.2.8.3 Check Emails..... 81
  - 3.8.2.8.4 Device Management..... 81
- 3.8.3 Save Config to FLASH..... 83
- 3.8.4 Logout..... 83
- 3.9 CONSOLE E/O TELNET..... 84

# CAPITOLO 4..... 88

- PROBLEMI ALLA PARTENZA DELL’I-STORM ADSL ROUTER..... 88
- PASSWORD?..... 88
- NON È POSSIBILE ENTRARE NEL ROUTER VIA WEB..... 89
- PROBLEMI CON L’INTERFACCIA WAN..... 89
- PROBLEMI CON L’INTERFACCIA LAN..... 89
- PROBLEMI DI CONNESSIONE AD UN REMOTE NODE OPPURE AD UN ISP..... 90
- CONFLITTO DI INDIRIZZI IP..... 90
- IL ROUTER NON RIESCE AD ALLINEARSI?..... 90
- COS’È IL NAT?..... 91
- PERCORSO DEI PACCHETTI..... 91
- NON FUNZIONA CORRETTAMENTE UN’APPLICAZIONE INTERNET..... 92
- PERCHÉ NONOSTANTE IL VS ALCUNE APPLICAZIONI NON VANNO?..... 93
- PERCHÉ NONOSTANTE LA DMZ ALCUNE APPLICAZIONI NON VANNO?..... 93
- RFC 1483 BRIDGE SU MAC OS 9..... 93
- RFC 1483 BRIDGE SU MAC OS X..... 94
- RFC 1483 BRIDGE SU MACCHINE WINDOWS 95, 98, ME..... 95
- RFC 1483 BRIDGE SU MACCHINE WINDOWS 2000..... 96
- RFC 1483 BRIDGE SU MACCHINE LINUX..... 96



LE PERFORMANCE DEL ROUTER NON SONO BRILLANTI? ..... 97  
COME POSSO ABILITARE LA FUNZIONALITÀ SPI? ..... 97  
COS'È IL DHCP RELAY? ..... 97  
COS'È L'IDLE TIME? ..... 98  
PERCHÉ IL ROUTER SI CONNETTE AUTOMATICAMENTE ALL'ISP? ..... 98  
COS'È UN ATTACCO DENIAL OF SERVICE? ..... 99  
COME POSSO IMPEDIRE AD UN GRUPPO DI UTENTI DI ANDARE IN INTERNET? ..... 100  
COS'È IL DDNS? ..... 101

**APPENDICE A ..... 102**

DYNAMIC DNS ..... 102

**APPENDICE B ..... 104**

PACKET FILTER ..... 104

**APPENDICE C ..... 107**

UPnP ..... 107

**APPENDICE D ..... 110**

TRAFFIC SHAPING ..... 110

**APPENDICE E ..... 111**

CARATTERISTICHE TECNICHE ..... 111

**APPENDICE F ..... 112**

SUPPORTO OFFERTO ..... 112



# Capitolo 1

## Introduzione

Questo manuale è stato pensato per un utilizzo avanzato del Router ADSL, per questo sono stati trattati con dovizia di particolari una moltitudine di argomenti che potrebbero, almeno inizialmente, essere di difficile comprensione.

Per una configurazione rapida è comunque disponibile una Guida all'Installazione presente sia su CDROM che su supporto cartaceo a corredo del prodotto. E' inoltre disponibile su CDROM (D:\Multimedia Guide) una **guida multimediale** (una serie di filmati con esempi di configurazione) utile per una rapida configurazione del dispositivo. Per una configurazione rapida (installazione e cablaggio, configurazione del PC e della connessione ADSL del Router) è sufficiente leggere, nel seguente manuale, i paragrafi 1.4 / 2.4 / 3.3 /3.6-7 e 3.8.2.2.

### 1.1 Panoramica dell'I-Storm Lan Router ADSL

#### Condivisione dell'Accesso ad Internet e dell'IP

L'I-Storm Lan Router ADSL dispone di 4 porte Fast Ethernet (con autonegoziazione 10/100Mbps) per la connessione alla Lan e consente, grazie al modem ADSL integrato, un downstream sino ad 8Mbps. Dotato di funzionalità NAT permette a diversi utenti di navigare in Internet e condividere simultaneamente la connessione ADSL usando un solo abbonamento con l'ISP ed un singolo indirizzo IP. E' inoltre possibile, tramite un semplice upgrade del firmware, aggiungere il supporto dello standard ADSL2.

#### Quality of Service e IP Throttling

Il Router ha la capacità di istradare con priorità prestabilite pacchetti in funzione della loro precedenza (IP e tipo di servizio). Sono proposte 3 classi di servizio. La velocità di navigazione non verrà più rallentata a causa dei programmi P2P utilizzati su altri computer. E' inoltre disponibile la funzionalità IP Throttling che permette un'assegnazione statica della banda (IP e tipo di servizio).

#### Firewall integrato (SPI, DoS) e VPN (IPSec, PPTP)

L'I-Storm Lan Router ADSL dispone di un sofisticato firewall integrato che, in aggiunta alla funzionalità NAT (che già rappresenta una prima difesa), offre anche funzionalità avanzate di ispezione dei pacchetti e URL blocking. Può infatti automaticamente riconoscere e bloccare gli attacchi di tipo Denial of Service (DoS) e grazie alla capacità di Stateful Packet Inspection (SPI) determina se un pacchetto dati che lo attraversa può essere inoltrato alla Lan. Ogni pacchetto infatti viene ispezionato a fondo e comparato coi pacchetti che sono riconosciuti come sicuri. Gestisce inoltre le VPN IPSec o PPTP facendosi carico dell'intero lavoro di autenticazione, confidenzialità ed integrità dei dati e consente pertanto di mettere in comunicazione sicura 2 LAN.



### Facile da usare e configurare

Tramite la comoda interfaccia Web è possibile accedere velocemente e facilmente a tutte le funzioni offerte dall'I-Storm LAN Router ADSL consentendo un risparmio di tempo. Il Router è configurabile anche tramite Telnet e Hyperterminal ed inoltre può essere configurato anche da remoto sia via Web che Telnet. Incorpora inoltre un client DynamicDNS.

## 1.2 Contenuto della Confezione

Una volta aperta la confezione in cartone dovrebbero esserci i seguenti componenti:

- I-Storm Lan Router ADSL
- CD-ROM contenente il manuale (Inglese, Italiano e Francese), le guide rapide (Inglese, Italiano, Francese, Tedesco e Spagnolo) e il firmware
- Guida di Quick Start multilingua (Inglese, Italiano, Francese, Tedesco e Spagnolo) stampata e/o su CD Rom
- Cavo RJ-11 ADSL
- Cavo CAT-5 LAN
- Cavo seriale RS232(DB9)-PS2
- Alimentatore AC-DC (12V DC@1A)

**Qualora mancasse uno qualsiasi di questi componenti è necessario rivolgersi immediatamente al rivenditore.**

## 1.3 Caratteristiche dell'I-Storm ADSL Firewall Router

Caratteristiche offerte dall'I-Storm ADSL Firewall Router:

- **ADSL Multi-Mode Standard:** Supporta in downstream un tasso di ricezione fino 8Mbps ed un tasso di trasmissione in upstream sino a 1024Kbps, inoltre soddisfa il Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G-lite (G992.2)).
- **Upgradeable ad ADSL2:** tramite un aggiornamento del firmware il dispositivo potrà essere reso compatibile con lo standard ADSL2 che consente in downstream un flusso fino 12Mbps.
- **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.
- **Quality of Service:** E' possibile assegnare ad ogni IP e servizio un livello di priorità. In questo modo il router processa determinati pacchetti provenienti da specifici IP con priorità. Questa caratteristica rende il dispositivo adatto ad espletare particolari servizi quali VoIP, Streaming Video etc..
- **IP Throttling:** E' possibile limitare per IP e servizio la banda massima utilizzabile ottenendo 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. E' 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 è possibile 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 : 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.atlantiland.it](http://www.atlantiland.it) o [www.atlantis-land.com](http://www.atlantis-land.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](http://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 permette di associare ad un indirizzo IP dinamico (che vi viene di volta in volta passato dal server dell'ISP) un nome statico (host-name). E' necessario, per utilizzare il servizio, effettuare una registrazione gratuita per esempio su <http://www.dyndns.org/>. Sono supportati oltre 8 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 dall'I-Storm ADSL Firewall Router 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.
- **VPN IPsec:** Il dispositivo integra inoltre un end-point IPsec.
- **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.
- **Virtual Server:** L'utente può specificare alcuni servizi che si rendono disponibili per utenti esterni. L'I-Storm ADSL Firewall Router può riconoscere le richieste entranti di questi servizi



e rigirarle all'opportuno PC della Lan. E' possibile, per esempio, assegnare una data funzione 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.

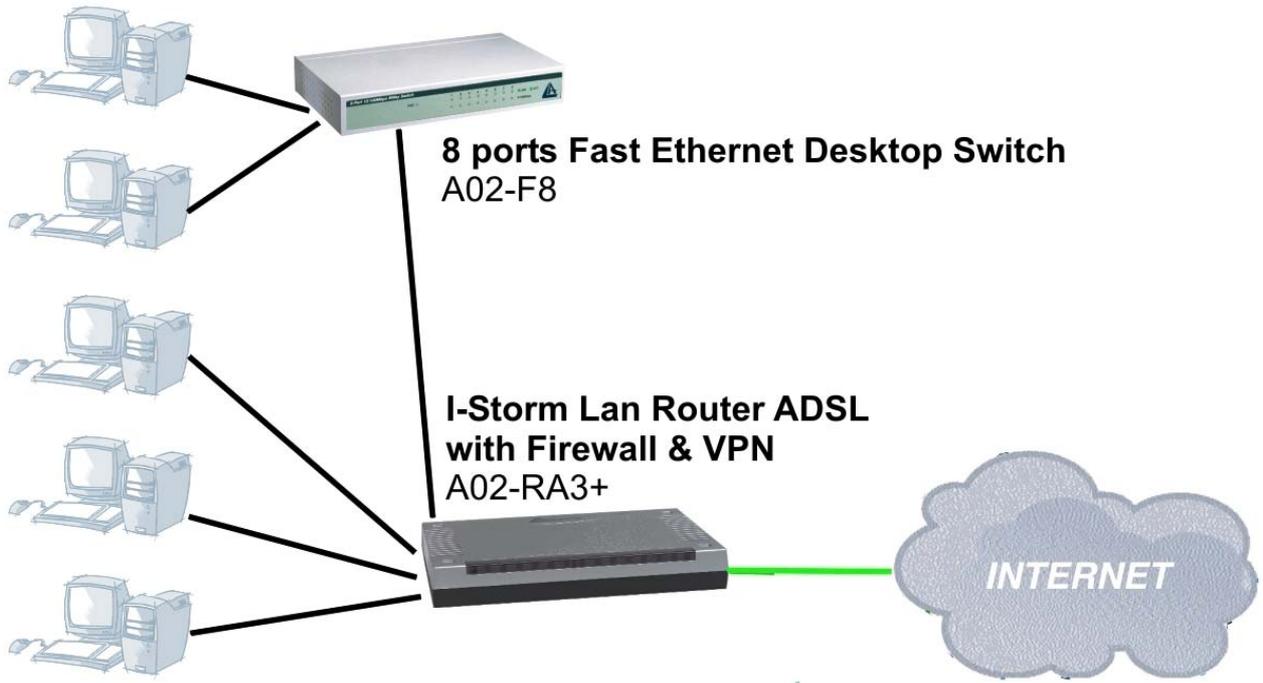
- **Dynamic Host Control Protocol (DHCP) client and server:** Lato WAN, il dispositivo può, grazie al DHCP client, prendere un indirizzo IP dall'ISP automaticamente. Nella LAN, il DHCP server può gestire sino a 253 client IP, distribuendo a ciascun PC un indirizzo IP, la subnet mask ed i DNS. Questa funzionalità consente una facile gestione della Lan.
- **Protocollo RIP1/2 per il Routing:** Supporto per 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. L'apparato 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 dell'I-Storm ADSL Firewall Router

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)
- L'I-Storm ADSL Firewall Router può essere collegato, tramite le 4 porte RJ45 (*LAN*), nelle seguenti modalità:
  - Direttamente a 4 **PC**, tramite cavi CAT 5 (in dotazione).
  - 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.
- E' possibile collegare l'I-Storm ADSL Firewall Router ad un PC tramite il cavo seriale (in dotazione tipo DB9-PS2) per configurarlo o effettuare operazioni di ripristino tramite la Console.

E' 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

### Uso dell'I-Storm ADSL Firewall Router

#### 2.1 Precauzioni nell'uso dell'I-Storm ADSL Firewall Router



Non usare il Router ADSL in un luogo in cui ci siano condizioni di alte temperatura ed umidità, il Router potrebbe funzionare in maniera impropria e danneggiarsi.

Non usare la stessa presa di corrente per connettere altri apparecchi al di fuori del Router ADSL.

Non aprire mai il case del Router ADSL né cercare di ripararlo da soli.

Se il Router ADSL dovesse essere troppo caldo, spegnerlo immediatamente e rivolgersi a personale qualificato.



Mettere il Router ADSL su una superficie piana e stabile.

Usare esclusivamente l'alimentatore fornito nella confezione, l'uso di altri alimentatori farà automaticamente decadere la garanzia.

#### 2.2 I LED frontali



LED		INFORMAZIONE
5	POWER	Acceso fisso quando connesso alla rete elettrica
6	SYS	Acceso fisso quando il sistema è pronto
8-11	LAN porta 1-4	Acceso quando connesso ad un dispositivo Ethernet Verde= connessione a 100Mbps Arancio= connessione a 10Mbps Lampeggiante quando vi è trasmissione/ricezione
12	ADSL	Acceso fisso quando connesso in modalità ADSL DSLAM. Lampeggiante durante la fase di allineamento.
13	PPP/MAIL	Acceso fisso quando una connessione PPPoE / PPPoA è attiva. Lampeggia quando tenta di costruire una connessione PPP. Spenta se si utilizza un protocollo diverso (RFC 1483 o 1577) Lampeggiante quando c'è una mail nell'account configurato.

## 2.3 Le PORTE posteriori



PORTE		UTILIZZO
1	<b>LINE (connettore RJ-11)</b>	Connettere il cavo RJ-11 a questa porta per effettuare l'allacciamento all'ADSL.
2	<b>PS2 (porta)</b>	Connettere il cavo PS2/DB9 fornito alla porta seriale (9 pin) del PC. Tale connessione è opzionale.
3	<b>LAN (4 connettori RJ-45)</b>	Connettere con un cavo UTP
4	<b>RESET</b>	Dopo che il dispositivo è acceso, premere per effettuare il reset o il restore. Le operazioni sono le seguenti: <b>0-3 secondi:</b> per resettare il dispositivo <b>3-6 secondi:</b> nessuna azione <b>10 secondi o più:</b> effettua un ritorno alle condizioni di default (utilizzare, per esempio, quando si è persa la password)
5	<b>POWER (Jack)</b>	Connettere l'alimentatore a questo jack
6	<b>POWER Switch</b>	Premere per accendere/spegnere il Router

## 2.4 Cablaggio

Il problema più comune è quello di un cattivo cablaggio per Ethernet o per la Lan. Accertarsi che tutti i dispositivi connessi siano accesi, usare inoltre i Led frontali per avere una diagnosi immediata dello stato del cablaggio. Controllare che siano accesi sia il Led Lan che quello ADSL (qualora così non fosse ricontrollate il cablaggio). Potete utilizzare qualunque tipologia di cavi (dritti o incrociati) per collegare il dispositivo.

Poiché l'ADSL ed il normale servizio telefonico si dividono (spesso) lo stesso filo per trasportare i rispettivi segnali è necessario, al fine di evitare interferenze dannose, dividere tramite un apposito filtro i 2 segnali. Tale filtro passa basso permetterà di estrarre la porzione di spettro utilizzata dal servizio telefonico impedendo così che la qualità di questo sia compromessa dalle alte frequenze introdotte dal segnale dell'ADSL. E' necessario pertanto utilizzare un filtro per ogni presa cui è collegato un telefono analogico. Esistono opportuni filtri che dispongono di 2 uscite (una PSTN ed una ADSL) e consentono di utilizzare sulla stessa presa sia un telefono analogico che il Router ADSL. Tale filtro non è incluso nella confezione e va acquistato separatamente. Atlantis Land raccomanda di utilizzare apparati certificati per il tipo di linee e consiglia la scelta del codice **A01-AF1** (filtro ADSL tripolare con omologazione Telecom Italia).



## Capitolo 3

# Configurazione

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

### 3.1 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. E' 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.

### 3.2 Collegare l'I-Storm Lan Router ADSL

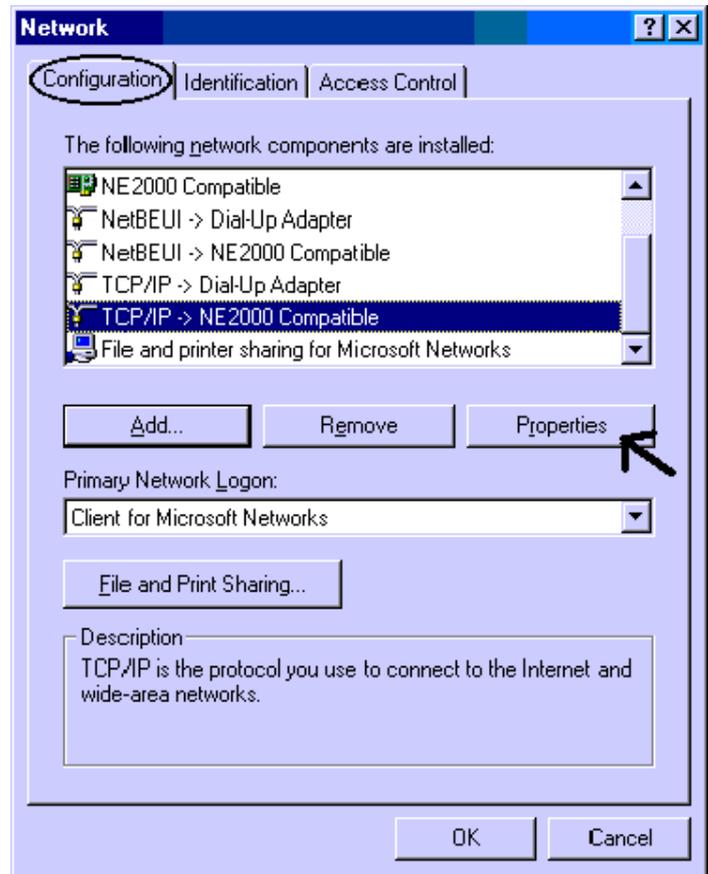
- Collegare il Router alla LAN, alla linea telefonica ed alla presa elettrica, tramite l'alimentatore fornito.
- Accendere il dispositivo.
- Accertarsi che i LED POWER e SYS siano accesi fissi. Controllare che i LED LAN siano accesi.
- Accertarsi che ogni software Firewall sia disinstallato dal PC.
- Passare adesso alla configurazione del TCP/IP sui vari PC.



## 3.3 Configurazione dei PC

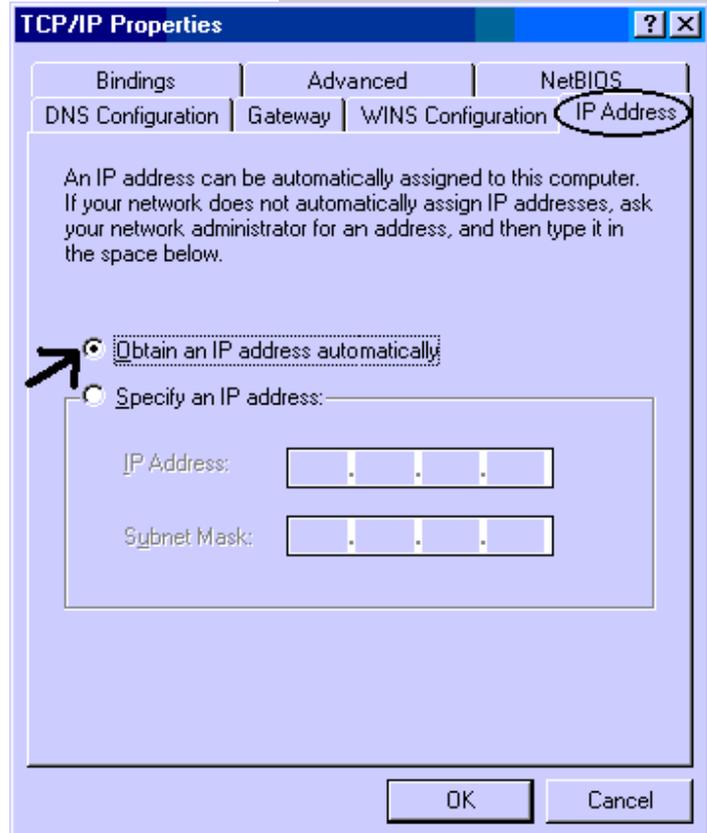
### Configurazione del PC in Windows 95/98/ME

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**.

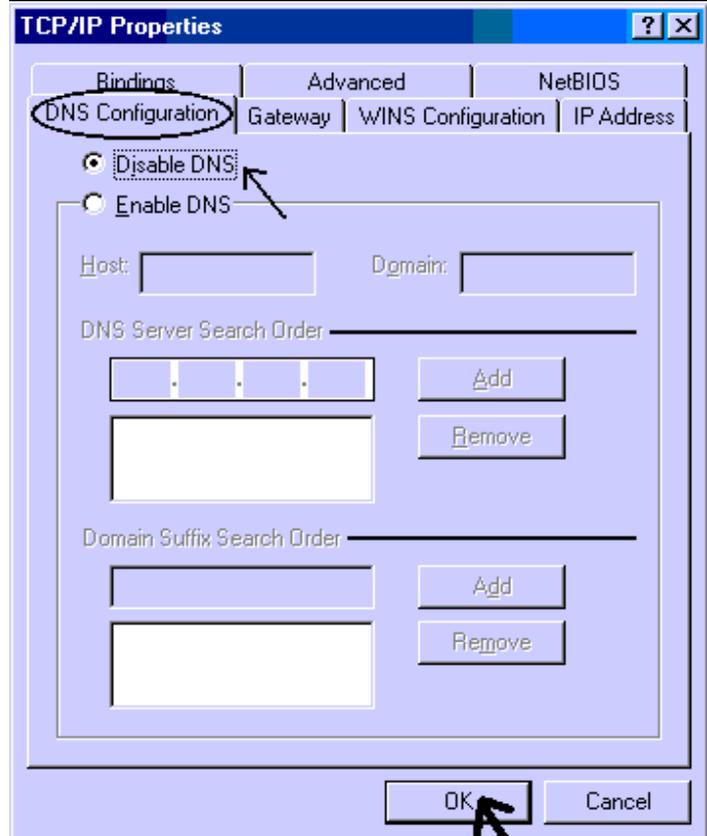




4. Selezionare l'opzione **Obtain an IP address automatically** (dopo aver scelto **IP Address**).



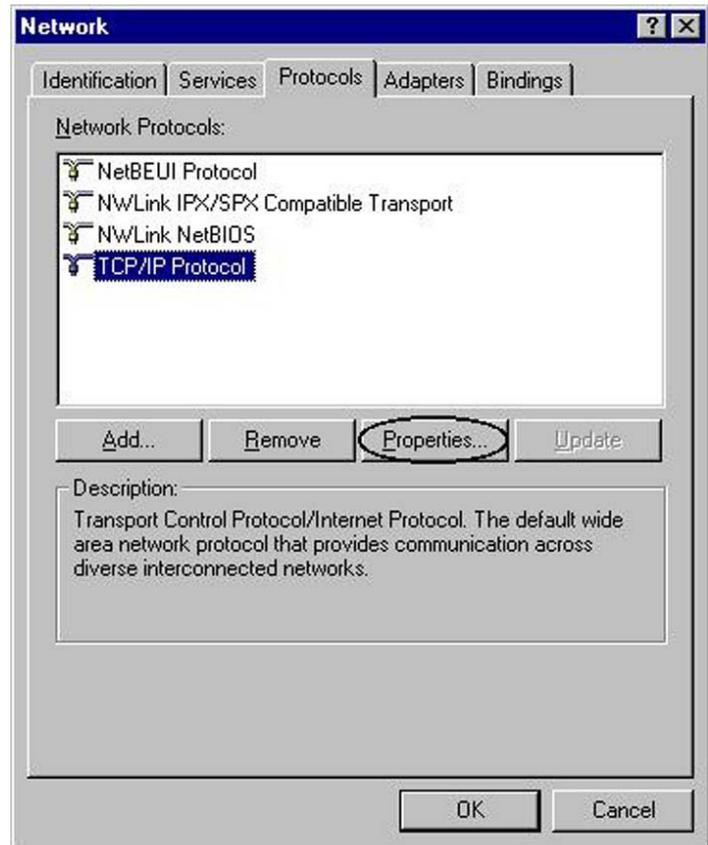
5. Andare su **DNS Configuration**
6. Selezionare l'opzione **Disable DNS** e premere su **OK** per terminare la configurazione.



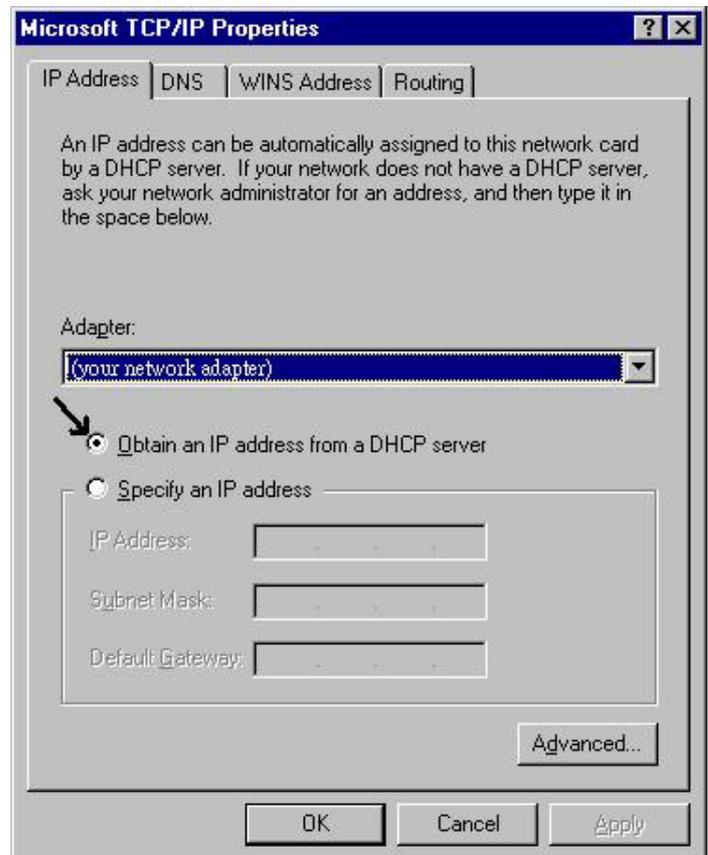


## Configurazione del PC in Windows NT4.0

1. Andare su **Start/Settings/Control Panel**. Cliccare per due volte su **Network** 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**.



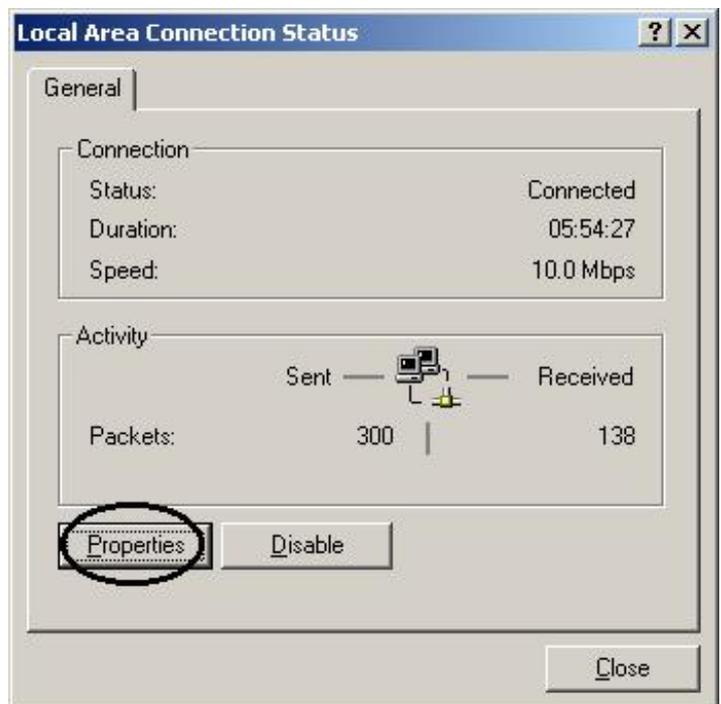


## Configurazione del PC in Windows 2000

1. Andare su **Start/Settings/Control Panel**. Cliccare due volte su **Network and Dial-up Connections**.
2. Cliccare due volte su **Local Area Connection**.

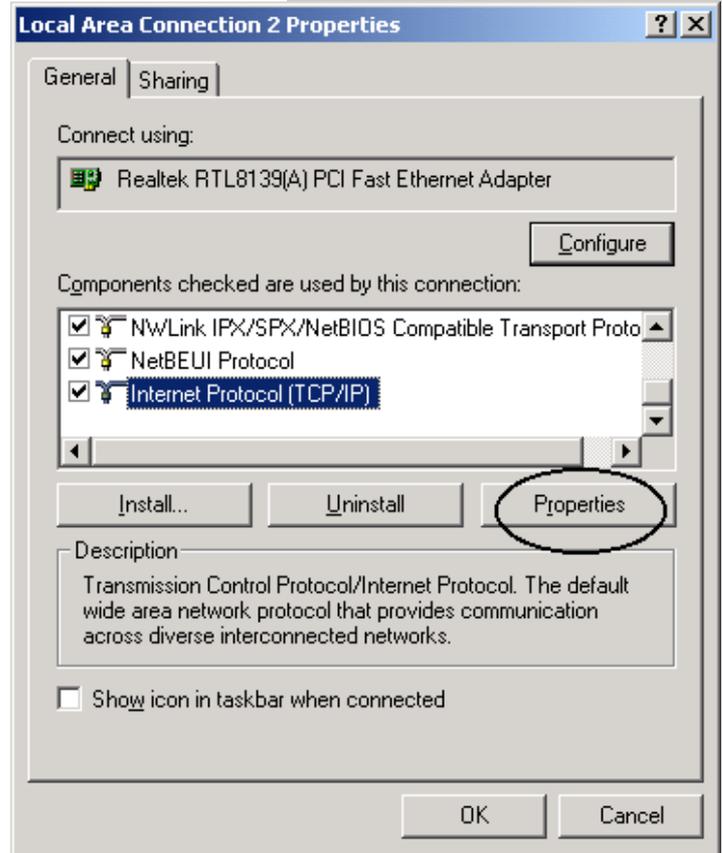


3. In **Local Area Connection Status** cliccare **Properties**.

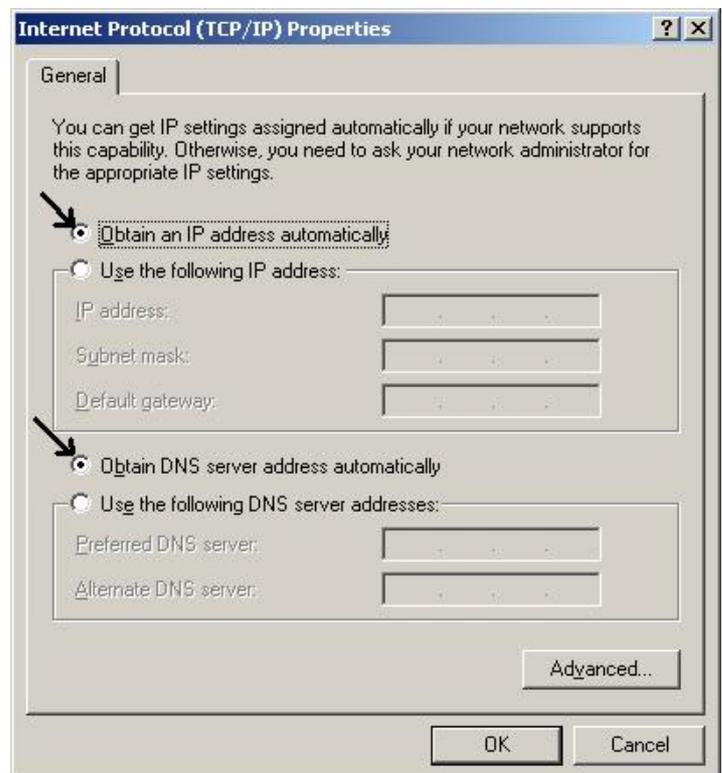




4. Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties**.



5. Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically**
6. Premere su **OK** per terminare la configurazione



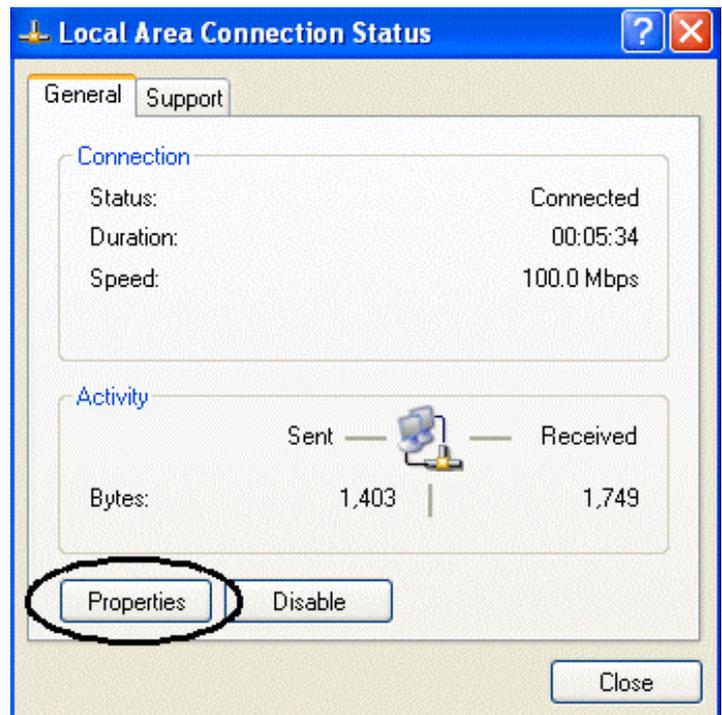


## Configurazione del PC in Windows XP

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**.

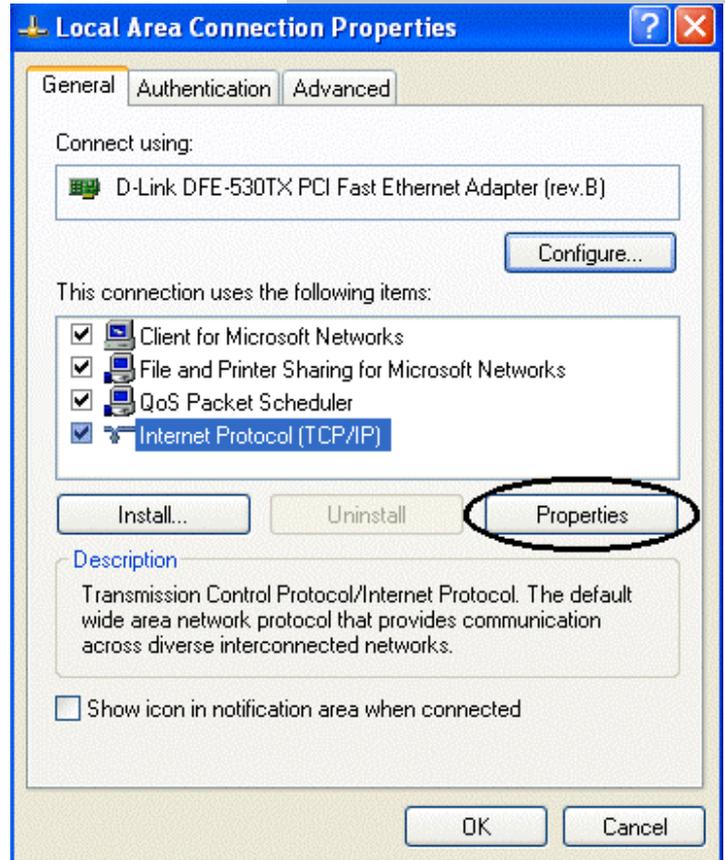


3. In **Local Area Connection Status** cliccare **Properties**.

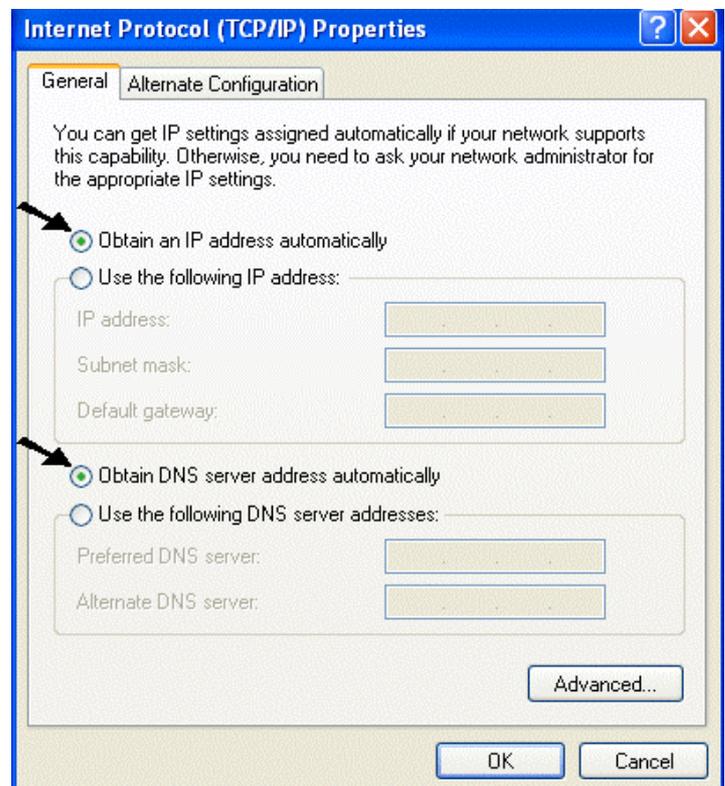




4. Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties**.



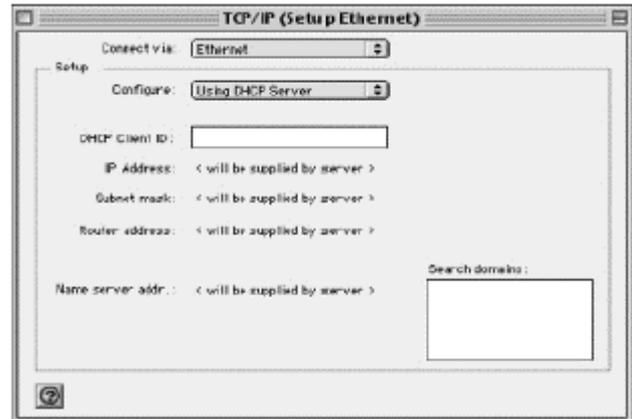
5. Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically**.
6. Premere su **OK** per terminare la configurazione.





## Configurazione in ambiente 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**.





## 3.4 Verifica

Per verificare il successo della configurazione (dopo aver riavviato il PC con Win95,98,98SE,ME, oppure dopo aver ottenuto il rilascio dell'IP su XP, 2000), utilizzare il comando **ping**. Da una finestra Dos digitare: **ping 192.168.1.254**.

Il seguente messaggio indica un corretto funzionamento della parte LAN:

```
Pinging 192.168.1.254 with 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
```

Il seguente messaggio indica un problema di funzionamento:

```
Pinging 192.168.1.254 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.
```

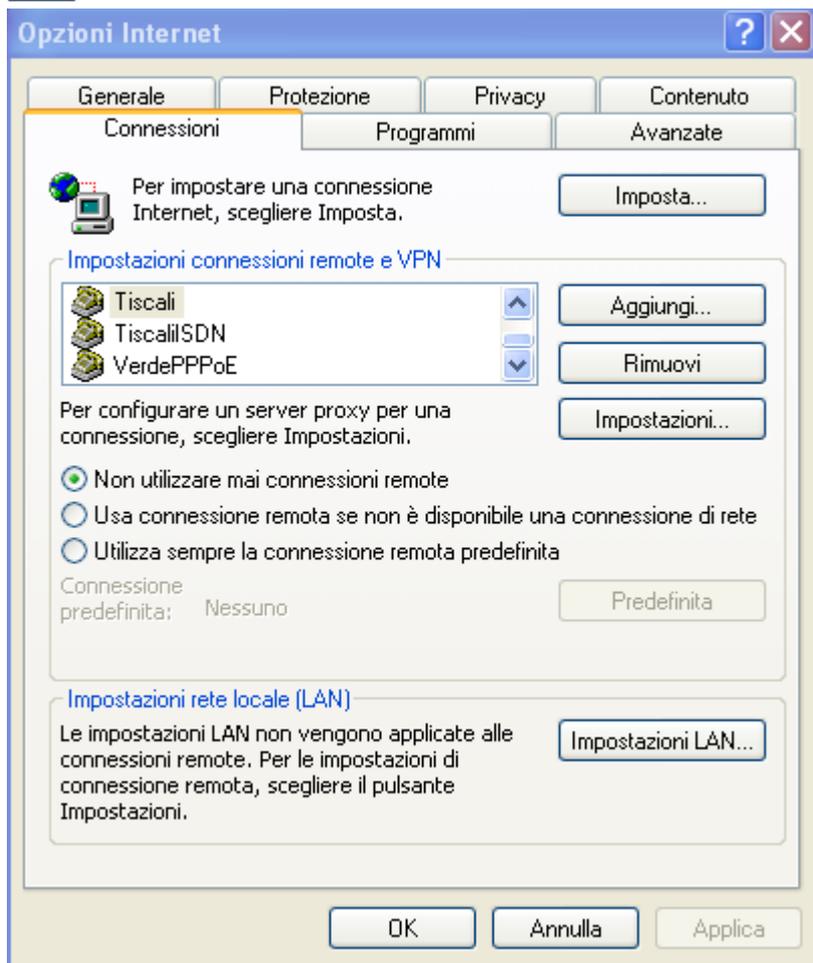
Controllare che il led LAN sia acceso (cambiare il cavo qualora non fosse così). Controllare l'indirizzo del PC digitando **winipcfg** per (Win95,98,98SE,ME) o **ipconfig** (per Win2000,XP) ed eventualmente reinstallare lo stack TCP/IP. Consultare eventualmente le FAQ nella parte finale di questo manuale.

## 3.5 Configurazione del Browser

A questo punto è necessario lanciare IE, andare nel menù **Strumenti**, poi scegliere la sezione **Connessioni** e spuntare le voci:

- Non utilizzare mai connessioni remote
- Usa connessione remota se non è disponibile una connessione di rete

Si osservi la figura sottostante.



## 3.6 Settaggi di Default

Prima di iniziare la configurazione dell'I-Storm ADSL Firewall Router è necessario conoscere quali siano i settaggi di default:

Web Configurator

Username : **admin**

Password: **atlantis**

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**

### 3.6.1 Recupero Password

Quando si configura l'I-Storm Lan Router ADSL con il browser premere su **OK** per entrare (dopo aver introdotto l'username=**admin** e password=**atlantis**) per la prima volta. E' consigliato cambiare la password, al fine di aumentare la sicurezza. L'I-Storm Lan Router ADSL conserva una sola password per volta.



Qualora si perdesse la password premere il tasto Reset (posto nel pannello posteriore) per più 8 secondi. In questo modo il Router caricherà i settaggi di default (Sez 3.6).

### 3.6.2 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	

## 3.7 Informazione sull'ISP

Prima di iniziare la configurazione dell'I-Storm ADSL Firewall Router 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:

<b>PPPoE</b>	<ul style="list-style-type: none"> <li>VPI/VCI, VC-based/LLC-based multiplexing, Username, Password.</li> <li>Opzionali: Service Name e indirizzo IP del Domain Name System (DNS) (può essere assegnato dall'ISP in maniera dinamica, oppure fisso).</li> </ul>
<b>PPPoA</b>	<ul style="list-style-type: none"> <li>VPI/VCI, VC-based/LLC-based multiplexing, Username, Password.</li> <li>Opzionali: indirizzo IP del Domain Name System (DNS) (può essere assegnato dall'ISP in maniera dinamica, oppure fisso).</li> </ul>
<b>RFC1483 Bridged</b>	<ul style="list-style-type: none"> <li>VPI/VCI, VC-based/LLC-based multiplexing e configurare il dispositivo in BRIDGE.</li> <li>Username e Password per la configurazione del Client PPPoE sul PC.</li> </ul>
<b>RFC1483 Routed</b>	<ul style="list-style-type: none"> <li>VPI/VCI, VC-based/LLC-based multiplexing, indirizzo IP, Subnet mask, Gateway address e indirizzi IP dei Domain Name System (DNS, sono IP fissi).</li> </ul>
<b>IPoA</b>	<ul style="list-style-type: none"> <li>VPI/VCI, IP address, Subnet mask, indirizzo del Gateway e indirizzi IP dei Domain Name System (DNS, sono IP fissi).</li> </ul>

## 3.8 Configurazione del Router tramite Browser

Accedere col browser web al seguente indirizzo IP (dove solitamente si inserisce l'URL) che di default è: **192.168.1.254**, e premere poi il tasto invio.





Immettere l'username e la password (utilizzare **admin** per username e **atlantis** come password, nel caso di primo accesso). Qualora la password fosse stata cambiata bisogna invece inserire quella memorizzata nel dispositivo. Premere **OK** per continuare.

Connetti a 192.168.1.254

Nome utente:

Password:

Memorizza password

OK Annulla



Si raccomanda, una volta configurato il Router di salvare sulla eeprom 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 è possibile accedere (come se si stessero vedendo i links in una homepage) a tutte le sezioni:

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

*I-Storm Lan Router ADSL*

Status	<b>Status</b>
Quick Start	<b>Device Information</b>
Configuration	Host Name ▶ home.gateway
Save Config to FLASH	System Up-Time 00:13:42s
Language	Current Time ▶ Thu, 01 Jan 1970 - 02:13:29
	Hardware Version ADSL G3-A v1.00 / Argon III CSP v1.0 (IOS 9.0)
	Software Version 4.52b
	MAC Address 00:04:ED:FF:FF:27
	Home URL Atlantis Land S.p.A.
	<b>LAN</b>
	IP Address ▶ 192.168.1.254
	SubNetmask 255.255.255.0
	DHCP Server ▶ Enable
	<b>WAN</b>
	Primary DNS ▶ None
	<b>Port Status</b>
	Port Ethernet ▶ Adsl ▶
	Connected ✓ ✗
	<b>Statistics</b>
	Ethernet ▶ Rx : 1189/0 Tx : 619/0

Cliccando sulla sezione desiderata appariranno, 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 configurazioni vere e proprie.

### 3.8.1 STATUS

In questa sezione del Router è possibile visualizzare tutti gli stati del dispositivo ed avere così un quadro immediato dello stato di funzionamento. E' altresì possibile utilizzare tale sezione per configurare determinati parametri del dispositivo.

Cliccando sul Menù Status si apriranno tutte le seguenti sottosezioni:

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

Queste sottosezioni mostrano 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 è possibile conoscere l'IP che ha attaccato, 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 è possibile



monitorare lo stato relativo alla VPN. E' importante sottolineare che nessun settaggio potrà essere cambiato.

Cliccando invece su **Status** apparirà la seguente schermata:

<b>Status</b>		
<b>Device Information</b>		
Host Name ▶	home.gateway	
System Up-Time	00:23:39s	
Current Time ▶	Thu, 01 Jan 1970 - 02:23:27	
Hardware Version	ADSL G3-A v1.00 / Argon III CSP v1.0 (ISOS 9.0)	
Software Version	4.52b	
MAC Address	00:04:ED:FF:FF:27	
Home URL	Atlantis Land S.p.A.	
<b>LAN</b>		
IP Address ▶	192.168.1.254	
SubNetmask	255.255.255.0	
DHCP Server ▶	Enable	
<b>WAN</b>		
Primary DNS ▶	None	
<b>Port Status</b>		
Port	Ethernet ▶	Adsl ▶
Connected	✓	✗
<b>Statistics</b>		
Ethernet ▶		Rx : 2114/ 0 Tx : 1065/ 0

Vediamo i parametri su cui possiamo agire:

## Host Name

<b>Host Name</b>	
<b>Device Host Name</b>	
Host Name	<input type="text" value="home.gateway"/>
<input type="button" value="Apply"/>	

E' possibile scegliere il nome con cui accedere al dispositivo.

## Current Time

Per la configurazione dell'orario. Consultare la sezione opportuna per maggiori dettagli.



## IP Address

E' possibile configurare l'indirizzo IP lato LAN del Router (sino a 2) ed i protocolli di RIP e Multicast. Per maggiori dettagli consultare la sezione opportuna.

## DHCP Server

E' possibile selezionare la modalità operativa del DHCP. Il Router può essere infatti server DHCP oppure può effettuare il DHCP relay. E' 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

E' possibile inserire i server DNS. Sono necessariamente 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(ADSL)

E' possibile forzare il tipo di modulazione e vedere la velocità della connessione.

## Statistics

E' possibile avere tutte le statistiche e maggiori dettagli sia sulla WAN che LAN.

## 3.8.2 CONFIGURATION

In questa sezione del Router è possibile effettuare la configurazione di quasi tutti i parametri. Cliccando sul Menù **Configuration** si apriranno tutti i seguenti sottomenù:

- LAN
- WAN
- System
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced

### 3.8.2.1 LAN

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



### 3.8.2.1.1 Ethernet

Ethernet				
<b>Primary IP Address</b>				
IP Address	192	168	1	254
SubNetmask	255	255	255	0
<b>Secondary IP Address</b>				
IP Address	0	0	0	0
SubNetmask	0	0	0	0
RIP	<input type="checkbox"/> RIP v1 <input type="checkbox"/> RIP v2 <input type="checkbox"/> RIP v2 Multicast			
<input type="button" value="Apply"/>				

Questo è l'indirizzo IP con cui l'I-Storm ADSL Firewall Router è visto nella LAN (potrebbe essere un IP pubblico nel caso l'ISP fornisca una classe). E' necessario, qualora si cambiasse IP con quello di un'altra subnet verificare 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 sulla stessa subnet. E' inoltre 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. E' 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 il Nat si isola, di fatto, la 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

**E' 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 non è garantito un corretto funzionamento.**

Vediamo gli scenari più comuni:

- **PC con IP appartenenti ad una classe privata**, il cui default gateway è l'IP del 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 inserito manualmente su informazione dell'ISP). Il management del Router può essere fatto da un qualunque PC collegato ad Internet (abilitando l'apposita funzione sull'I-Storm ADSL Firewall Router) oppure dai PC della Lan. Il collegamento con l'ISP può essere uno qualsiasi tra quelli supportati (il default gateway e l'IP pubblico del Router ADSL verranno forniti automaticamente come gli IP dei 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 l'I-Storm ADSL Firewall Router) di default. E' possibile in questo caso abilitare il DHCP server del Router (per assegnare ulteriori indirizzi IP, magari a PC portatili) ma è necessario prestare attenzione nello scegliere un pool di indirizzi compatibile (in questo caso bisognerà settare come IP starting 192.168.1.n+1, dove  $n+1 < 254$ ).

E' comunque possibile cambiare la rete, avendo l'accortezza di sceglierla tra quelle riservate 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 avrà un IP che può essere pubblico o privato (per il fornitore del servizio è un risparmio di indirizzi IP), l'ISP fornirà comunque l'indirizzo del default gateway dell'I-Storm ADSL Firewall Router 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 o punto-multipunto composta da indirizzi IP che possono essere pubblici o privati.

### 3.8.2.1.2 Port Settings

In questa sezione è possibile forzare il tipo di modalità di funzionamento su ognuna delle 4 porte. E' possibile infatti scegliere (usando il combo box) tra **Auto**, **10Full Duplex**, **10Half Duplex**, **100Full Duplex** e **100Half Duplex**. E' possibile scegliere la modalità di funzionamento per ogni porta, indipendentemente dalle altre.



Port Setting	
Parameters	
Port1 Connection Type	Auto
Port2 Connection Type	Auto
Port3 Connection Type	Auto
Port4 Connection Type	Auto
IPv4 TOS Priority Control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Set High Priority TOS	<input type="checkbox"/> 7 <input type="checkbox"/> 6 <input type="checkbox"/> 5 <input type="checkbox"/> 4 <input type="checkbox"/> 3 <input type="checkbox"/> 2 <input type="checkbox"/> 1 <input type="checkbox"/> 0

Apply

E' 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 è possibile dare priorità maggiore ad opportuni servizi ed evitare fastidiosi rallentamenti. Questo renderà più fruibili particolari servizi. Si ricorda però che i Gateway in Internet ignorano (generalmente) il campo TOS.

### 3.8.2.1.3 DHCP Server

Sono disponibili 3 differenti opzioni:

- **Disable**
- **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 è necessario 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 dell'I-Storm ADSL Firewall Router).
- **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:** Introdurre gli indirizzi IP dei server DNS, questi saranno passati ai vari client.
  - Use Router as Default Gateway:** Se selezionato l'indirizzo IP del Router verrà dato, ai client DHCP, come default Gateway



Qualora fosse già presenti nella LAN un server DHCP è opportuno disabilitare tale funzionalità nel Router ADSL (o nel PC che opera da server DHCP) per evitare possibili conflitti. Un'attenta configurazione dei 2 server può permettere comunque il loro utilizzo simultaneo.

E' inoltre disponibile la funzionalità Fixed Host:

Fixed Host	
<b>Create</b>	
Name	<input type="text"/>
IP Address	<input type="text"/>
MAC Address	<input type="text" value="00:00:00:00:00:00"/>
Maximum Lease Time	<input type="text"/>
<input type="button" value="Apply"/>	

E' possibile infatti selezionare un PC come client DHCP ma fare in modo che il server DHCP gli assegni permanentemente 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 l'I-Storm ADSL Firewall Router 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 necessita 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.

DHCP	
<b>DHCP Relay Agent</b>	
DHCP Server IP Address	<input type="text"/>
<input type="button" value="Apply"/>	

### 3.8.2.2 WAN

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

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

Vediamo nel dettaglio come configurare la sezione WAN:

#### 3.8.2.2.1 ISP

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



- **VPI/VCI:** Consultare l'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 in Italia: **VPI =8** e **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 del PC della Lan, che è un IP privato non valido in Internet) con l'IP pubblico dell'I-Storm ADSL Firewall 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 spedisce al PC interessato nella Lan.
- **Encapsulation Method:** Assicurarsi di usare lo stesso metodo di incapsulamento richiesto dall'ISP (LLC/SNAP or VC MUX).



Disabilitando la funzionalità NAT il Virtual Server e la sezione VPN verranno automaticamente disabilitate.

Passiamo adesso alla configurazione vera e propria dell'interfaccia WAN (**E' necessario conoscere i parametri dell'ISP per la connessione ADSL**). Individuato il tipo di protocollo seguire la sezione opportuna.

Evidenziare la sezione **Configuration**, poi **WAN** e poi **ISP**. Apparirà la seguente immagine:

ISP		
Please select the type of service you wish to create		
ATM	<input checked="" type="radio"/> RFC 1483 Routed	<input type="radio"/> RFC 1483 Bridged
	<input type="radio"/> PPPoA Routed	<input type="radio"/> IPoA Routed
	<input type="radio"/> PPPoE Routed	<b>Quick Start</b> ▶
<input type="button" value="Next"/>		

- **QUICK START**

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



### Quick Start

**Connection**

Encapsulation	PPPoA	<input type="button" value="Auto Scan"/>
VPI	8	
VCI	35	
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	

**Optional Settings**

IP Address	<input type="text"/>	(0.0.0.0 means 'Obtain an IP address automatically')
SubNetmask	<input type="text"/>	
Default Gateway	<input type="text"/>	

**DNS**

Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>

**PPP**

Username	<input type="text"/>
Password	<input type="text"/>

Cliccare su **Auto Scan** (e poi su **Start**) per ottenere le informazioni sul tipo di protocollo ed i valori di VCI/VPI. Questa rilevazione è da usarsi coi soli protocolli PPPoA/PPPoE. Dopo aver premuto il tasto **START** verranno mostrati parametri caratteristici della linea ADSL.

1 found PPPoA PVC on 8/35

### Auto Scan

A questo punto evidenziare (qualora siano state rilevate più configurazioni possibili) la configurazione e premere su **Apply**. Inserire poi 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'abbonamento 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.

WAN Connection	
RFC 1483 Bridged	
Description	RFC 1483 bridged mode
VPI	8
VCI	35
ATM Class	UBR
Encapsulation Method	LLC Bridged
Ether Filter Type	All
Spanning Bridge Interface	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/>	

E' sufficiente inserire il valore dei parametri **VCI** e **VPI** ed il tipo di incapsulamento (da scegliere tra **LLC** e **VCMux**) per terminare la configurazione del router.

In **ATM Class** è possibile scegliere la classe di servizio per il layer ATM.

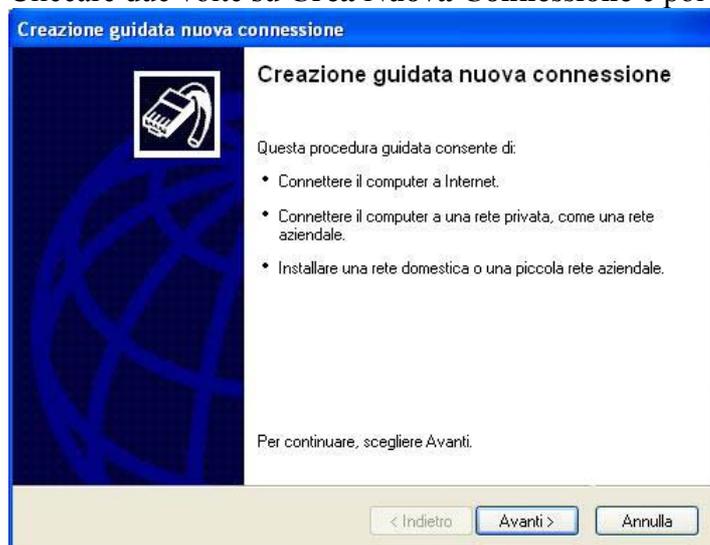
**Ether Filter Type:** Specificare il tipo di filtro da operare sul traffico che attraversa l'interfaccia in modalità bridge (scegliere il tipo di traffico tra: **IP**, **All** e **PPPoE**)

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, valida su Windows XP, è sufficiente seguire i seguenti passaggi:

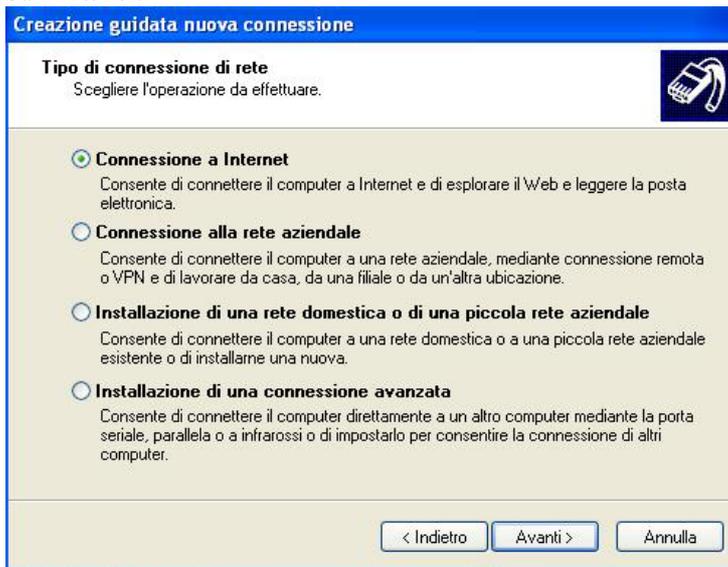
Dal **Pannello di Controllo** cliccare due volte sull'icona **Connessioni di Rete**.

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

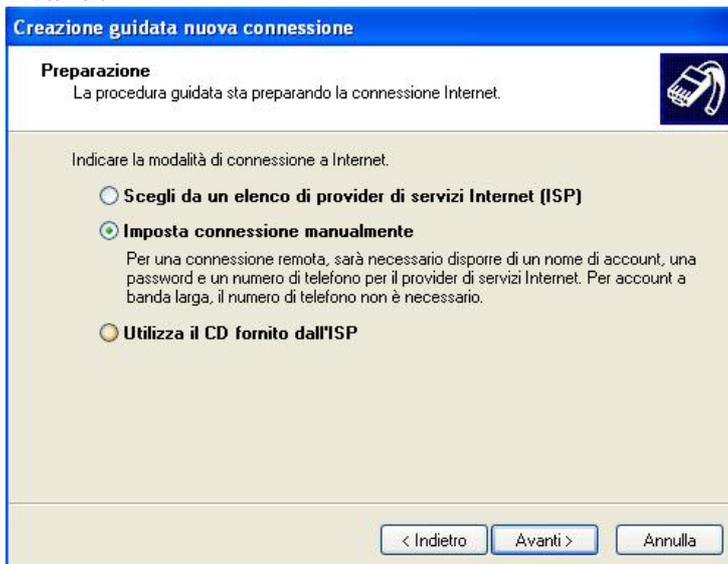




Partirà il Wizard di Windows XP, selezionare la voce: **Connessione ad Internet** e poi cliccare su **Avanti**.



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



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



**Creazione guidata nuova connessione**

**Connessione Internet**  
Indicare la modalità di connessione a Internet.

**Connessione tramite modem remoto**  
Connessione mediante modem e normale linea telefonica o ISDN.

**Connessione a banda larga con immissione di nome utente e password**  
Connessione a velocità elevata mediante modem via cavo o linea DSL. Questo tipo di connessione può anche essere definita PPoE (Point-to-Point Protocol over Ethernet).

**Connessione a banda larga sempre attiva**  
Connessione a velocità elevata mediante modem via cavo o connessione DSL o LAN. È sempre attiva e non richiede l'immissione di nome utente e password.

< Indietro   Avanti >   Annulla

Inserire il nome dell'ISP e poi cliccare su **Avanti**.

**Creazione guidata nuova connessione**

**Nome connessione**  
Specificare il nome del servizio che fornisce la connessione Internet.

Immettere il nome dell'ISP nello spazio sottostante.

Nome ISP

A02-RA3

Il nome immesso sarà il nome della connessione che si sta creando.

< Indietro   Avanti >   Annulla

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

**Creazione guidata nuova connessione**

**Informazioni sull'account Internet**  
È necessario disporre di un nome account e di una password per accedere all'account Internet.

Immettere un nome di account ISP e la relativa password, quindi prendere nota di tali informazioni e conservarle in un luogo sicuro. Se il nome di account o la password esistenti sono state dimenticate, contattare l'ISP.

Nome utente:

Password:

Conferma password:

Utilizza questo nome di account e password per la connessione a internet di tutti gli utenti

Imposta questa connessione Internet come predefinita

Abilita il firewall della connessione Internet per questa connessione

< Indietro   Avanti >   Annulla



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



**Mac OS X** al pari di Windows XP incorpora già il client PPPoE. Si rimanda al Capitolo 4 per dettagli sulla configurazione. Per sistemi con Mac OS 9 è invece necessario utilizzare un client PPPoE di terze parti, si rimanda sempre al Capitolo 4 per ulteriori informazioni.



Windows 95, 98, ME, 2000 ed NT4.0 contrariamente a Windows XP non incorporano il client PPPoE. Si rimanda al Capitolo 4 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 e condividere lo stesso account Internet tra diversi PC.

WAN Connection	
<b>PPPoA Routed</b>	
Description	PPPoA Routed
VPI	8
VCI	35
ATM Class	UBR <input type="button" value="v"/>
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/>
IP Address	<input type="text"/> (0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Chap(Auto) <input type="button" value="v"/>
Connection	Always On <input type="button" value="v"/>
Idle Timeout	0 minutes
RIP	<input type="checkbox"/> RIP v1 <input type="checkbox"/> RIP v2 <input type="checkbox"/> RIP v2 Multicast
MTU	1500
<input type="button" value="Apply"/>	

Vediamo i parametri da configurare:

1. **VPI=8**
2. **VCI=35**
3. **ATM Class**= è possibile scegliere la classe di servizio per il layer ATM.
4. **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.



5. **Username:** Introdurre l'username fornita dal vostro ISP. Tale username può essere composta da massimo 128 caratteri (case sensitive) alfanumerici.
6. **Password:** Introdurre la password fornita dal vostro ISP. Tale password può essere composta da massimo 128 caratteri (case sensitive) alfanumerici.
7. **IP address:** lasciare tale parametro con il valore 0.0.0.0
8. **Authentication Protocol:** Di default è: **Chap(Auto)**. Le altre opzioni possibili sono **CHAP** e **PAP**, in caso di dubbio lasciare il valore di default.
9. **PPPoA Connection:** Scegliere **Always On** se si desidera stabilire una sessione PPPoA nel momento dello starting up. Inoltre viene automaticamente ristabilita la connessione PPPoA qualora il dispositivo venga disconnesso dall'ISP (o per ragioni tecniche la connessione cada). Scegliere **Connect on Demand** se si vuole stabilire una connessione PPPoA solo quando ci sono pacchetti (**non necessariamente generati da IE**) diretti verso Internet.
10. **Idle-Timeout (in minutes):** Disconnette automaticamente l' I-Storm Router ADSL quando non è rilevata alcuna attività di pacchetti verso Internet per un tempo predeterminato. Il valore settato a 0 non fa attivare questa funzionalità.

Scegliere se utilizzare il protocollo RIP ed eventualmente quale versione utilizzare. Impostare infine il valore di MTU (Maximum Transmission Unit) non superando il valore di 1500.

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/MAIL** prima lampeggerà e poi diventerà fisso (il Led **ADSL** dovrebbe essere fisso per indicare l'avvenuto allineamento).

- **PPPoE 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 e condividere lo stesso account Internet tra diversi PC.



WAN Connection	
<b>PPPoE Routed</b>	
Description	PPPoE Routed
VPI	8
VCI	35
ATM Class	UBR
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	
Password	
Service Name	
IP Address	<input type="text"/> (0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Chap(Auto)
Connection	Always On
Idle Timeout	<input type="text"/> minutes
RIP	<input type="checkbox"/> RIP v1 <input type="checkbox"/> RIP v2 <input type="checkbox"/> RIP v2 Multicast
MTU	1492
<input type="button" value="Apply"/>	

Vediamo i parametri da configurare:

1. **VPI=8**
2. **VCI=35**
3. **ATM Class**= è possibile scegliere la classe di servizio per il layer ATM.
4. **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.
5. **Username**: Introdurre l'username fornita dal vostro ISP. Tale username può essere composta da massimo 128 caratteri (case sensitive) alfanumerici.
6. **Password**: Introdurre la password fornita dal vostro ISP. Tale password può essere composta da massimo 128 caratteri (case sensitive) alfanumerici.
7. **Service Name**: Alcuni ISP forniscono tale parametro. In caso di dubbio lasciate il campo vuoto.
8. **IP address**: lasciare tale parametro con il valore 0.0.0.0
9. **Authentication Protocol**: Di default è: **Chap(Auto)**. Le altre opzioni possibili sono **CHAP** e **PAP**, in caso di dubbio lasciare il valore di default.
10. **PPPoE Connection**: Scegliere **Always On** se si desidera stabilire una sessione PPPoE nel momento dello starting up. Inoltre viene automaticamente ristabilita la connessione PPPoE qualora il dispositivo venga disconnesso dall'ISP (o per ragioni tecniche la connessione cada). Scegliere **Connect on Demand** per stabilire una connessione PPPoE solo quando ci sono pacchetti diretti verso Internet.



11. **User Idle-Timeout (in minutes)**: Disconnette automaticamente l' I-Storm Router ADSL quando non è rilevata alcuna attività di pacchetti verso Internet per un tempo predeterminato. Il valore settato a 0 non fa attivare questa funzionalità.

Scegliere se utilizzare il protocollo RIP ed eventualmente quale versione utilizzare. Impostare infine il valore di MTU (Maximum Transmission Unit) non superando il valore di 1492.

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/MAIL** prima lampeggerà e poi diventerà fisso (il Led **ADSL** dovrebbe essere fisso per indicare l'avvenuto allineamento).

- **RFC1483 Routed/ IpoA Routed (RFC1577)**

Le modalità in cui l'ISP può fornire RFC1483/1577 possono essere le seguenti:

1. **Un indirizzo IP pubblico statico**. In questo caso è necessario configurare la sezione **WAN-ISP** nella seguente modalità: **NAT=abilitato, IP address=IP statico pubblico, Subnet mask e Default Gateway** (che sarà un IP pubblico). Tutti questi valori sono contenuti nel contratto dell'ISP. Il LAN-IP è invece in una classe privata e sarà il default gateway di tutti i PC.
2. **Una classe di IP statici con Punto-(multi)Punto pubblica**. In questo caso è necessario configurare la sezione **WAN-ISP** nella seguente modalità: **Nat=disabilitato, IP address=IP statico pubblico** (quello della punto-punto) **Subnet mask e Default Gateway** (che sarà un IP pubblico). Tutti questi valori sono contenuti nel contratto dell'ISP. Il Lan IP invece è sempre un IP statico pubblico e fa parte della classe assegnata con la rispettiva subnet mask. Gli altri IP di questa classe (e la subnet mask) dovranno essere assegnati ai PC assieme al default gateway che sarà il LAN-IP (ed i DNS).
3. **Una classe di IP statici con Punto-(multi)Punto privata**. In questo caso è necessario configurare la sezione **WAN-ISP** nella seguente modalità: **Nat=disabilitato, IP address=IP privato** (quello della punto-punto) **Subnet mask e Default Gateway** (che sarà un IP privato). Tutti questi valori sono contenuti nel contratto dell'ISP. Il Lan IP invece è sempre un IP statico pubblico e fa parte della classe assegnata con la rispettiva subnet mask. Gli altri IP di questa classe (e la subnet mask) dovranno essere assegnati ai PC assieme al default gateway che sarà il LAN-IP (ed i DNS).

Vediamo i parametri da configurare:



WAN Connection		
RFC 1483 Routed		
Description	RFC 1483 routed mode	
VPI	8	
VCI	35	
ATM Class	UBR	
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Encapsulation Method	LLC Routed	
IP Assignment	<input checked="" type="radio"/> Obtain an IP address automatically via DHCP client	
	<input type="radio"/> Use the following IP address	
	IP Address	
	Netmask	
	Gateway	
RIP	<input type="checkbox"/> RIP v1 <input type="checkbox"/> RIP v2 <input type="checkbox"/> RIP v2 Multicast	
MTU	1500	
<input type="button" value="Apply"/>		

Vediamo i parametri da configurare:

1. **VPI=8**
2. **VCI=35**
3. **ATM Class**= è possibile scegliere la classe di servizio per il layer ATM.
4. **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 RFC1483): Scegliere il metodo di incapsulazione utilizzato dall'ISP. Sono disponibili: **LLC Bridged**, **VCMux Bridged**, **VCMux Routed**, **LLC Routed** ed **LLC MER**. In genere il tipo di incapsulamento è **LLC Routed**.



Non resta che selezionare la voce **Use the following IP address** ed introdurre:

1. **IP Address**: Introdurre l'IP pubblico.
2. **Netmask**: Introdurre la Netmask fornita dall'ISP.
3. **Gateway**: Introdurre il Default Gateway del Router.

Se questi dati sono forniti dal server dall'ISP in maniera automatica, spuntare la voce **Obtain an IP address automatically via DHCP client**.

Scegliere se utilizzare il protocollo RIP ed eventualmente quale versione utilizzare. Impostare infine il valore di MTU (Maximum Transmission Unit) non superando il valore di 1500.



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/MAIL** resterà spento.

### 3.8.2.2.2 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](http://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 del 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.

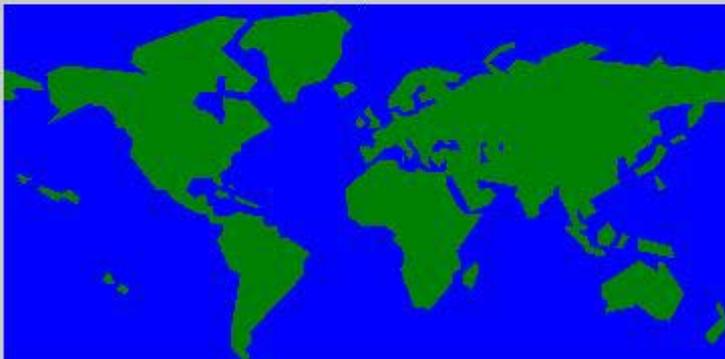
### 3.8.2.3 SYSTEM

Cliccando sul menù **Configuration** e poi **System** si apriranno tutti i seguenti sottomenù:

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

#### 3.8.2.3.1 Time Zone

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

Time Zone	
<b>Parameters</b>	
Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time Zone List	<input checked="" type="radio"/> By City <input type="radio"/> By Time Difference
Local Time Zone (+GMT Time)	(GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna <span>▼</span>
SNTP Server IP Address	140.162.8.3      192.43.244.18
	128.138.140.44      129.6.15.29
Daylight Saving	<input checked="" type="checkbox"/> Automatic
Resync Period	1 minutes <input type="button" value="Sync Now"/>
v	
	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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



### 3.8.2.3.2 Remote Access

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

Remote Access	
You may temporarily permit remote administration of this network device	
Allow Access for	<input type="text" value="30"/> minutes.
<input type="button" value="Enable"/>	

Mettere **0** per consentire una configurazione permanente.

Al riavvio dell'apparato questo rimarrà comunque non configurabile da remoto.



Per rendere permanente la configurazione remota creare una rotazione nel Virtual Server ruotando la porta su cui si effettua l'accesso WEB sull'IP lato LAN del dispositivo.

E' necessario accedere alla sezione **Configuration** poi **Advanced** ed infine **Device management**. Scegliere la porta su cui il Router può essere controllato.

Device Management		
Embedded Web Server		
* HTTP Port	<input type="text" value="8081"/>	(80 is default HTTP port)
Management IP Address	<input type="text" value="0.0.0.0"/>	(0.0.0.0 means Any)
Expire to auto-logout	<input type="text" value="180"/>	seconds

Nella foto si è spostato la porta di gestione http sulla 8081 (per permettere così di offrire un servizio http pubblico). A questo punto nella sezione **Virtual Server** effettuare una rotazione di tale porta sull'IP LAN del Router (in figura sotto si è assunto l'IP LAN del Router sull'IP di default 192.168.1.254).

<input checked="" type="checkbox"/>	HTTPremoto	tcp	<input type="text" value="8081"/> ~ <input type="text" value="8081"/>	<input type="text" value="8081"/> ~ <input type="text" value="8081"/>	<input type="text" value="192.168.1.254"/>
-------------------------------------	------------	-----	---	---	--

A questo punto salvare i settaggi ed effettuare un riavvio del dispositivo (**System** poi **Restart** e scegliere **current settings** e poi premere sul tasto restart).

Da remoto digitare a questo punto <http://IPWAN ROUTER:8081> per avere accesso alla configurazione remota del dispositivo.



Nel caso in cui l'abbonamento con ADSL sia con IP dinamico, l'accesso da remoto può comunque sempre essere effettuato. Utilizzare il client **Dynamic DNS** integrato nel dispositivo. Per maggiori dettagli consultare l'Appendice A. In questo modo non è necessario conoscere l'indirizzo IP del Router ma solo il nome registrato.

### 3.8.2.3.3 Firmware Upgrade

Firmware Upgrade	
You may upgrade the system software on your network device	
New Firmware Image	<input type="text"/> <input type="button" value="Sfoglia..."/>
<input type="button" value="Upgrade"/>	

Per effettuare l'upgrade del firmware del Router ADSL è necessario anzitutto scaricare dal sito [www.atlantisland.it](http://www.atlantisland.it) o [www.atlantis-land.com](http://www.atlantis-land.com) (nella sezione opportuna) un nuovo firmware (se disponibile). Aprire il file compresso in una directory. Accedere a questo punto, sotto il menù



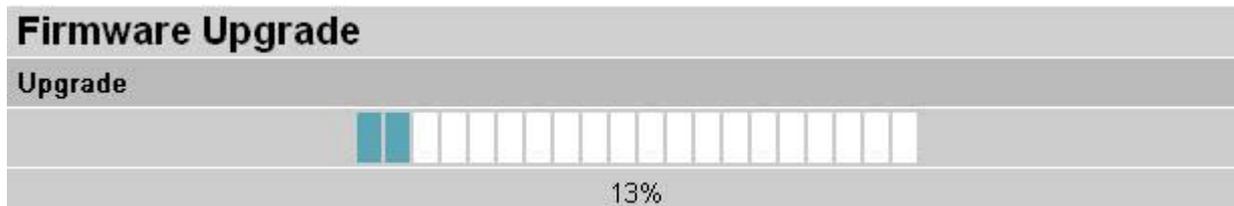
**Configuration** e poi **System**, alla voce **Firmware Upgrade** e premere poi il tasto **Sfoglia** ed indicare la path contenente il firmware decompresso. Premere poi sul tasto **Upgrade** per terminare l'aggiornamento. **E' opportuno staccare, durante la fase di upgrade, la linea ADSL dal dispositivo.**



**E' opportuno garantire, durante l'intera fase di upgrade, al Router ADSL l'alimentazione elettrica. Qualora questa venisse a mancare il dispositivo potrebbe non essere recuperabile.**

**Questo potrebbe danneggiare il dispositivo ed invalidare così la garanzia.**

Durante la fase di upgrade il Router indicherà lo stato di completamento della riscrittura del firmware mostrando un indicatore percentuale.



Completata la procedura apparirà la seguente schermata:

Firmware Upgrade	
Your FLASH chips have been updated	
Firmware Update Complete. Please restart to take effect.	
Restart Router with	<input checked="" type="radio"/> Current Settings
	<input type="radio"/> Factory Default Settings
<input type="button" value="Restart"/>	

in cui è possibile scegliere se mantenere gli attuali settaggi (**Current Settings**) o ripristinare il dispositivo alle condizioni iniziali (**Factory Default Settings**).

#### 3.8.2.3.4 Backup / Restore

L'I-Storm ADSL Firewall Router consente di effettuare un backup (ripristino) sul (dal) disco fisso del vostro PC. Grazie a questa comoda funzionalità è possibile salvare complesse configurazioni e rendere nuovamente operativo il Router in pochi veloci passaggi.



## Backup/Restore

Allows you to backup the configuration settings to your computer, or restore configuration from your computer.

### Backup Configuration

Backup configuration to your computer.

Backup

### Restore Configuration

Configuration File

Sfoggia...

"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.

Restore

Per effettuare il Backup cliccare sul bottone **Backup**. Non 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 **Sfoggia**, indicando il percorso dove è contenuto il file contenente la configurazione, e cliccare poi su **Restore**.

### 3.8.2.3.5 Restart Router

## Restart Router

After restarting. Please wait for several seconds to let the system

Restart Router with

Current Settings

Factory Default Settings

Restart

Se per necessità si desidera reimpostare il router ADSL con la configurazione di default (perdendo tutti i settaggi inseriti) è sufficiente accedere, sotto il menù **Configuration-System** alla voce **Restart Router** e spuntare la voce **Factory default settings**. Premere poi il tasto **Restart Router**. Il Router effettuerà un reboot e caricherà i settaggi di default (per ulteriori dettagli consultare la sezione 3.6). Premendo invece il solo tasto **Restart** il router effettuerà un reboot caricando la configurazione attuale. Dopo ogni cambiamento di configurazione cliccare sul bottone **Save config to Flash** per rendere permanenti (e dunque salvare su eeprom) le modifiche.

### 3.8.2.3.6 User Management

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



## User Management

### Current Defined Users

Valid	User	Comment		
true	admin	Default admin user	Edit	

Create

E' 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 è possibile immettere **Username** e **Password** e tramite il campo **Valid** rendere attivo o meno il nuovo utente.

## User Management

### Create

Username	<input type="text"/>
Password	<input type="password"/>
Valid	false
Comment	<input type="text"/>

Create

Reset

Se si perdesse la password di accesso è possibile riportare il Router alle condizioni iniziali eseguendo la procedura sotto riportata (creare un nuovo utente, provare la password e solo adesso cancellare il vecchio utente):

Dopo che il dispositivo è acceso, premere delicatamente l'apposito forellino (nel pannello posteriore), utilizzando un cacciavite, per effettuare il reset o il restore. Le operazioni sono le seguenti:

- **0-3 secondi:** per resettare il dispositivo
- **3-6 secondi:** nessuna azione
- **6 secondi o più:** effettua un ritorno alle condizioni di default



### 3.8.2.4 Firewall

Il Router ADSL include un firewall avanzato comprendente la funzionalità SPI (Stateful Packet Inspection) che consente una prima valida difesa nei confronti di attacchi provenienti da qualche malintenzionato di cui Internet è piena.

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, è consigliabile non considerare mai come inattaccabile la rete LAN. 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.

Il firewall del Router è 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. E’ molto più difficile pertanto per un hacker accedere alla singola macchina.
  - **General Settings/Packet Filter:** e’ 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:** e’ 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

E’ consigliabile visitare periodicamente il sito di AtlantisLand ([www.atlantis-land.com](http://www.atlantis-land.com)) al fine di reperire aggiornamenti di Firmware che potrebbe migliorare le caratteristiche del firewall.

#### 3.8.2.4.1 General Settings/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. E’ 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 un'ottima conoscenza di Internet in quanto è necessario creare una regola per ogni "servizio" da usare. E' certamente più sicura ma richiede una maggiore conoscenza delle problematiche ed una più lunga preparazione delle regole dei filtri (che possono essere moltissimi). Questo è l'approccio utilizzato dal modulo firewall presente nell'apparato.

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.

General Settings	
Firewall Security	
Security	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Policy	<input type="radio"/> All blocked/User-defined
	<input type="radio"/> High security level
	<input checked="" type="radio"/> Medium security level
	<input type="radio"/> Low security level
<i>(! If some applications cannot work after enabling Firewall, please check the Packet Filter especially Port Filter rules. For example, adding (TCP:443,outbound allowed) will let HTTPS data go through Firewall.)</i>	
Block WAN Request	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/>	

Anzitutto è necessario abilitare il Firewall spuntando Enable.

E' 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**. E' consigliato davvero a chi ritiene di possedere una buona conoscenza di Internet.
- **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 la voce Enable in **Block WAN Request**, il router non risponderà alle richieste di Ping sull'interfaccia WAN.



Scegliendo l'opzione **All blocked/User-defined** è necessario aggiungere nel Firewall una regola per ogni servizio. Ogni pacchetto infatti viene bloccato.



Vediamo nel dettaglio le impostazioni preconfigurate.

Come già detto scegliendo il livello di sicurezza tra **High/Medium e Low**, il router applicherà le seguenti matrice di regole.

Application	Protocol	Port Number		Firewall (High)		Firewall(Medium)		Firewall (Low)	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
<b>HTTP(80)</b>	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
<b>DNS (53)</b>	UDP(17)	53	53	NO	YES	NO	YES	YES	YES
<b>DNS (53)</b>	TCP(6)	53	53	NO	YES	NO	YES	YES	YES
<b>FTP(21)</b>	TCP(6)	21	21	NO	NO	NO	YES	NO	YES
<b>Telnet(23)</b>	TCP(6)	23	23	NO	NO	NO	YES	NO	YES
<b>SMTP(25)</b>	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
<b>POP3(110)</b>	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
<b>NEWS(119)</b>	TCP(6)	119	119	NO	NO	NO	YES	NO	YES
<b>RealAudio (7070)</b>	UDP(17)	7070	7070	NO	NO	YES	YES	YES	YES
<b>ICMP</b>	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
<b>H.323(1720)</b>	TCP(6)	1720	1720	NO	NO	NO	YES	YES	YES
<b>T.120(1503)</b>	TCP(6)	1503	1503	NO	NO	NO	YES	YES	YES
<b>SSH(22)</b>	TCP(6)	22	22	NO	NO	NO	YES	YES	YES
<b>NTP(123)</b>	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
<b>HTTPS(443)</b>	TCP(6)	443	443	N/A	N/A	NO	YES	NO	YES
<b>ICQ(5190)</b>	TCP(6)	5190	5190	N/A	N/A	N/A	N/A	YES	YES
<b>PPTP</b>	TCP(1723)	1723	1723	N/A	N/A	YES	NO	N/A	N/A

Si ricorda che tutto il traffico non contemplato nel set di regole viene scartato. E' 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 consentirà lo scaricamento via FTP di file dalla rete. Per modificare questa situazione è sufficiente accedere alla sezione **Configuration, Firewall, Packet Filter**. Apparirà l'immagine sottostante.

**Packet Filter**

**Firewall Security**

Type	Configuration	Note
external < > internal	<a href="#">Port Filters</a> <span style="margin-left: 20px;"><a href="#">Address Filters</a> </span>	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.

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 (scaricamento da un sito FTP esterno) ed ingresso (server FTP su un PC della LAN) possibile.

In figura è possibile osservare adesso il nuovo insieme di regole.



Filtering Table						
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 ▶

Cliccare su **Edit** della regola da modificare (nel nostro caso FTP[TCP,21]). Apparirà la schermata sotto riportata.

### Port Filters

**Edit**

Transport	Type	TCP
Port Range	Start Port	21
	End Port	21
Direction	Inbound	Block ▼
	Outbound	Block ▼
		Allow
		Block

Apply Return ▶

A questo punto modificare il campo **OutBound** su **Allow** (è possibile scaricare) ed il campo **Inbound** su **Allow** (è possibile offrire un servizio FTP, cioè dall'esterno possono accedere al server FTP). In questo modo il traffico uscente/entrante FTP è permesso.



Per offrire un servizio FTP è necessario accedere alla sezione Virtual Server ed effettuare un redirect delle porte 20-21 in TCP verso un indirizzo IP di un PC della LAN su cui gira un server FTP. Per ulteriori dettagli consultare la sezione Virtual Server.

In figura si è assunto un PC con IP 192.168.1.102 su cui gira un servizio FTP.

<input checked="" type="checkbox"/>	ServerFTP	tcp ▼	20 ~ 21	20 ~ 21	192.168.1.102
-------------------------------------	-----------	-------	---------	---------	---------------

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) :



## Port Filters

### Filtering Rules

[Add TCP/UDP Filter](#)[Add Raw IP Filter](#)[Return](#)

Scegliendo **Add TCP/UDP Filter** è possibile aggiungere regole che utilizzino il protocollo TCP/UDP. Scegliendo **Add RAW IP Filter** è possibile filtrare ogni protocollo contenuto nell'IP (ICMP, GRE etc.). 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). E' 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). E' 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** è necessario creare un set di regole ex novo, infatti con questa selezione tutto il traffico, tanto entrante che uscente, viene scartato.

### 3.8.2.4.2 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 LAN 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).



Questo modulo del Firewall è attivabile solo se in **General Settings** è stato impostato uno dei 4 livelli di sicurezza previsti.

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 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.

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

- **Enable**: selezionare True per rendere attiva l'Intrusion Detection.
- **Victim Protection Block Duration**: tipico esempio è un attacco di tipo **Smurf**. Introdurre un valore in secondi.
- **Scan Attack Block Duration**: una volta determinato un attacco di tipo Scan, il router blocca il traffico dall'host esterno (il cui IP è stato inserito nella blacklist) per un intervallo di tempo stabilito. Tipici attacchi Scan sono **X'mas scan**, **IMAP Syn/Fin scan**.
- **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 è stato inserito nella blacklist) per un intervallo di tempo stabilito. Tipici attacchi DoS sono **WinNuke** ed **Ascend Kill**.
- **Maximum TCP Open Handshaking Count**: stabilisce il massimo numero di 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 (sono esclusi Echo Request) il router considera questo come un attacco **ICMP Flood**.

Intrusion Detection	
Parameters	
Intrusion Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Victim Protection Block Duration	<input type="text" value="600"/> seconds
Scan Attack Block Duration	<input type="text" value="86400"/> seconds
DOS Attack Block Duration	<input type="text" value="1800"/> seconds
Maximum TCP Open Handshaking Count	<input type="text" value="100"/> per second
Maximum Ping Count	<input type="text" value="15"/> per second
Maximum ICMP Count	<input type="text" value="100"/> per second

Riguardo ad attacchi di tipo SYN Flood, ICMP Echo Storm e ICMP flood, il modulo IDS si limiterà ad inserire nell'Event Log la segnalazione opportuna. Non viene attuata alcuna protezione contro tali attacchi.



Attack	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
<b>Ascend Kill</b>	Ascend Kill	Src IP	DoS	Yes	Yes
<b>Win Nuke</b>	TCP, Port=135, 137-139 Flag:URG	Src IP	DoS	Yes	Yes
<b>Smurf</b>	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
<b>Land Attack</b>	SrcIP = DstIP			Yes	Yes
<b>Echo/CharGen Scan</b>	UDP Echo Port and CharGen Port			Yes	Yes
<b>Echo Scan</b>	UDP Dst Port =Echo(7)	Src IP	Scan	Yes	Yes
<b>CharGen Scan</b>	UDP Dst Port =CharGen(19)	Src IP	Scan	Yes	Yes
<b>X'Mas Tree Scan</b>	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
<b>IMAP SYN/FIN Scan</b>	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
<b>SYN/FIN/RST/ACK Scan</b>	TCP, No Existing session And Scan Hosts more than five	Src IP	Scan	Yes	Yes
<b>Net Bus Scan</b>	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	Src IP	Scan	Yes	Yes
<b>Back Orifice Scan</b>	UDP, DstPort=Orifice Port (31337)	Src IP	Scan	Yes	Yes
<b>SYN Flood</b>	Max TCP Open Handshaking Count(Def=100 s)				Yes
<b>ICMP Flood</b>	Max ICMP Count (Def=100 s)				Yes
<b>ICMP Echo</b>	Max Ping Count (Def=15 s)				Yes

**Src IP:**Source IP

**Dst IP:**Destination IP

**Dst Port:**Destination Port

**Src Port:**Source Port

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 all' 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 nell'I-Storm ADSL Firewall Router 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 security 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 viene 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. L'I-Storm ADSL Firewall Router 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 specifiche 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. L'I-Storm ADSL Firewall Router elimina tutti i pacchetti con questa caratteristica.

### 3.8.2.4.3 MAC Address Filter

Tramite questa funzionalità è possibile filtrare ulteriormente il traffico limitando l'accesso in base all'indirizzo MAC degli apparati di rete. E' possibile bloccare l'accesso ad una lista di MAC Address oppure consentire l'accesso solo ad una lista di 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

MAC Address Filter	
Filtering Rules	
MAC Address Filter	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
For LAN ethernet frames, only the following Source MAC Address(es) are	<input type="radio"/> Allowed <input checked="" type="radio"/> Blocked
MAC Address	<input type="text" value="00:00:00:00:00:00"/>
	<input type="text"/>
<input type="button" value="Apply"/>	

E' possibile inserire sino a 10 indirizzi MAC.



### 3.8.2.4.4 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. E' possibile bloccare l'accesso ad alcuni siti oppure consentire l'accesso solo ad una lista opportuna di siti. E' 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).

URL Filter	
Configuration	
URL Filtering	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Block Mode	<input checked="" type="radio"/> Always Block
	<input type="radio"/> Block from <input type="text" value="08"/> : <input type="text" value="00"/> to <input type="text" value="18"/> : <input type="text" value="00"/> <input type="text" value="Monday"/> to <input type="text" value="Friday"/>
Keywords Filtering	<input type="checkbox"/> Enable <a href="#">Details</a>
Domains Filtering	<input type="checkbox"/> Enable <a href="#">Details</a>
	<input type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict URL Features	<input type="checkbox"/> Block Java Applet
	<input type="checkbox"/> Block surfing by IP address

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 filtri.

Spuntando la voce **URL Blocking Log** (nella sezione **Firewall 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.

E' 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 **Disable all Web traffic except for Trusted Domain**).

In questo modo è possibile limitare l'accesso ai soli siti ritenuti opportuni e controllare comunque in **Status Event Log** tutti i tentativi di violazione dell'URL **Filtering**.

Selezionando **Block Java Applet** è possibile bloccare Applet Java.

Selezionando **Block surfing by IP address** è possibile impedire l'inserimento di IP al posto dell'URL (questo serve per evitare che utenti smalzati aggirino il blocco dell'URL inserendo direttamente l'indirizzo IP del sito bloccato).

#### Esempio:

E' possibile permettere l'accesso solo ad una lista di domini determinata.

Abilitare, come da figura sotto, la funzionalità URL Blocking. E, visto che lo scopo è quello di consentire l'accesso ad una lista di domini determinata e bloccare tutti quelli non contenuti nella lista l'approccio da seguire è quello di creare una lista contenente i domini permessi e vietare l'accesso a quelli esclusi. Si termini la configurazione del dispositivo come in figura.



### URL Filter

**Configuration**

URL Filtering	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Block Mode	<input checked="" type="radio"/> Always Block
	<input type="radio"/> Block from <input type="text" value="08"/> : <input type="text" value="00"/> to <input type="text" value="18"/> : <input type="text" value="00"/> <input type="text" value="Monday"/> to <input type="text" value="Friday"/>
Keywords Filtering	<input type="checkbox"/> Enable <a href="#">Details</a>
Domains Filtering	<input checked="" type="checkbox"/> Enable <a href="#">Details</a>
	<input checked="" type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict URL Features	<input type="checkbox"/> Block Java Applet
	<input type="checkbox"/> Block surfing by IP address

A questo punto non resta che immettere la lista di siti Trusted.

In figura vogliamo permettere l'accesso ai soli domini: [www.asus.it](http://www.asus.it), [www.dslreport.com](http://www.dslreport.com) e [www.iol.it](http://www.iol.it).

### Domain Name Filtering Configuration

**Parameters**

Behavior	Domain Name	Action
<input type="text" value="Trust"/>	<input type="text"/>	<input type="button" value="Add"/>

[Go back to URL Blocking Configuration](#)

#	Trust Domain Name	Action
1	<a href="http://www.iol.it">www.iol.it</a>	<input type="button" value="Delete"/>
2	<a href="http://www.libero.it">www.libero.it</a>	<input type="button" value="Delete"/>
3	<a href="http://www.asus.it">www.asus.it</a>	<input type="button" value="Delete"/>
4	<a href="http://www.dslreports.com">www.dslreports.com</a>	<input type="button" value="Delete"/>

#	Forbid Domain Name	Action
---	--------------------	--------



Nella lista dei siti Trusted si è però aggiunto [www.libero.it](http://www.libero.it). Questo perché il sito [www.iol.it](http://www.iol.it) viene reindirizzato. **Porre attenzione a questo fenomeno.**

E' possibile completare la configurazione attivando anche il Keyword Filtering, in questo modo anche questa ulteriore condizione viene verificata. Se, come da figura, viene bloccato la keyword **IT**, nell'esempio di prima il solo sito [www.dslreports.com](http://www.dslreports.com) resterebbe accessibile.



## Keywords Filtering Configuration

### Parameters

Keyword	Action	
<input type="text"/>	<input type="button" value="Add"/>	
<a href="#">Go back to URL Blocking Configuration</a>		
#	Keyword	Action
1	it	<input type="button" value="Delete"/>



Se contemporaneamente al **Domains Filtering** è attivato il **Keyword Filtering** il dispositivo farà uscire solo il traffico che soddisfa entrambi i filtri.

### 3.8.2.4.5 Firewall Log

E' possibile conservare nello status Log del dispositivo (consultabile alla sezione **Status-Event Log**) tutti gli eventi relativi alle sezioni: URL Blocking, Intrusion Detection e Packet Filtering. Per fare questo è sufficiente impostare su Enable la sezione opportune del Firewall.

## Firewall Log

### Event will be shown in the Status - Event Log

Filtering Log	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Intrusion Log	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
URL Blocking Log	<input checked="" type="radio"/> Enable <input type="radio"/> Disable



### 3.8.2.5 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 nascondere 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 caratteristiche 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 modalità:

- **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 crittazione per fornire servizi di autenticazione, integrità 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:

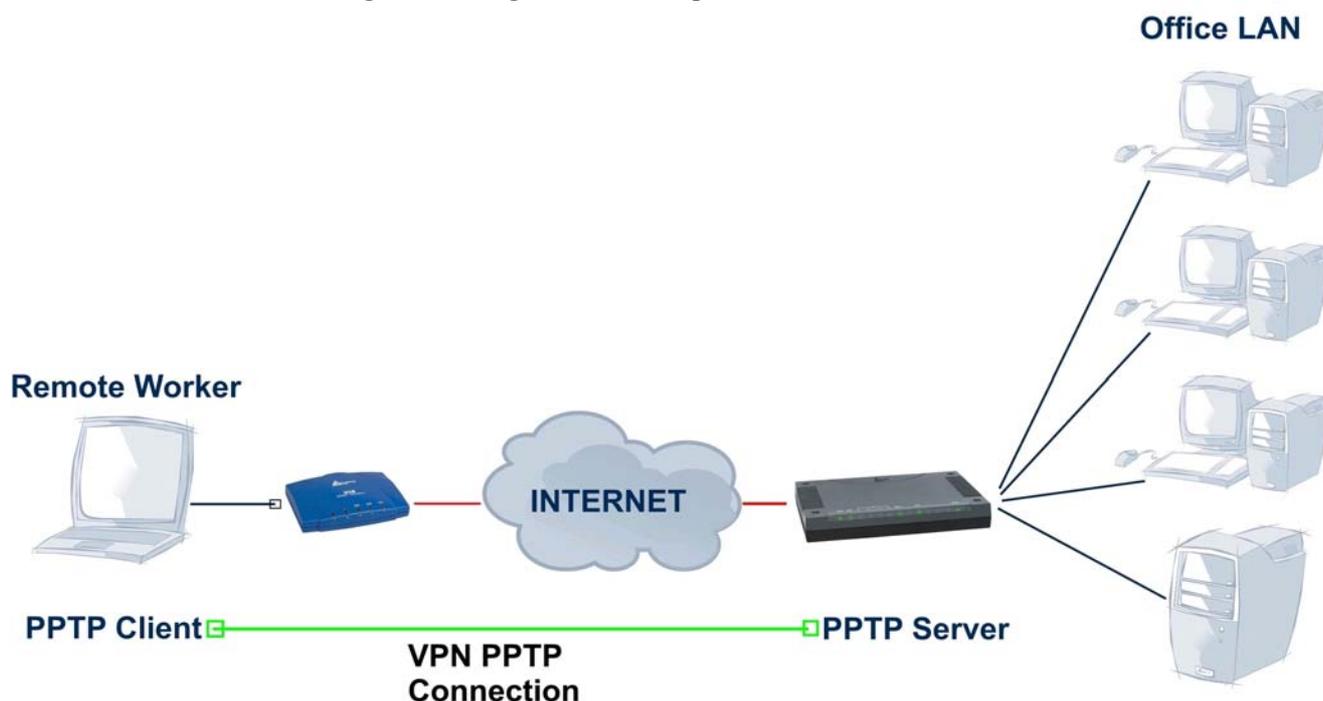
- **TRANSPORT MODE:** L’header del pacchetto IP viene lasciato inalterato, viene quindi preso in considerazione dagli algoritmi di crittaggio solo il payload del pacchetto stesso. Questo garantisce un livello di protezione minima delle informazioni perché è possibile scoprire mittente e destinatario dei dati.
- **TUNNELL MODE:** L’intero pacchetto IP viene crittato 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

### 3.8.2.5.1 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 conatterà 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**.



**PPTP**

**Remote Access Connection**

Connection Name	Dial-IN		
Type	<input type="radio"/> Dial out,	Server IP Address (or Hostname)	
	<input checked="" type="radio"/> Dial in,	Private IP Address Assigned to Dialin User	192.168.1.200
Username	Username		
Password	*****		
Auth. Type	Chap(Auto) ▾		
Data Encryption	Auto ▾	Key Length	Auto ▾
		Mode	stateful ▾
Idle Timeout	0 minutes		

Apply

Inserire nel campo **Connection Name** un nome che identifichi la connessione, selezionare **Dial-In** come tipologia di connessione e inserire l'IP (in **Private IP Address Assigned to Dialin User**) 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.

In Authentication Type (il valore di default è **Auto**) è possibile scegliere il tipo di autenticazione. Sono disponibili i protocolli CHAP (Challenge Handshake Authentication Protocol) e PAP (Password Authentication Protocol). Nel protocollo PAP la password viene inviata in maniera non criptata, mentre utilizzando il CHAP la password viene criptata prima di essere inviata.

In **Data Encryption** (il valore di default è **Auto**) è possibile forzare l'algoritmo MPPE per la criptazione. Nel campo **Key Length** è possibile forzare la lunghezza della chiave utilizzata per l'algoritmo MPPE (maggiori bit sono usate più elevato è il grado di sicurezza raggiunto).

In **Mode** è possibile scegliere tra le modalità **Stateful** (la chiave è cambiata ogni 256 pacchetti) o **Stateless** (cambiata in ogni pacchetto).

Nel campo **Idle Time** va inserito un valore positivo. Superato tale tempo senza alcuna attività la connessione VPN viene abbattuta. Mettendo come valore « 0 » la VPN viene sempre mantenuta attiva. 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 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.

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.



**Creazione guidata nuova connessione**



### Creazione guidata nuova connessione

Questa procedura guidata consente di:

- Connettere il computer a Internet.
- Connettere il computer a una rete privata, come una rete aziendale.
- Installare una rete domestica o una piccola rete aziendale.

Per continuare, scegliere Avanti.

< Indietro   **Avanti >**   Annulla

**Creazione guidata nuova connessione**

**Tipo di connessione di rete**  
Scegliere l'operazione da effettuare.



- Connessione a Internet**  
Consente di connettere il computer a Internet e di esplorare il Web e leggere la posta elettronica.
- Connessione alla rete aziendale**  
Consente di connettere il computer a una rete aziendale, mediante connessione remota o VPN e di lavorare da casa, da una filiale o da un'altra ubicazione.
- Installazione di una rete domestica o di una piccola rete aziendale**  
Consente di connettere il computer a una rete domestica o a una piccola rete aziendale esistente o di installarne una nuova.
- Installazione di una connessione avanzata**  
Consente di connettere il computer direttamente a un altro computer mediante la porta seriale, parallela o a infrarossi o di impostarlo per consentire la connessione di altri computer.

< Indietro   **Avanti >**   Annulla



**Creazione guidata nuova connessione**

**Connessione di rete**  
Scegliere la modalità di connessione alla rete aziendale.



Crea la seguente connessione:

- Connessione remota**  
Consente di connettere il computer alla rete mediante un modem e una normale linea telefonica oppure mediante una linea ISDN.
- Connessione VPN**  
Consente di connettere il computer alla rete mediante una connessione VPN (Virtual Private Network) su Internet.

< Indietro   Avanti >   Annulla

**Creazione guidata nuova connessione**

**Nome connessione**  
Specificare un nome per la connessione alla rete aziendale.

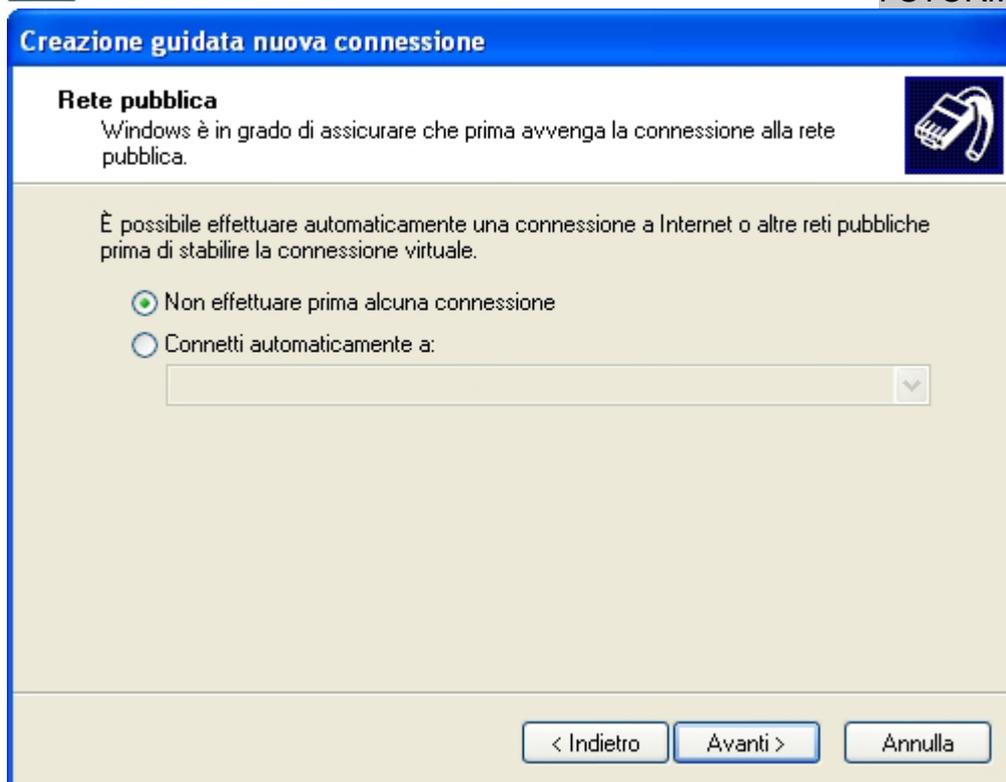


Immettere un nome per la connessione nella seguente casella.

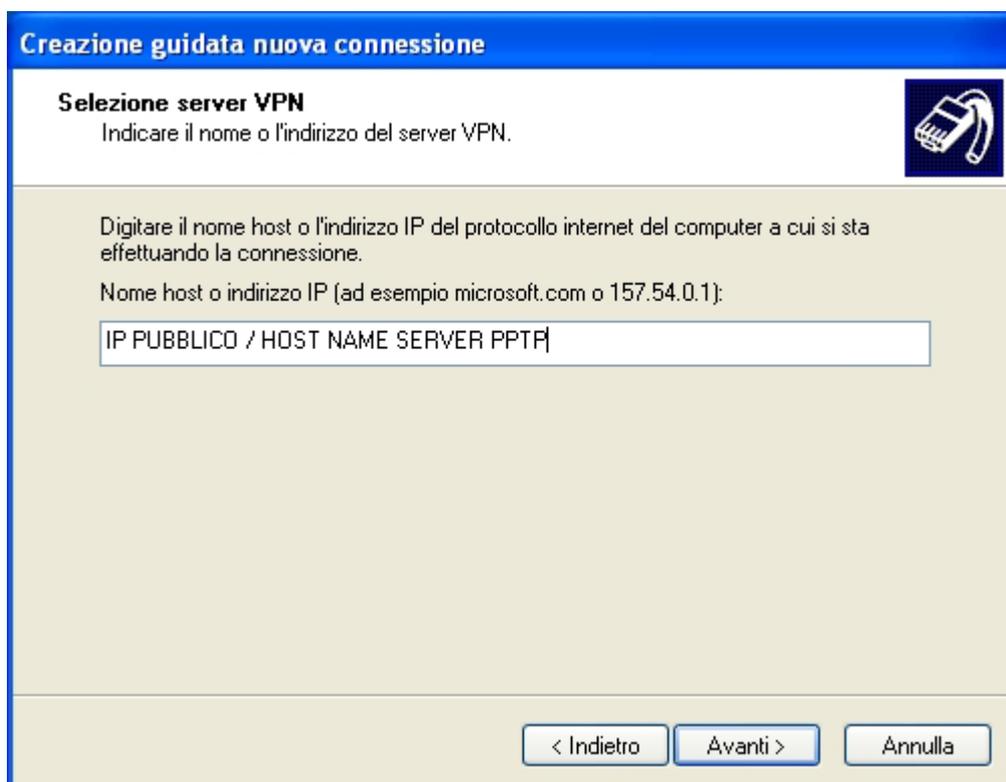
Nome società

Ad esempio, è possibile immettere il nome della rete aziendale o del server a cui si effettuerà la connessione.

< Indietro   Avanti >   Annulla



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 all’Appendice A di questo manuale.

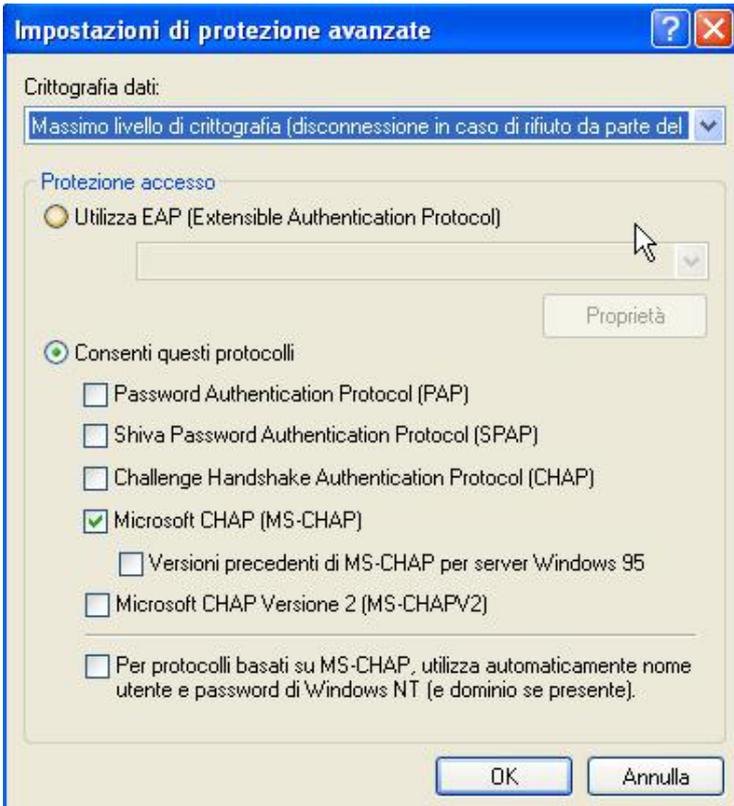


Verrà quindi creata sul desktop un'icona che permette di lanciare la connessione PPTP verso il router A02-RA3+.

Cliccare sull'icona col tasto destro, andare su **Proprietà**, poi su **Protezione**.



Spuntare la voce **Avanzate(impostazioni personalizzate)** e cliccare su **Impostazioni**.



Spuntare la voce **Microsoft CHAP (MS-CHAP)** e premere **OK** pre terminare.

La configurazione del client è terminata. Cliccare sull'icona della VPN, apparirà la finestra sottostante:



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.

E' 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.



## PPTP Status

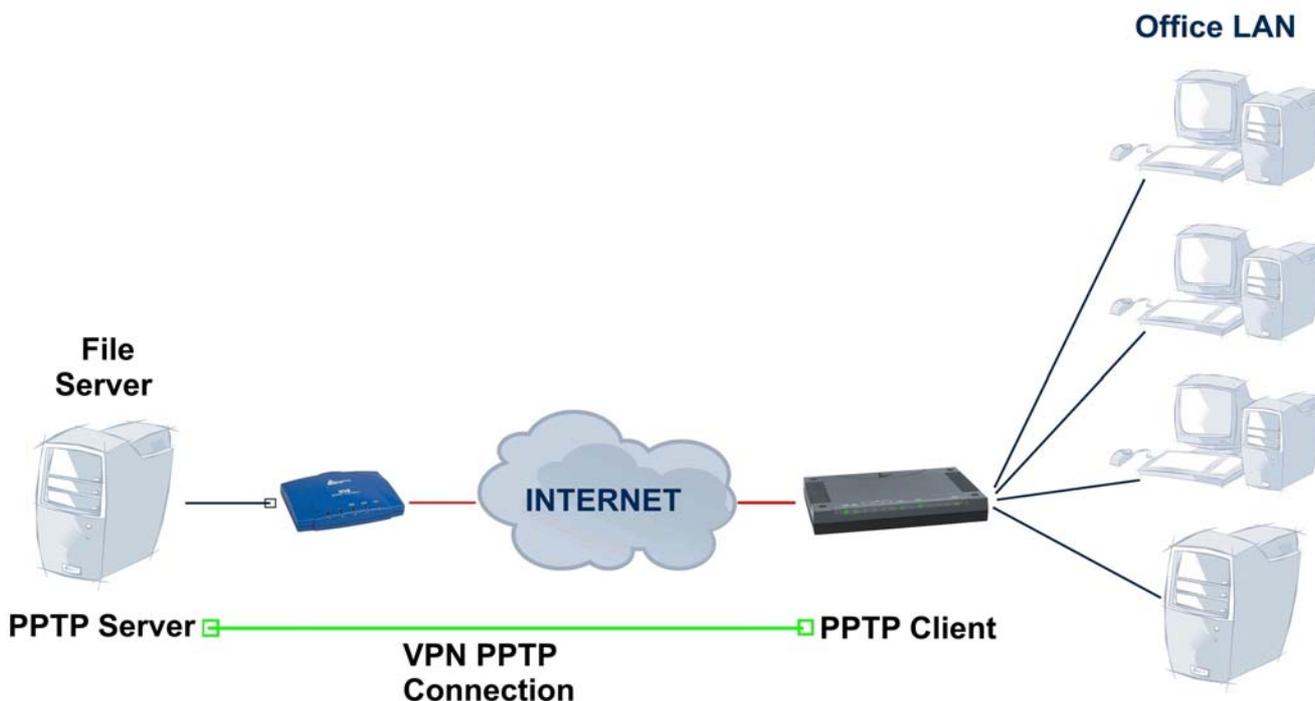
### VPN/PPTP for Remote Access Application

Name	Type	Enable	Active	Session Connected	Call Connected	Encryption
A02-RA4(In1)	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**.

### 3.8.2.5.2 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.

**PPTP****Remote Access Connection**

Connection Name	Dial-OUT		
Type	<input checked="" type="radio"/> Dial out,	Server IP Address (or Hostname)	82.107.134.56
	<input type="radio"/> Dial in,	Private IP Address Assigned to Dialin User	
Username	Username		
Password	*****		
Auth. Type	Chap(Auto) ▾		
Data Encryption	Enable ▾	Key Length	128 bits ▾ Mode stateful ▾
Idle Timeout	0 minutes		
<input type="button" value="Apply"/>			

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.

In Authentication Type (il valore di default è **Auto**) è possibile scegliere il tipo di autenticazione. Sono disponibili i protocolli CHAP (Challenge Handshake Authentication Protocol) e PAP (Password Authentication Protocol). Nel protocollo PAP la password viene inviata in maniera non criptata, mentre utilizzando il CHAP la password viene criptata prima di essere inviata.

In **Data Encryption** (il valore di default è **Auto**) è possibile forzare l'algoritmo MPPE per la criptazione. Nel campo **Key Length** è possibile forzare la lunghezza della chiave utilizzata per l'algoritmo MPPE (maggiori bit sono usate più elevato è il grado di sicurezza raggiunto).

In **Mode** è possibile scegliere tra le modalità **Stateful** (la chiave è cambiata ogni 256 pacchetti) o **Stateless** (cambiata in ogni pacchetto).

Nel campo **Idle Time** va inserito un valore positivo. Superato tale tempo senza alcuna attività la connessione VPN viene abbattuta. Mettendo come valore « 0 » la VPN viene sempre mantenuta attiva. 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 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.

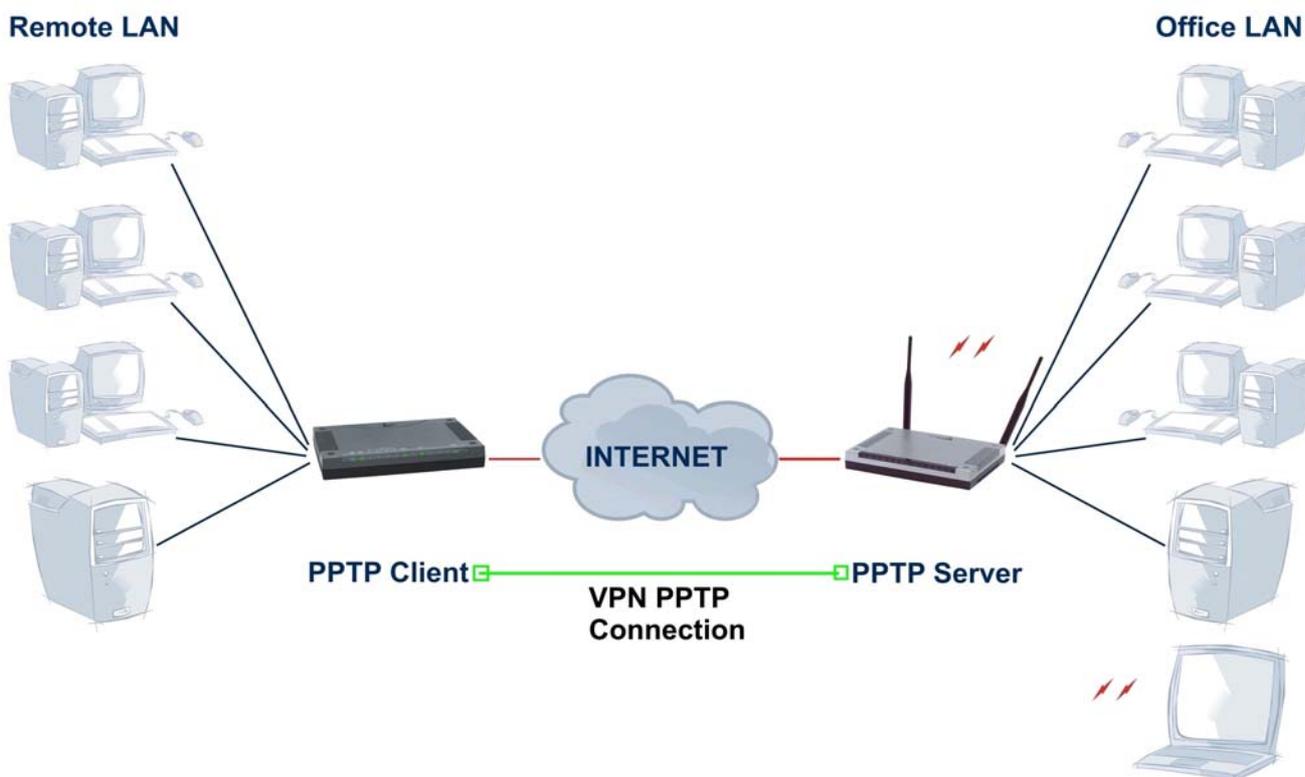
**PPTP Status****VPN/PPTP for Remote Access Application**

Name	Type	Enable	Active	Session Connected	Call Connected	Encryption
A02-RA4(In1)	dialin	✓	✓	✓	✓	encryption enabled mppe 128bits stateful mode



### 3.8.2.5.3 PPTP VPN – Lan to Lan

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



Vediamo quindi come configurare i due router A02-RA3+ / A02-WRA4-54G per mettere in comunicazione le due sedi:

	Remote LAN	Office LAN
<b>Product Code</b>	A02-RA3+	A02-WRA4-54G
<b>Picture</b>		
<b>Public IP</b>	80.17.56.78	69.121.1.32
<b>NAT</b>	Yes	Yes
<b>LAN IP</b>	192.168.1.X	192.168.2.X
<b>Subnet Mask</b>	255.255.255.0	255.255.255.0
<b>PPTP</b>	Client PPTP	Server PPTP

- **Remote LAN(A02-RA3+):** 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**.

PPTP			
LAN to LAN			
Connection Name	Lan-To-Lan		
Type	<input checked="" type="radio"/> Dial out,	Server IP Address (or Hostname)	69.121.1.32
	<input type="radio"/> Dial in,	Private IP Address Assigned to Dialin User	
Peer Network IP	192.168.2.0	Netmask	
Username	Username		
Password	*****		
Auth. Type	Chap(Auto) ▾		
Data Encryption	Auto ▾	Key Length	Auto ▾ Mode stateful ▾
Idle Timeout	0 minutes		
<input type="button" value="Apply"/>			

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.

- **Office LAN(A02-WRA4-54G):** 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**.

PPTP			
LAN to LAN			
Connection Name	Lan-To-Lan		
Type	<input type="radio"/> Dial out,	Server IP Address (or Hostname)	
	<input checked="" type="radio"/> Dial in,	Private IP Address Assigned to Dialin User	192.168.2.200
Peer Network IP	192.168.1.0	Netmask	255.255.255.0
Username	Username		
Password	*****		
Auth. Type	Chap(Auto) ▾		
Data Encryption	Auto ▾	Key Length	Auto ▾ Mode stateful ▾
Idle Timeout	0 minutes		
<input type="button" value="Apply"/>			

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.

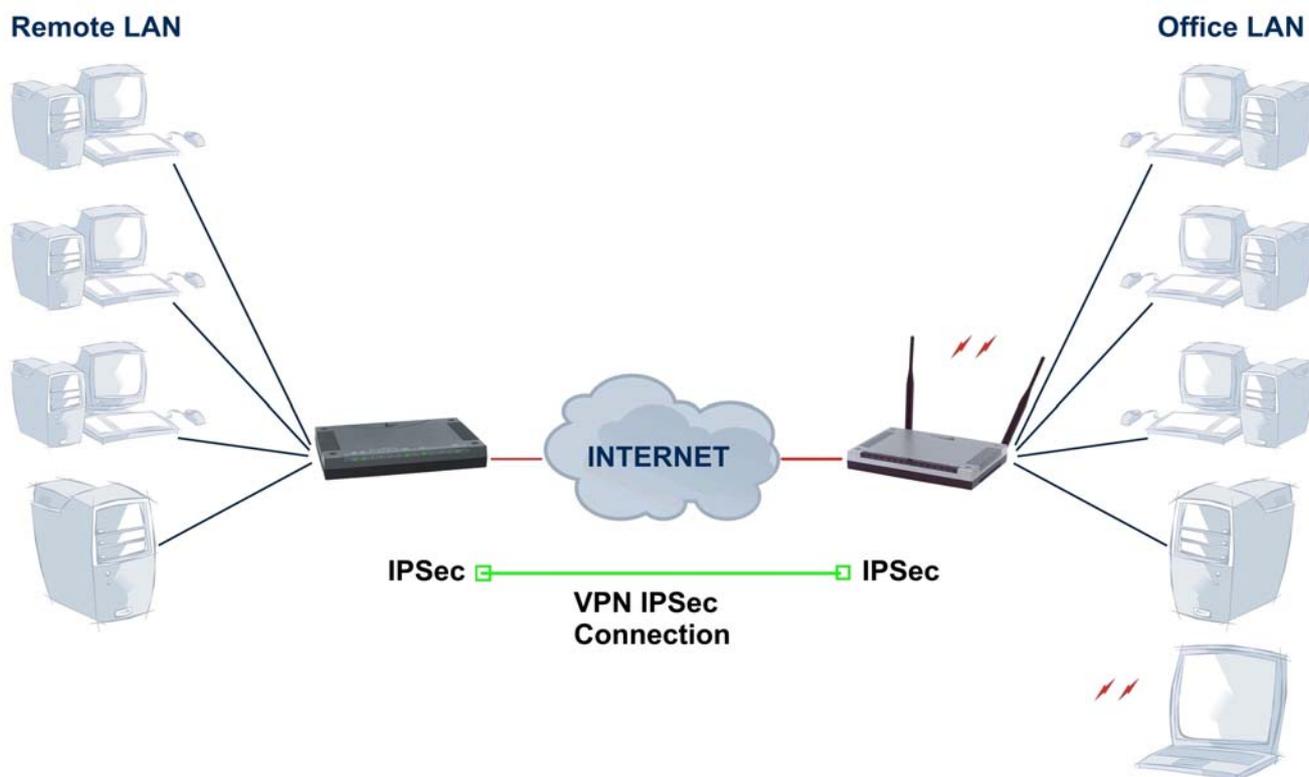
Ora le due reti potranno possono scambiare informazioni crittate. **E' importante che le due LAN appartengano a due subnet differenti, la configurazione mostrata sopra utilizza infatti una rete 192.168.1.0 e una 192.168.2.0.**

E' possibile verificare il corretto funzionamento della VPN PPTP cliccando sulla voce **Status** del menù e poi sulla voce **PPTP Status**.



### 3.8.2.5.4 IPsec VPN

In questo scenario due sedi remote verranno connesse tramite una VPN IPsec, gli utenti della Remote LAN devono condividere risorse e servizi con la Office LAN. La figura che segue riassume quanto detto.



	Remote LAN	Office LAN
<b>Product Code</b>	A02-RA3+	A02-WRA4-54G
<b>Picture</b>		
<b>Public IP</b>	69.121.1.31	69.121.1.32
<b>NAT</b>	Yes	Yes
<b>LAN IP</b>	192.168.1.X	192.168.2.X
<b>Subnet Mask</b>	255.255.255.0	255.255.255.0
<b>VPN IPsec</b>	ESP	ESP
<b>Encryption</b>	DES	DES
<b>Authentication</b>	MD5	MD5
<b>Perfect Forward Secrety</b>	None	None
<b>Pre Shared Key</b>	123456789	123456789



Selezionare in **Proposal** la tipologia di VPN. Sono disponibili 2 modalità differenti:

- AH (authentication header): provvede all'Autenticazione ma non alla Riservatezza
- ESP (Encapsulating Security Payload): provvede all'Autenticazione e Riservatezza

Selezionare poi in **Authentication** la modalità di autenticazione [permette di verificare l'identità del mittente (evitando ad esempio fenomeni di spoofing) e l'integrità della trasmissione]. Sono disponibili 3 differenti scelte:

- MD5 (Message Digest 5) : Algoritmo one-way hashing per generare hash di 128 bit
- SHA-1 (Secure Hash Algorithm) : Algoritmo one-way hashing per generare hash di 160 bit
- NONE

L'SHA-1 è senza dubbio la soluzione più sicura ma anche la più pesante.

Selezionare poi in **Encryption** (disponibile solo nelle VPN ESP) una delle quattro scelte:

- DES :algoritmo di criptazione che usa 56 bit
- 3DES : algoritmo di criptazione che usa in cascata 3 DES arrivando a 168 bit
- AES(Advanced Encryption Standards) : algoritmo di criptazione con 128 bit
- NONE

Il 3DES e AES sono certamente gli algoritmi più robusti ma incrementano i tempi di latenza.

In **Perfect Forward Secrecy** è possibile abilitare la metodologia Diffie-Hellman per cambiare le chiavi della VPN durante la seconda fase di negoziazione. Questa funzionalità aumenta la sicurezza ma allunga il tempo necessario alla costruzione della VPN. Diffie-Hellman è un protocollo di crittografia a chiave pubblica che permette a 2 parti di stabilire una chiave condivisa utilizzando un mezzo di comunicazione pubblico ed insicuro quale Internet. Sono disponibili 3 diverse modalità (MODP :Modular Exponentiation Groups.):MODP 768-bit, MODP 1024-bit e MODP 1536-bit.

In **Pre-shared Key** introdurre la chiave IKE (Internet Key Exchange). Immettere una stringa da 4 a 128 caratteri. Tale chiave va condivisa da entrambi i terminatori VPN. L'IKE è usata per stabilire una chiave condivisa.

Vediamo quindi come configurare i due router A02-RA3+ ed A02-WRA4-54G per mettere in comunicazione le due sedi (la configurazione è identica, il modello A02-WRA4-54G integra però un acceleratore 3DES hardware capace di 3.5Mbps di throughput e sino a 16 VPN IPSec):

- **Remote LAN(A02-RA3+):** 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**.



IPSec					
Create					
Connection Name	<input type="text" value="Lan-To-Lan"/>				
Local					
NetWork	<input type="radio"/> Single Address	IP Address	<input type="text"/>		
	<input checked="" type="radio"/> Subnet	IP Address	<input type="text" value="192.168.1.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
	<input type="radio"/> IP Range	IP Address	<input type="text"/>	End IP	<input type="text"/>
Remote					
Secure Gateway Address(or Hostname)	<input type="text" value="69.121.1.32"/>				
NetWork	<input type="radio"/> Single Address	IP Address	<input type="text"/>		
	<input checked="" type="radio"/> Subnet	IP Address	<input type="text" value="192.168.2.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
	<input type="radio"/> IP Range	IP Address	<input type="text"/>	End IP	<input type="text"/>
Proposal					
<input checked="" type="radio"/> ESP	Authentication	<input type="text" value="MD5"/>			
	Encryption	<input type="text" value="DES"/>			
<input type="radio"/> AH	Authentication	<input type="text" value="MD5"/>			
Perfect Forward Secrecy	<input type="text" value="None"/>				
Pre-shared Key	<input type="text" value="123456789"/>				
<input type="button" value="Apply"/> <a href="#">Advanced Options</a>					

Inserire nel campo **Connection Name** un 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**. E' 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**.

- **Office LAN(A02-WRA4-54G)::** 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**.



IPSec					
Create					
Connection Name	Lan-To-Lan				
Local					
NetWork	<input type="radio"/> Single Address	IP Address			
	<input checked="" type="radio"/> Subnet	IP Address	192.168.2.0	Netmask	255.255.255.0
	<input type="radio"/> IP Range	IP Address		End IP	
Remote					
Secure Gateway Address(or Hostname)		69.121.1.31			
NetWork	<input type="radio"/> Single Address	IP Address			
	<input checked="" type="radio"/> Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
	<input type="radio"/> IP Range	IP Address		End IP	
Proposal					
<input checked="" type="radio"/> ESP	Authentication	MD5			
	Encryption	DES			
<input type="radio"/> AH	Authentication	MD5			
Perfect Forward Secrecy	None				
Pre-shared Key	123456789				
<input type="button" value="Apply"/> <a href="#">Advanced Options</a>					

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**. E' 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**.

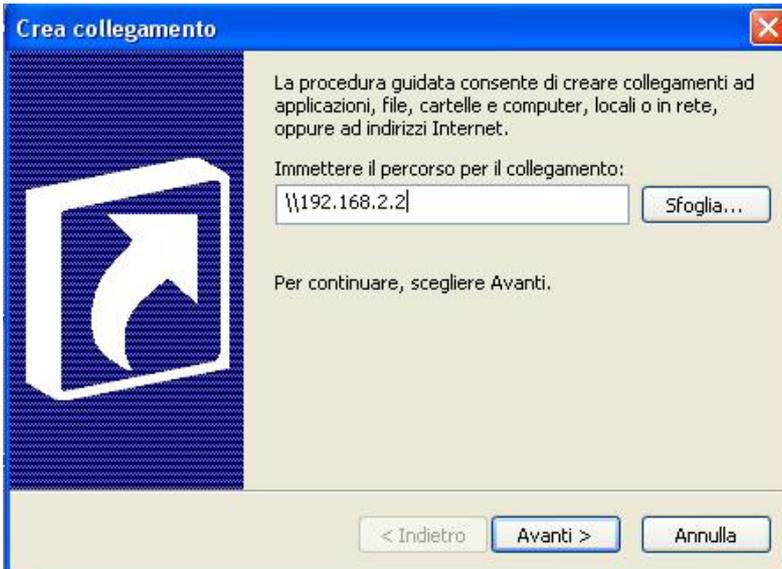
Ora le due reti potranno possono scambiare informazioni crittate. E' importante che le due LAN appartengano a due subnet differenti, la configurazione mostrata sopra utilizza infatti una rete 192.168.1.0 e una 192.168.2.0.

E' 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, verrà creato un tunnel VPN in IPSec tra le 2 LAN. Per verificare questo provare a pingare da un PC della LAN un PC dell'altra (settando opportunamente la sezione Firewall del Router affinché non tagli l'ICMP).

E' 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**. Apparirà la schermata sotto riportata.



Inserire nel campo vuoto l'indirizzo IP di un PC nella LAN remota per poter accedere alle risorse condivise.



Nel caso in cui l'abbonamento con uno dei Router ADSL sia con IP dinamico, la creazione della VPN IPsec può comunque essere costruita (almeno uno dei 2 Router deve comunque avere IP statico). In questo caso nella voce **Remote Secure Gateway Access** del Router con IP fisso immettere il valore 0.0.0.0. In questo modo potrà costruire tunnel VPN IPsec con un Router remoto di cui non è, a priori, noto l'IP.



### 3.8.2.6 QoS

Grazie alla funzionalità QoS è possibile controllare il traffico diretto alla LAN verso la WAN. E' possibile assegnare diversi profili con diverse priorità oppure velocità di upload determinate per ogni applicazione proveniente dalla LAN. In questo modo, quando l'upstream della connessione ADSL è saturo, è comunque possibile avere una qualità di servizio accettabile.

Sotto la voce QoS sono disponibili 2 differenti voci:

- Prioritization
- IP Throttling

#### 3.8.2.6.1 Prioritization

Sono disponibili 3 livelli:

- High
- Normal (tutti il traffico ha questo livello di default)
- Low

Il router alloca il 60% delle risorse ai pacchetti appartenenti al livello High, il 10% ai pacchetti appartenenti al livello Low. Il resto delle risorse (30%) viene utilizzato dai restanti pacchetti.

Prioritization					
Configuration (from LAN to WAN packet)					
Enable	Application	Priority	Protocol	Source Port	Source IP Address Range (0.0.0.0' means Any)
				Destination Port	Destination IP Address Range (0.0.0.0' means Any)
<input type="checkbox"/>	PPTP	High	GRE	none	
<input type="checkbox"/>		High	any	0 ~ 0	
<input type="checkbox"/>		High	any	0 ~ 0	

Vediamo le varie voci presenti :

- **Enable:** spuntare per attivare
- **Application:** introdurre un nome univoco (senza spazi) che identifichi la regola.
- **Priority:** impostare il livello di priorità tra High o Low.
- **Protocol:** scegliere il protocollo di livello 4 tra: TCP, UDP, IGMP, ANY o GRE.
- **Source Port:** introdurre la porta o intervallo di porte di provenienza.
- **Destination Port:** introdurre la porta o intervallo di porte di destinazione.
- **Source IP Address Range:** introdurre l'IP o intervallo IP di provenienza.
- **Destination IP address Range:** introdurre l'IP o intervallo IP di destinazione.

In figura, un esempio, in cui si è data la massima priorità al traffico :

HTTP[navigazione WEB], proveniente da un determinato IP [192.168.1.5]

SMTP[invio posta], proveniente da un range di IP [192.168.1.5 : 192.168.1.9]

POP3[ricezione posta], proveniente da un range di IP [192.168.1.10 : 192.168.1.20]

Si è lasciato come IP di destinazione 0.0.0.0 per non perdere in generalità.



<input checked="" type="checkbox"/>	HTTP	High	tcp	0	~ 0	192.168.1.5	~ 192.168.1.5
				80	~ 80	0.0.0.0	~ 0.0.0.0
<input checked="" type="checkbox"/>	SMTP	High	tcp	0	~ 0	192.168.1.5	~ 192.168.1.9
				25	~ 25	0.0.0.0	~ 0.0.0.0
<input checked="" type="checkbox"/>	POP3	High	tcp	0	~ 0	192.168.1.10	~ 192.168.1.20
				110	~ 110	0.0.0.0	~ 0.0.0.0

### 3.8.2.6.2 IP Throttling

Grazie all'IP Throttling è possibile limitare, in maniera statica, la velocità di upload in multipli di 32Kbps.

Vediamo le varie voci presenti :

- **Enable:** spuntare per attivare
- **Application:** introdurre un nome univoco (senza spazi) che identifichi la regola.
- **Protocol:** scegliere il protocollo di livello 4 tra: TCP, UDP, IGMP, ANY o GRE.
- **Source Port:** introdurre la porta o intervallo di porte di provenienza.
- **Destination Port:** introdurre la porta o intervallo di porte di destinazione.
- **Source IP Address Range:** introdurre l'IP o intervallo IP di provenienza.
- **Destination IP address Range:** introdurre l'IP o intervallo IP di destinazione.
- **Upstream Rate Limit :** Limite fisico del traffico da LAN-WAN. Introdurre un numero intero, il valore è in multipli di 32Kbps del numero introdotto.

Vediamo un esempio in figura:

IP Throttling							
Configuration (from LAN to WAN packet)							
Enable	Application	Protocol	Source Port		Source IP Address Range (0.0.0.0' means Any)		Upstream Rate Limit
			Destination Port		Destination IP Address Range (0.0.0.0' means Any)		
<input checked="" type="checkbox"/>	FTP	tcp	20	~ 21	192.168.1.9	~ 192.168.1.9	2 *32 (kbps)
			0	~ 0	0.0.0.0	~ 0.0.0.0	

In figura si è limitato un ipotetico server FTP (sull'IP 192.168.1.9) ad un traffico in Upload di 64Kbps.



### 3.8.2.7 Virtual Server

Il firewall/NAT 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 utilizza 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. E' 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.



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

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

Virtual Server					
Port Mapping Table					IP Table
Enable	Application	Protocol	External Port	Redirect Port	IP Address
<input type="checkbox"/>	FTP	TCP	21	0 ~ 0	192.168.1.
<input type="checkbox"/>	Telnet	TCP	23	0 ~ 0	192.168.1.
<input type="checkbox"/>	SMTP	TCP	25	0 ~ 0	192.168.1.
<input type="checkbox"/>	HTTP	TCP	80	0 ~ 0	192.168.1.
<input type="checkbox"/>	POP3	TCP	110	0 ~ 0	192.168.1.
<input type="checkbox"/>	NNTP	TCP	119	0 ~ 0	192.168.1.
<input type="checkbox"/>	NTP	UDP	123	0 ~ 0	192.168.1.
<input type="checkbox"/>	HTTPS	TCP	443	0 ~ 0	192.168.1.
<input type="checkbox"/>	IKE	UDP	500	0 ~ 0	192.168.1.
<input type="checkbox"/>	T.120	TCP	1503	0 ~ 0	192.168.1.
<input type="checkbox"/>	H.323	TCP	1720	0 ~ 0	192.168.1.
<input type="checkbox"/>	PPTP	TCP	1723	0 ~ 0	192.168.1.
<input type="checkbox"/>	SIP	TCP/UDP	5060	0 ~ 0	192.168.1.
<input type="checkbox"/>	CUSeeMe	TCP	7648	0 ~ 0	192.168.1.
<input type="checkbox"/>		tcp	0 ~ 0	0 ~ 0	192.168.1.
<input type="checkbox"/>		tcp	0 ~ 0	0 ~ 0	192.168.1.
<input type="checkbox"/>		tcp	0 ~ 0	0 ~ 0	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.

<input checked="" type="checkbox"/>	HTTP	TCP	80	0 ~ 0	192.168.1.2
-------------------------------------	------	-----	----	-------	-------------

In questo caso non va impostato il client DHCP sul PC poichè in tal caso l'IP [che è il server Web ] potrebbe cambiare (benchè la funzionalità Fixed Host permette di risolvere questo problema).

E' importante capire che l'I-Storm ADSL Router 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.

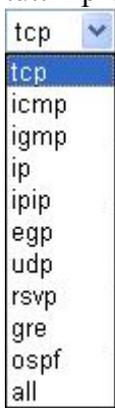
Sono anche presenti 10 Virtual Server non preconfigurati, come da figura:



## I-STORM LAN ROUTER ADSL

<input type="checkbox"/>		tcp	0	~0	0	~0	192.168.1.	
<input type="checkbox"/>		tcp	0	~0	0	~0	192.168.1.	
<input type="checkbox"/>		tcp	0	~0	0	~0	192.168.1.	
<input type="checkbox"/>		tcp	0	~0	0	~0	192.168.1.	
<input type="checkbox"/>		tcp	0	~0	0	~0	192.168.1.	
<input type="checkbox"/>		tcp	0	~0	0	~0	192.168.1.	
<input type="checkbox"/>		tcp	0	~0	0	~0	192.168.1.	
<input type="checkbox"/>		tcp	0	~0	0	~0	192.168.1.	
<input type="checkbox"/>		tcp	0	~0	0	~0	192.168.1.	
<input type="checkbox"/>		tcp	0	~0	0	~0	192.168.1.	

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



**DMZ:** E' 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).

Enable	Application	Protocol	Port	IP Address
<input type="checkbox"/>	DMZ	ALL	ALL	192.168.1.



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.



Per problemi sul 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. Consultare eventuali aggiornamenti di questo manuale (scaricabile dal sito [www.atlantis-land.com](http://www.atlantis-land.com))

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 Messenger	Nessuno	TCP da 6891-6900 TCP 1863 TCP 6901 UDP 1863 UDP 6901 UDP 5190
VNC	Nessuno	TCP 5900

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).

<input checked="" type="checkbox"/>	T.120	TCP	1503	0	~0	192.168.1.12
<input checked="" type="checkbox"/>	H.323	TCP	1720	0	~0	192.168.1.12



Attenzione il Router può gestire un numero non infinito di connessioni entranti, pertanto per grandi range (o centinaia di connessioni cointemporanee) 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



### 3.8.2.8 Advanced

Sono disponibili le seguenti sottosezioni:

- **Static Route**
- **Dynamic DNS**
- **Check Emails**
- **Device Management**

#### 3.8.2.8.1 Routing Table

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

Static Route			
Create			
Destination	<input type="text"/>		
Netmask	<input type="text"/>		
via Gateway	<input type="text"/>	or Interface	<input type="text" value="v"/>
Cost	<input type="text" value="1"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

**Destination:** Introdurre l'IP di destinazione.

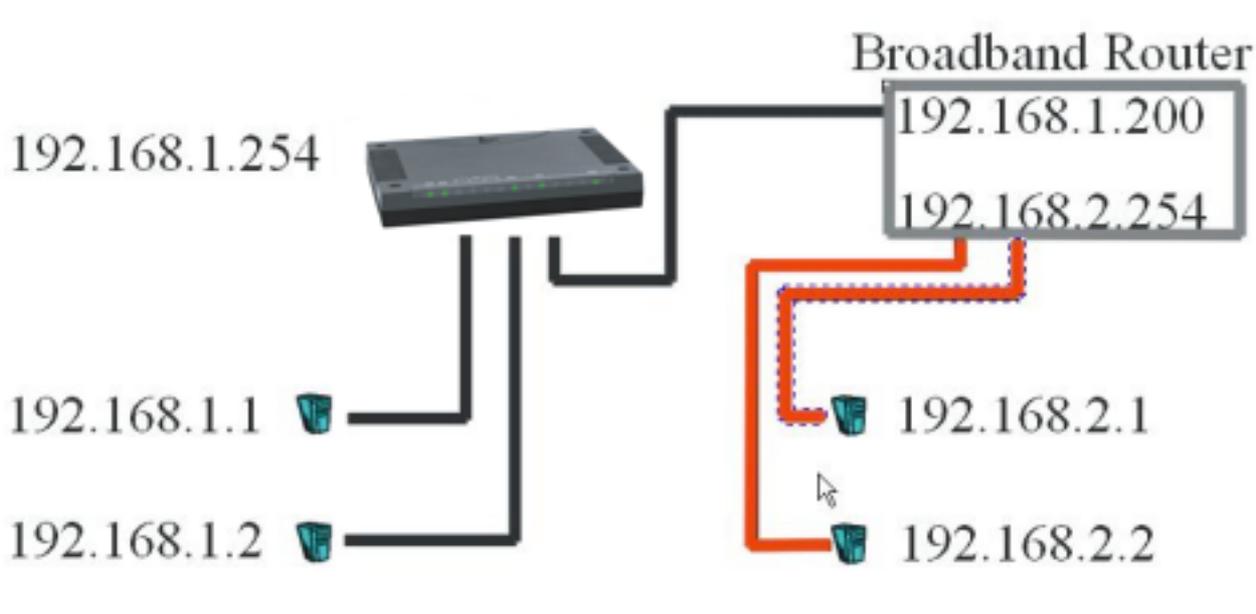
**Netmask:** Introdurre la Subnet.

**Gateway:** Introdurre l'IP della macchina che fa Nat sulla classe indirizzata

**Cost:** Introdurre il costo in HOP. Usualmente tale valore è 1. Mettere tale valore in funzione del numero di Router che è necessario attraversare per arrivare alla rete desiderata.

**Interface:** Selezionare il tipo di interfaccia (iplan, per l'interfaccia LAN)

Viene riportato un esempio per meglio chiarire questo concetto. 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.



### Static Route

**Create**

Destination	192.168.2.1		
Netmask	255.255.255.0		
via Gateway	192.168.1.200	or Interface	ip1an
Cost	1		

Apply Cancel

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'I-Storm 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**.

### 3.8.2.8.2 Dynamic 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 DDNS il nuovo indirizzo IP. Associando tale funzionalità con il Virtual Server è, ad esempio, possibile:

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

I passaggi da seguire sono i seguenti:

### Dynamic DNS

**Parameters**

Dynamic DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Dynamic DNS Server	www.dyndns.org (dynamic)
Domain Name	atlantisland.dyndns.org
Username	username
Password	*****
Period	28 Day(s)

Apply Cancel

I passaggi da seguire sono i seguenti:

- Registrare il proprio dominio gratuitamente e istantaneamente su **www.dyndns.org**, **www.zoneedit.com**.
- Configurare il client sull'I-Storm Router 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. E' 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 DDNS che gli restituirà di volta in volta l'indirizzo IP assegnato al Router A02-RA3+ dall'ISP. Usando la funzionalità di riconnessione (disponibile in PPPoA e PPPoE), qualora la connessione dovesse cadere, il Router la rialzerà immediatamente.



E' buona norma, al fine di evitare la sospensione per abuso del servizio, prendere nota delle condizioni praticate dal fornitore di servizio Dynamic DNS e aumentare il campo **Period** in modo rispettare tali politiche.

### 3.8.2.8.3 Check Emails

Questa funzionalità permette al Router di controllare se nell'account di posta preconfigurato è arrivata una nuova mail. In caso affermativo farà lampeggiare il LED PPP/MAIL. In questo modo, semplicemente guardando il Router, è possibile sapere se sono arrivate nuove mail.

Check Email	
Parameters	
Check Email	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Account Name	<input type="text"/>
Password	<input type="text"/>
POP3 Mail Server	<input type="text"/>
Period	<input type="text" value="60"/> minutes
Dial-out for Checking Emails	<input type="checkbox"/> Automatic
<input type="button" value="Apply"/>	

Per la configurazione è sufficiente spuntare **Enable** e configurare l'account da controllare, scegliendo l'intervallo di controllo. Abilitando la voce **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.**

Quando il Router rileverà una mail nell'account configurato farà lampeggiare il LED PPP/MAIL.

### 3.8.2.8.4 Device Management

E' possibile spostare la porta tramite cui si effettua la configurazione remota del Router, impostare il tempo di auto-logout ad un preciso indirizzo IP (lasciando invece 0.0.0.0 è possibile configurare il Router da qualsiasi IP).

E' inoltre possibile Abilitare/Disabilitare la funzionalità Universal Plug and Play e stabilirne la porta.



## Device Management

### Embedded Web Server

* HTTP Port	<input type="text" value="80"/>	(80 is default HTTP port)
Management IP Address	<input type="text" value="0.0.0.0"/>	('0.0.0.0' means Any)
Expire to auto-logout	<input type="text" value="180"/>	seconds

### Universal Plug and Play (UPnP)

UPnP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
* UPnP Port	<input type="text" value="2800"/>

Infine è possibile configurare il protocollo SNMP.

SNMP Access Control			
SNMP V1 and V2			
Read Community	<input type="text" value="public"/>	IP Address	<input type="text" value="0.0.0.0"/>
Write Community	<input type="text" value="password"/>	IP Address	<input type="text" value="0.0.0.0"/>
Trap Community	<input type="text"/>	IP Address	<input type="text"/>
SNMP V3			
Username	<input type="text"/>	Password	<input type="text"/>
Access Right	<input checked="" type="radio"/> Read <input type="radio"/> Read/Write	IP Address	<input type="text"/>

**SNMP Access Control** (E' richiesto un software apposito in un PC della LAN) – Simple Network Management Protocol.

- **Read Community:** Specificare il nome per identificare la Read Community (e l'indirizzo IP da cui si può accedere). E' una sorta di password che il dispositivo controlla prima di concedere l'accesso in lettura dei dati.
- **Write Community:** Specificare il nome per identificare la Write Community (e l'indirizzo IP da cui si può accedere). E' una sorta di password che il dispositivo verifica prima di poter accedere alla configurazione.
- **Trap Community:** Specificare un nome per identificare una Trap Community e un indirizzo IP cui verranno inviate le Trap.

### SNMP: SNMPv2c eSNMPv3

L'SNMPv2c include le caratteristiche avanzate del protocollo SNMPv2, esclusa la sicurezza che è rimasta quella del protocollo SNMPv1.

SNMPv3 include un robusto meccanismo di autenticazione per la configurazione remota.

Le **Traps** supportate sono: Cold Start, Authentication Failure.

Le **MIBs** supportate sono:

- **RFC 1213 (MIB-II):**
  - System group
  - Interfaces group
  - Address Translation group
  - IP group
  - ICMP group
  - TCP group
  - UDP group



- EGP (not applicable)
- Transmission
- SNMP group
- **RFC1650 (EtherLike-MIB):**
  - dot3Stats
- **RFC 1493 (Bridge MIB):**
  - dot1dBase group
  - dot1dTp group
  - dot1dStp group (if configured as spanning tree)
- **RFC 1471 (PPP/LCP MIB):**
  - pppLink group
  - pppLqr group
- **RFC 1472 (PPP/Security MIB):**
  - PPP Security Group)
- **RFC 1473 (PPP/IP MIB):**
  - PPP IP Group
- **RFC 1474 (PPP/Bridge MIB):**
  - PPP Bridge Group
- **RFC1573 (IfMIB):**
  - ifMIBObjects Group
- **RFC1695 (atmMIB):**
  - atmMIBObjects
- **RFC 1907 (SNMPv2):**
  - only snmpSetSerialNo OID

### 3.8.3 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 cliccare su **Save Config to FLASH** e poi su **Save**. In questo modo verrà scritto su eeprom e dunque caricato ad ogni boot del dispositivo.

### 3.8.4 Logout

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



## 3.9 Console e/o Telnet

E' possibile configurare il Router ADSL sia tramite Telnet (username=**admin** e la password=**atlantis**) che tramite Console.

Per la configurazione tramite Telnet è sufficiente 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). Collegare al PC il Wireless Router tramite il cavo DB9-PS2 incluso nella confezione.

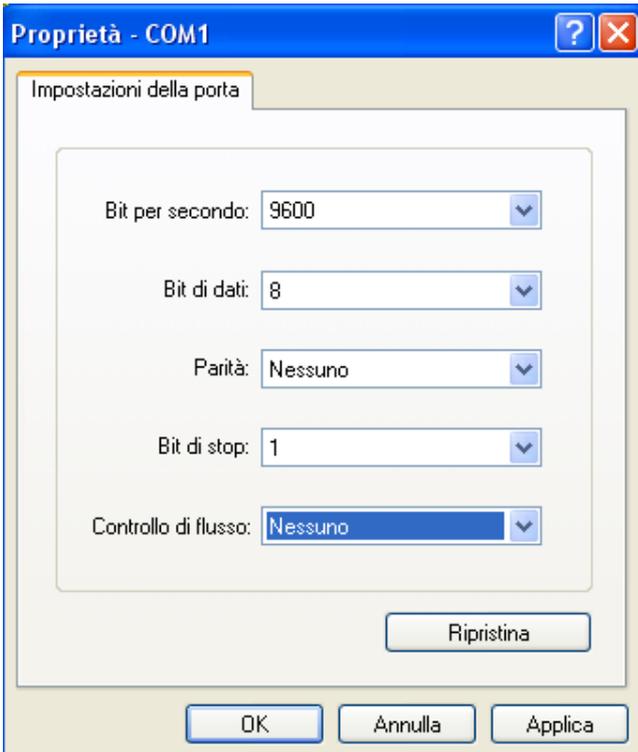
In XP, ad esempio, andare su **Start-tutti programmi-accessori-comunicazioni-hyperterminal**



Introdurre il nome da dare alla connessione e premere **OK**.

Scegliere la porta **COM** cui è collegato l'I-Storm ADSL Router

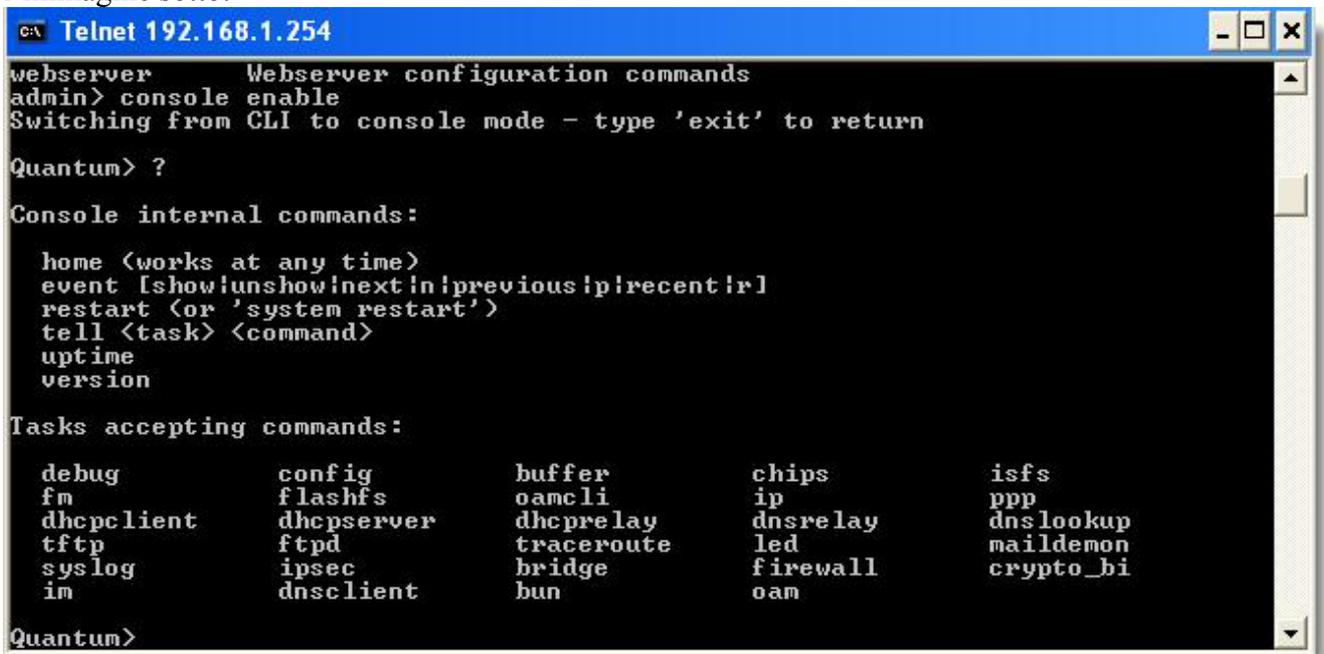
Inserire i settaggi come da figura (bit per secondo=9600, Bit di dati=8, Parità=Nessuno, Bit di Stop=1, controllo di flusso=Nessuno):



Premere su **Applica** e poi **OK**.

Premere **INVIO** e digitare username e password.

Digitando **Console Enable** seguito da **INVIO** il router passerà nella modalità console. Apparirà l'immagine sotto:



Utilizzando il comando **help** seguito dal tasto invio è possibile vedere la lista di tutti i comandi disponibili. Digitando il nome del comando (se riferito ad un processo) seguito da invio e poi digitando **help all** è possibile vedere tutti i comandi relativi all'opportuno processo. Per tornare alla root è 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 firmware installato nel dispositivo)



Per una più dettagliata descrizione si rimanda al manuale **ATMOS 9.0** di **Virata** su cui questo firmware è basato. Tutte le principali funzionalità sono comunque state implementate nell'interfaccia WEB la cui configurazione è stata ampiamente trattata in questo manuale.





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

## Problemi alla partenza dell'I-Storm ADSL Router

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 sulla posizione ON. Qualora il problema persistesse potrebbe essere un problema hardware. Rivolgersi, in questo caso, al supporto tecnico di Atlantis Land.

## Password ?

Problema	Azioni correttive
Password e/o IP dimenticata.	E' possibile , perdendo la configurazione del dispositivo, resettarlo premendo l'apposito bottone (per almeno 6 secondi) posto sul retro. Per ritrovare l'IP è sufficiente lanciare l'utility (CDRom:\utility\A02-RA3+Finder.exe) e cliccare su <b>search</b> .



## Non è possibile entrare nel Router via WEB

Problema	Azioni correttive
Pur digitando l'IP del Router (192.168.1.254) non si ottiene alcuna risposta.	<p>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 senza autopolarità.</p> <p>Effettuare un Ping verso l'IP del Router, se questo risponderà è possibile configurare il Router via web utilizzando IE.</p> <p>Qualora non si riuscisse ancora ad entrare, è opportuno controllare l'indirizzo IP del PC (digitare WINIPCFG per Win98/ME/SE o IPCONFIG per WIN2000/XP) e spostarlo sulla classe 192.168.1.x (ad esempio 192.168.1.1, subnet=255.255.255.0 e default gateway quello del Router).</p>

## Problemi con l'interfaccia WAN

Problema	Azioni correttive
Fallisce l'inizializzazione della connessione PVC.	<p>Anzitutto è necessario 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.</p> <p>Andare (se si utilizza il protocollo PPPoA o PPPoE) in System e qui sotto la sezione WAN controllare lo stato della connessione (il bottone deve essere sullo stato DISCONNECT e , qualora così non fosse cliccarci sopra).</p> <p>Qualora il problema persistesse contattare l'ISP e verificare tali parametri.</p>

## Problemi con l'interfaccia LAN

Problema	Azioni correttive
Non è possibile fare il ping con alcun PC della LAN.	<p>Controllare i LED LAN, nel pannello frontale. Tale LED dovrebbe essere acceso(almeno uno dei 4). Se così non fosse controllare il cablaggio.</p> <p>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.</p>



## Problemi di Connessione ad un Remote Node oppure ad un ISP

Problema	Azioni correttive
Il Router non riesce a connettersi ad un remote node o ad un ISP.	Fare riferimento alla Status e poi ADSL 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 " <b>winipcfg</b> " 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 " <b>winipcfg.exe</b> " è disponibile per Win95, 98 e ME. Per WinNT, Win2000 e WinXP utilizzare l'utility " <b>ipconfig</b> ".

## 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 ( <b>glite, gdmr, multi, ansi etc</b> ). Andare su <b>Status</b> e poi premere su <b>A1</b> ed impostare tramite la combo box di <b>Connect Mode</b> la modulazione più adatta. Cliccare su <b>Save config to Flash</b> e poi su <b>save</b> per rendere permanenti le modifiche.



## Cos'è il NAT?

Quesito	Risposta
Cosa fa esattamente il NAT?	<p>Nat significa Network Address Translation (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 realizza 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 privata a quelli pubblici ed il contrario. Il Router I-Storm 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 <b>IP provenienza</b> 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 questo in base a tabelle memorizzate provvederà al processo contrario e li spedisirà al PC interessato nella Lan.</p>

## Percorso dei pacchetti

Problema	Azioni correttive
Non funziona il Server settato su un PC della LAN privata.	<p>Il Router ADSL applica, ad ogni pacchetto, nell'ordine:</p> <ul style="list-style-type: none"><li>• Firewall</li><li>• Virtual Server</li><li>• DMZ</li></ul> <p>Affichè il Server funzioni bisogna accertarsi che nessun blocco antecedente al VS (Firewall) o DMZ (Firewall e VS) non operi in conformità.</p> <p>Settare il PC che funge da Server con un indirizzo IP privato fisso (o usare la modalità Fixed Host nel DHCP).</p>



## Non funziona correttamente un'applicazione Internet

Problema	Azioni correttive
<p>Alcune applicazioni, quando il Router fa NAT oppure è attivo il firewall, potrebbero non funzionare propriamente.</p>	<p>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:</p> <ul style="list-style-type: none"><li>• Alcuni Programmi di Email</li><li>• Alcuni Giochi Multi-Players</li><li>• Alcune Applicazioni Phone/Video Conferenza</li></ul> <p>Per trovare le porte da aprire per il corretto funzionamento dell'applicazione solitamente la strada più breve è quella di consultare il sito web del produttore dell'applicazione stessa. 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.</p>



## Perché nonostante il VS alcune applicazioni non vanno?

Problema	Azioni correttive
Per effettuando la rotazione delle porte col VS l'applicazione non funziona correttamente, cosa posso fare?	Potrebbe rendersi necessario effettuare una DMZ verso il PC su cui si vuole far girare una particolare applicazione.

## Perché nonostante la DMZ alcune applicazioni non vanno?

Problema	Azioni correttive
Pur utilizzando la DMZ l'applicazione non funziona ancora, che soluzioni adottare?	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 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) potrà accedere ad Internet.

## RFC 1483 Bridge su MAC OS 9

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



## RFC 1483 Bridge su MAC OS X

Problema	Soluzione
<p>Avendo un abbonamento di tipo PPPoE è possibile utilizzare il Router in modalità RFC 1483 Bridge con una macchina con MAC OS X ?</p> <p>Come va configurata ?</p>	<p>Al pari di Windows XP della Microsoft, il MacOSX di Apple, 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.</p> <p>La configurazione della connessione è molto semplice ed immediata:</p> <p>Innanzitutto, dal menù mela, cliccare sulla voce <b>Preferenze di sistema</b>.</p> <p>Nella cartella <b>Preferenze di sistema</b> cliccare su <b>Network</b>.</p> <p>Nella finestra <b>Network</b>, alla voce <b>Configura</b> selezionare <b>ETHERNET INTEGRATA</b>; poi, cliccare su <b>PPPoE</b>, ed inserire i dati forniti dal Provider:</p> <p>Se necessario, cliccare su "TCP/IP" dove è possibile inserire i DNS del Provider:</p> <p>A questo punto cliccare su <b>Registra</b> per salvare le modifiche.</p> <p>La connessione in PPPoE è stata creata!</p> <p>Per lanciare la connessione è sufficiente andare, dal menù <b>VAI</b>, nella cartella Applicazioni.</p> <p>Qui cliccare su <b>Internet Connect</b>, selezionare di nuovo, alla voce Configurazione, <b>Ethernet Integrata</b>, e cliccare su <b>COLLEGAMENTO</b> per la connessione ad Internet.</p>



## RFC 1483 Bridge su macchine Windows 95, 98, ME

Problema	Soluzione
Avendo un abbonamento di tipo PPPoE è possibile utilizzare il Router in modalità RFC 1483 Bridge con una macchina con Windows 95, 98, ME ? Come va configurata ?	<p>E' possibile usare un qualunque software (Enthernet, Win PoET, RasPPPoE). Sono allegate le istruzioni per RasPPPoE(freeware).</p> <p>Scompattare i vari file del pacchetto software in una cartella.</p> <p>Doppio click sull'icona <b>pannello di controllo</b> e poi doppio click su <b>rete</b>.</p> <p>Selezionare la voce <b>aggiungi</b>, poi scegliere <b>protocollo</b> e cliccare su <b>aggiungi</b>.</p> <p>Selezionare a questo punto <b>Disco Driver</b>.</p> <p>Selezionare la cartella dove precedentemente sono stati scompattati i driver e quindi scegliere uno qualsiasi dei 3 file.inf.</p> <p>A questo punto cliccare su <b>OK</b> e far riavviare la macchina. Al riavvio è necessario creare la connessione remota. A tal fine seguire i seguenti passaggi:</p> <p>Aprire la cartella <b>C:\Windows\System</b> e cliccare due volte sul file <b>rasppoe.exe</b>.</p> <p>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 <b>Create a Dial-Up connection for the selected Adapter</b> ed infine scegliere <b>exit</b>.</p> <p>Il processo è terminato, in Accesso Remoto è stata creata un'icona che basterà cliccare per azionare il collegamento ad internet.</p>



## RFC 1483 Bridge su macchine Windows 2000

Problema	Soluzione
Avendo un abbonamento di tipo PPPoE è possibile utilizzare il Router in modalità RFC 1483 Bridge con una macchina con Windows2000. Come va configurata ?	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). 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 scegliere 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 è possibile utilizzare il Router in modalità RFC 1483 Bridge con una macchina Linux. Come va configurata ?	Per Linux è necessario installare un software chiamato Roaming's Pinguins. Per dettagli sulla configurazione si rimanda alla documentazione allegata al pacchetto.



## 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 (Computer con lo chassis aperto, monitor CRT, cellulari) ed interferire. Qualora non si ottenesse il risultato sperato controllare il proprio contratto ( <b>vedere la banda minima garantita</b> ) ed eventualmente contattare l'ISP. Se i problemi continuassero, contattare l'assistenza tecnica di Atlantis Land spa.

## Come posso abilitare la funzionalità SPI?

Quesito	Risposta
Voglio accrescere la sicurezza del 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'intera 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). <b>Nota Bene:</b> 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 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 necessita 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 e 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 <b>Always On</b> per mantenere sempre alta la connessione (in PPPoA e PPPoE se tale modalità è abilitata il Router ADSL alzerà nuovamente la connessione se questa dovesse cadere). <b>Consigliamo di non utilizzare l'IDLE Time e mantenere il Router su Always ON</b> a meno che l'abbonamento non sia 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). Fare 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 classe di appartenenza. 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?	<p>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.</p> <p><b>1</b>-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.</p> <p><b>2</b>-Attacchi che mirano all'esaurimento delle risorse.</p> <p><b>3</b>-Attacchi contro difetti di programmazione, che mirano a sfruttare bug software o hardware.</p> <p><b>4</b>-Attacchi DoS generici.</p> <p>Il Router può automaticamente rilevare e bloccare un attacco di tipo DoS (Denial of Service) se questa funzione è attiva.</p>



## 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?	<p>Vi sono 2 possibili alternative:</p> <p>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).</p> <p>Anzitutto è necessario assegnare ai PC che si vogliono limitare degli indirizzi IP fissi e disabilitare così, qualora fosse attivo, il client DHCP (benché è possibile utilizzare la funzionalità Fixed Host, ma è necessario conoscere i vari Mac address). In questo modo, avendo sempre i medesimi indirizzi IP è possibile operare correttamente (si ricorda che invece se fossero client DHCP l'indirizzo IP potrebbe mutare). Le idee da seguire sono le seguenti: Utenti appartenenti al <b>gruppo A</b> saranno filtrati ed Utenti appartenenti al <b>gruppo B</b> avranno invece accesso senza alcuna limitazione a tutti i servizi internet (compatibili con il livello di sicurezza impostato). Per ottenere questo scegliere nel firewall dell'I-Storm il livello di sicurezza opportuno (tutta una serie di regole che consentiranno il passaggio dei servizi ritenuti necessari). Andare poi nella sezione Packet Filter-Address Filter e metteremo gli IP da bloccare. Volendo è possibile mettere un indirizzo IP e la sua subnet bloccare (oppure un indirizzo IP e la sua subnet).</p>



## Cos'è il DDNS?

Quesito	Risposta
A cosa serve il DDNS?	<p>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 (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:</p> <ul style="list-style-type: none"><li>• Registrare il proprio dominio(ad esempio) gratuitamente <a href="http://www.dyndns.org">www.dyndns.org</a>, <a href="http://www.zoneedit.com">www.zoneedit.com</a>. L'operazione richiederà qualche minuto.</li><li>• 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, oltre che ogni volta che riceve dalla sfida PPPoA/PPPoE un nuovo indirizzo IP) nel rispetto delle policy del gestore DDNS.</li><li>• Predisporre il PC che deve fungere da Server Web o configurare il Router affinché sia gestibile da remoto o configurarlo come server VPN.</li><li>• Configurare il Virtual Server affinché rigiri sull'indirizzo IP del PC (di sopra) predisposto le connessioni provenienti dall'esterno</li></ul> <p>In questo modo ogni utente che voglia connettersi all'indirizzo registrato interrogherà il server DDNS che gli restituirà di volta in volta l'indirizzo IP datogli dal Router cui lo ha assegnato l'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).</p>



# 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. E' sufficiente registrarsi per attivare in maniera gratuita ed immediata il servizio che consentirà di raggiungere (da remoto) sempre il Router. E' possibile in questo modo effettuare facilmente configurazioni da remoto, ospitare un 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 conoscerà anche 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](http://www.dyndns.org), cliccare su **Account**.

The screenshot shows the DynDNS.org website interface. The browser window title is "DynDNS.org -- Welcome - Microsoft Internet Explorer". The address bar displays "https://www.dyndns.org/". The website features a navigation menu with "About", "Services", "Account", "Support", "Developers", and "News". The main content area is titled "Welcome" and contains several paragraphs of text. On the right side, there is a "Recent News" section with three news items: "Router Certification Program Announced (May 13, 2003)", "DynDNS.org Pricing/Service Survey Launched (May 08, 2003)", and "DynDNS.org Offers Domain Registration (May 01, 2003)". Below that is a "Stories" section with "Redundancy" and "Open Source" articles. At the bottom, there is an "Applications" section. A login form is visible in the top right corner of the website content area.

Effettuare la registrazione (cliccando su **Create Account**) inserendo: **Username**, **Indirizzo Mail e Password**.



Una mail di verifica registrazione sarà inviata all'indirizzo inserito. In questa mail sono contenute le istruzioni per proseguire la registrazione (è necessario confermare così il tutto entro 48 ore). Seguire le istruzioni contenute e compilare il form per terminare la fase di registrazione.

A questo punto tornare nel sito, andare su **Services**, evidenziare (nella parte sinistra) il menù **Dynamic DNS** e poi cliccare su **Add Host**.

Non resta che introdurre il **Nome dell'host** (evidenziare Enable WildCard) e scegliere il suffisso preferito e premere poi sul bottone **Add Host** per terminare.

Passiamo adesso alla configurazione del client nel Router (nella sezione **DynDNS, Configuration/Advanced**).

I-Storm ADSL Router with Firewall & VPN Built-in

**Dynamic DNS**

Enable  Disable

Dynamic DNS:

Domain Name:

Username:

Password:

Period:  Day(s)

Spuntare il bottone **Enable**.

Alla voce Dynamic DNS scegliere, dalla combo box, **www.dyndns.org(dynamic)**.

Compilare il campo **Domain Name** inserendo per esteso il dominio registrato e inserire poi **Username** e **Password**.

Impostare il campo **Period** su 99 Days (come da figura).

Premere su **Apply** e poi su **Save Config to FLASH** per rendere permanenti le modifiche.

Andando sul sito [www.dyndns.org](http://www.dyndns.org), (effettuare il Login ed andare nella sezione Account poi sotto Dynamic DNS all'URL) è possibile controllare che l'IP sia stato aggiornato (alternativamente è possibile effettuare un ping verso il vostro URL).



## 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 verranno evidenziate le varie modifiche subite da un pacchetto durante il percorso.

Verranno utilizzate le seguenti convenzioni:

- **BLU** per indicare una INVERSIONE
- **ROSSO** per indicare un CAMBIAMENTO

Condizioni di partenza:

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

Il caso da esaminare prevede una LAN in cui il PC con IP 192.168.1.X vuole visualizzare un sito WEB.

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

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

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

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

	Direzione Pacchetto	Router-Internet[Uscente]	
I P	IP Provenienza	<b>IP lato WAN del Router</b>	
	IP Destinazione	IP del Server DNS	
	Pacchetto contenuto	Tipo UDP	U D P
	Porta Provenienza	C	
	Porta Destinazione	53	



Arrivato al server DNS il pacchetto torna indietro, reindirizzato al Router (che 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]	
I P	IP Provenienza	<b>IP del Server DNS</b>	
	IP Destinazione	<b>IP lato WAN del Router</b>	
	Pacchetto contenuto	Tipo UDP	U D P
	Porta Provenienza	<b>53</b>	
	Porta Destinazione	<b>C</b>	

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

	Direzione Pacchetto	Internet-Router[Entrante]	
I P	IP Provenienza	IP del Server DNS	
	IP Destinazione	<b>192.168.1.X</b>	
	Pacchetto contenuto	Tipo UDP	U D P
	Porta Provenienza	53	
	Porta Destinazione	C	

A questo punto, dal pacchetto UDP arrivato, il PC (con IP 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).

	Direzione Pacchetto	PC-Router[Uscente]	
I P	IP Provenienza	192.168.1.X	
	IP Destinazione	IP URL	
	Pacchetto contenuto	Tipo TCP	T C P
	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]	
I P	IP Provenienza	<b>IP lato WAN del Router</b>	
	IP Destinazione	IP URL	
	Pacchetto contenuto	Tipo TCP	T C P
	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]	
I P	IP Provenienza	<b>IP URL</b>	
	IP Destinazione	<b>IP lato WAN del Router</b>	
	Pacchetto contenuto	Tipo TCP	T C P
	Porta Provenienza	<b>80</b>	
	Porta Destinazione	<b>K</b>	

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

	Direzione Pacchetto	Router-PC[Entrante]	
I P	IP Provenienza	IP URL	
	IP Destinazione	<b>192.168.1.X</b>	
	Pacchetto contenuto	Tipo TCP	T C P
	Porta Provenienza	80	
	Porta Destinazione	K	

E' stato evidenziato tanto il percorso dei pacchetti che le trasformazioni che questi subiscono. 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 reinviato al mittente sulla porta su cui questo aspetta la risposta (viene effettuata un'inversione a livello di porte).

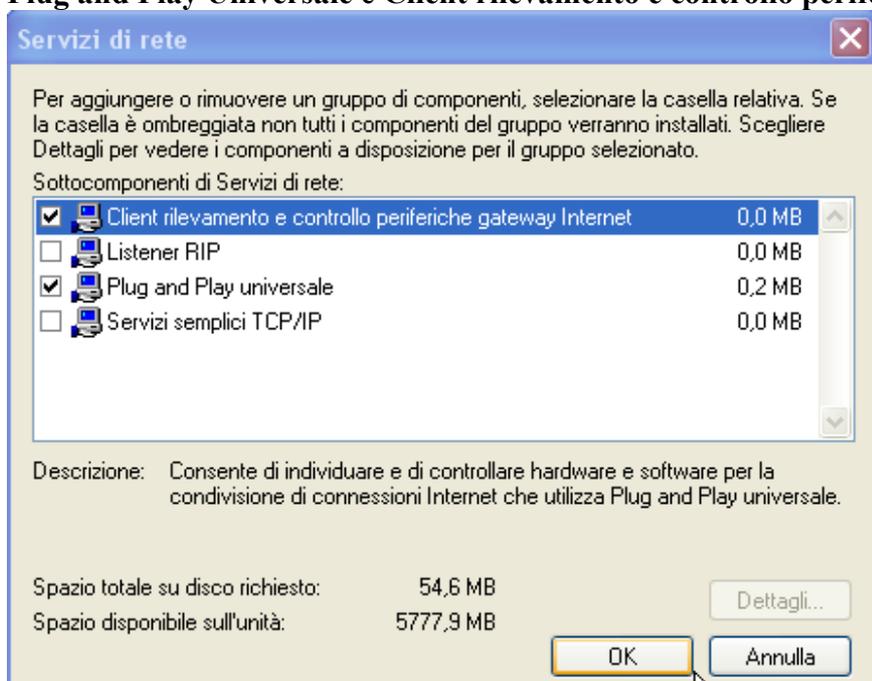
# APPENDICE C

## UPnP

Grazie alla funzionalità UPnP è possibile configurare facilmente tutte quelle applicazioni che hanno problemi nell'attraversamento del NAT. L'utilizzo del NAT Trasversale renderà le applicazioni in grado di configurarsi 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.

Attivazione dell'UPnP in Windows XP.

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

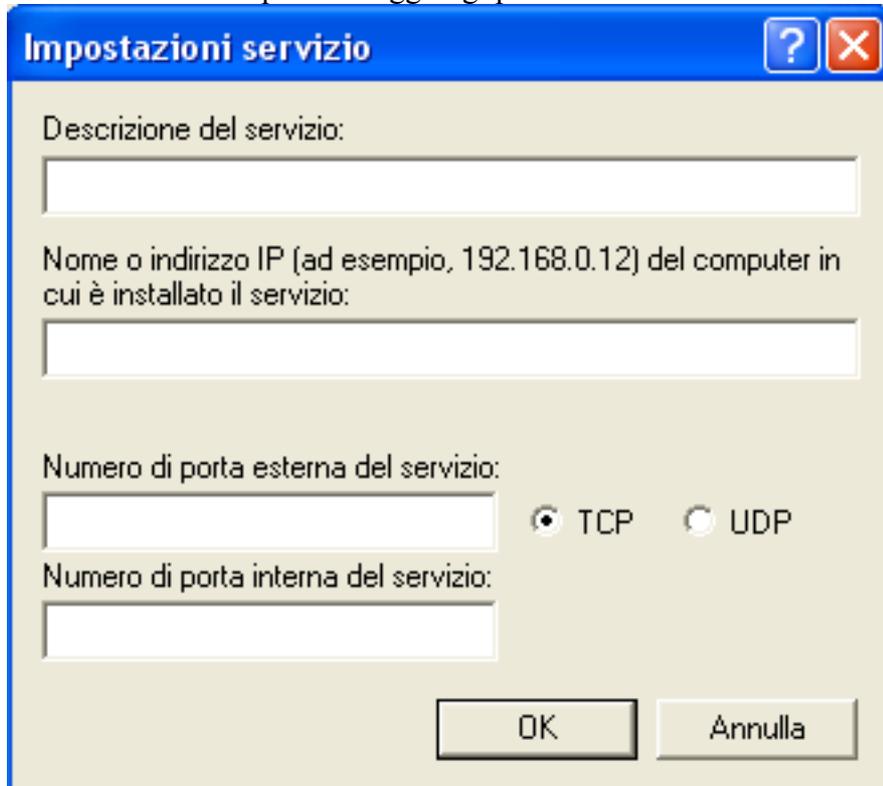


Andando su **Risorse di Rete** è possibile trovare il nome del campo **Set Host Name**. Cliccandoci sopra è possibile entrare nella configurazione del Router ADSL. Cliccando il tasto destro e poi Proprietà è possibile avere accesso ad informazioni supplementari.

Andando su **Pannello di Controllo** e poi **Connessioni di rete** è possibile cliccare sull'icona **Connessione Internet**.



Scegliendo **proprietà** e poi **impostazioni** è possibile impostare le configurazioni necessarie all'uso dell'UPnP. 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** è possibile 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 è possibile configurare una sorta di **Virtual Server** da ogni PC senza accedere al Router vero e proprio.

Alcune applicazioni sono in grado di configurare in maniera autonoma il servizio UPnP.



E' necessario configurare l'I-Storm Lan Router ADSL affinché utilizzi una porta superiore a 1024 (Windows XP altrimenti non funzionerebbe correttamente) per l'UPnP.

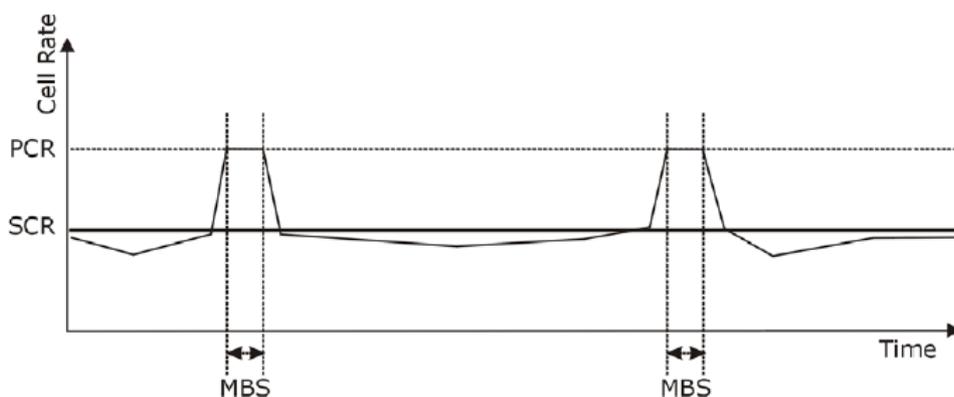
## Traffic Shaping

Il "Traffic Shaping" è una sorta di accordo tra il Provider e l'utente per regolare la percentuale media e il "burstiness" o la fluttuazione di trasmissione di dati su una rete ATM. Questo accordo aiuta ad eliminare la congestione sulla rete, fattore importante per la trasmissione di dati in tempo reale come audio e collegamenti video.

Il Peak Cell Rate (PCR) è la massima velocità alla quale il mittente può spedire celle. Questo parametro può essere più basso (ma non alto) della velocità di linea massima. 1 cella ATM è composta da 53 bytes (424 bits), quindi una velocità massima di 832 Kbps ha un PCR massimo di 1962 cells/sec. Questo parametro non è garantito perché è dipendente dalla velocità della linea.

Il Sustained Cell Rate (SCR) è il throughput medio garantito. L' SCR non può essere più grande del PCR; il parametro di default è 0 cells/sec.

Il Maximum Burst Size (MBS) è il numero di massimo di celle che possono essere spedite al PCR. Dopo che l'MBS è stato raggiunto, il numero di celle inviate precipita di nuovo sotto l'SCR fino a che la media di celle inviate non raggiunge nuovamente il valore di SCR. A questo punto, più celle possono essere inviate nuovamente (fino all' MBS) al PCR. La figura seguente illustra la relazione tra PCR, SCR e MBS.





## Caratteristiche Tecniche

Protocolli	IP, NAT, PPTP, ARP, ICMP, DHCP(server, relay e client), PPTP client, RIP1/2, SNMP, SNTTP client, UPnP, Telnet server
Porta LAN	RJ-45, 4 porte 10/100Base-T con autonegoziazione e autopolarità
Porta WAN	RJ-11 (1 porta ADSL/ADSL2)
Porta Console	RS232 DB9(9600,8,Nessuno,1,Nessuno)
Tasti	Reset, Bottone accensione/spegnimento
LED Indicatori	Power, System, Lan (4), MAIL/PPP ed ADSL
Standard ADSL Compliance	ANSI T1.413 Issue 2, ITU-T G.992.1(Full Rate DMT), ITU-T G.992.2 (Lite DMT), ITU-T G.994.1 (Multimode)
Standard ADSL2 Compliance	ITU G.992.3 (G.dmt.bis) (12Mbps download, 1Mbps upload)*
Protocolli ADSL	RFC2364(PPPoA), RFC2516(PPPoE), RFC1577 e RFC1483
ATM	ATM AAL2/AAL5 and ATM service class : CBR, UBR, VBR-rt, VBR, ATM Forum UNI 3.0, 3.1 and 4.0
Firewall	Intrusion Detection, DoS, Port Filters, URL blocking, MAC blocking
QoS	Quality of Service and IP Throttling
VPN	1 VPN IPsec
Alimentatore(esterno)	12V DC @ 1A
Potenza assorbita	< 10watts
Conformità con	CE
Dimensioni Fisiche	180 x 120 x 32 mm <sup>3</sup> (L x P x A)
Peso	500g
Temperatura Operativa	Da 0°C a 40°C
Temperatura supportata (non in funzionamento)	Da -10°C a 70°C
Umidità Operativa	5-95% senza condensazione

\* Firmware upgradeable to ADSL2



## Supporto Offerto

Per ogni problema con l'I-Storm Lan Router ADSL consultare questo manuale. Molti problemi potrebbero essere risolti cercando la soluzione del problema nel Capitolo 4.

Per qualunque altro problema o dubbio (prima è necessario conoscere tutti i parametri usati dall'ISP) potete contattare l'help desk telefonico (**02/93907634**) gratuito di Atlantis Land che fornirà assistenza da lunedì a venerdì dalle 9:00 alle 13:00 e dalle 14:00 alle 18:00. E' possibile anche utilizzare il fax (02/93906161) la posta elettronica ([info@atlantis-land.com](mailto:info@atlantis-land.com) oppure [tecnici@atlantis-land.com](mailto:tecnici@atlantis-land.com)).

**AtlantisLand spa**

**Viale De Gasperi 122**

**20017 Mazzo di Rho(MI)**

**Tel: 02/93906085 (centralino), 02/93907634(help desk)**

**Fax: 02/93906161**

**Email: [info@atlantis-land.com](mailto:info@atlantis-land.com) oppure [tecnici@atlantis-land.com](mailto:tecnici@atlantis-land.com) (mettere nell'oggetto il prodotto su cui si chiede assistenza)**

**WWW: <http://www.atlantisland.it> o [www.atlantis-land.com](http://www.atlantis-land.com)**