# FIREGATE WAVE 54


Manuale Operativo
rev. 1.0 del 06/2004

digicom
http://www.digicom.it

# INDICE

# PREMESSA

*E' vietata la riproduzione di qualsiasi parte di questo manuale, in qualsiasi forma, senza esplicito permesso scritto della Digicom S.p.A. Il contenuto di questo manuale può essere modificato senza preavviso.*
*Ogni cura é stata posta nella raccolta e nella verifica della documentazione contenuta in questo manuale, tuttavia la Digicom non può assumersi alcuna responsabilità derivante dall'utilizzo della stessa.*

Al fine di salvaguardare la sicurezza, l'incolumità dell'operatore ed il funzionamento dell'apparato, devono essere rispettate le seguenti norme installative:

## CONDIZIONI AMBIENTALI

| Temperatura ambiente | Umidità relativa |
|---|---|
| da -5 a +45 °C | dal 20 a 80% n.c. |

Si dovrà evitare ogni cambiamento rapido di temperatura e umidità

- Polvere, umidità, calore elevato ed esposizione diretta alla luce del sole.
- Oggetti che irradiano calore. Questi potrebbero causare danni al contenitore o altri problemi.
- Oggetti che producono un forte campo elettromagnetico (altoparlanti Hi-Fi, ecc.)
- Liquidi o sostanze chimiche corrosive.

## AVVERTENZE GENERALI

Per tutti gli apparati alimentati direttamente da rete:
Classe di isolamento: solo quella indicata sull'etichetta dell'apparato
Correnti nominali: solo quelle indicate sull'etichetta dell'apparato

Per evitare scosse elettriche, non aprite l'apparecchio o il trasformatore. Rivolgetevi solo a personale qualificato. Scollegate il cavo di alimentazione dalla presa a muro quando non intendete usare l'apparecchio per un lungo periodo di tempo.
Per scollegare il cavo tiratelo afferrandolo per la spina. Non tirate mai il cavo stesso.
In caso di penetrazione di oggetti o liquidi all'interno dell'apparecchio, scollegate il cavo di alimentazione e fate controllare da personale qualificato prima di utilizzarlo nuovamente.

## PULIZIA DELL'APPARATO

Usare un panno soffice asciutto senza l'ausilio di solventi.

## VIBRAZIONI O URTI

Attenzione a non causare vibrazioni o urti.

# DICHIARAZIONE CE DI CONFORMITA'

Noi, Digicom S.p.A. via Volta 39 - 21010 Cardano al Campo (Varese - Italy) dichiariamo sotto la nostra esclusiva responsabilità, che i prodotti, Nome: **FireGATE Wave 54** al quale questa dichiarazione si riferisce, soddisfa i requisiti essenziali della sotto indicata Direttiva:

- 1999/5/CE del 9 marzo 1999, R&TTE, ( riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento della loro conformità). Come designato in conformità alle richieste dei seguenti Standard di Riferimento o ad altri documenti normativi:
  EN 300 328-2
  EN 301 489-1
  EN 301 489-17
  EN 60950

# 1. INTRODUZIONE

1

**Gentile Cliente,**
**la ringraziamo per la fiducia accordataci nell'acquistare un prodotto Digicom.**

Con FireGate Wave 54 le sarà possibile fornire accesso sicuro ad Internet a tutta la sua LAN cablata e a tutti i client Wireless.
Fino a 253 stazioni della sue rete locale LAN o WLAN avranno la possibilità di accedere ad Internet per la navigazione (WWW, HTTP) o l'accesso alla posta elettronica (e-mail) utilizzando un modem* ADSL, xDSL o Cable Modem ed un abbonamento per singolo utente.
La sua LAN sarà inoltre protetta dai più comuni attacchi di hacker che potenzialmente possono provenire da Internet (Denial Of Service). FireGate Wave 54 supporta trasparentemente i protocolli L2TP, PPTP e IPSEC per il VPN passthrough.
Tutte le operazioni di linea saranno gestite in modo completamente automatico e trasparente da FireGate Wave 54, senza
intervento alcuno da parte degli utilizzatori della rete.
Potrà inoltre sfruttare le funzionalità avanzate di FireGate Wave 54 per gestire in modo efficiente l'accesso ad Internet dei suoi computer, realizzando esportazioni di servizi, gruppi di utenti a cui permettere/negare l'accesso, bloccare protocolli o applicazioni e molto altro.
Grazie alle funzionalità di roaming potrà utilizzare più access point Wireless per creare una rete WLAN omogenea dove i client potranno muoversi liberamente senza mai dover modificare alcuna impostazione.
In questo manuale troverà tutte le informazioni necessarie per collegare FireGate Wave 54 alla rete di computer e configurare opportunamente l'insieme in pochi minuti.
Per una configurazione più estesa e completa del prodotto viene fornito un manuale On-line disponibile su CDROM e consultabile da browser o Acrobat® Reader™.
Per comodità, per indicare il modem connesso alla porta WAN, questo verrà convenzionalmente chiamato "Modem xDSL", indipendentemente dalla sua tipologia (ADSL, HDSL, SDSL, Cable o altra tecnologia similare).

## 1.1. WIRELESS LAN

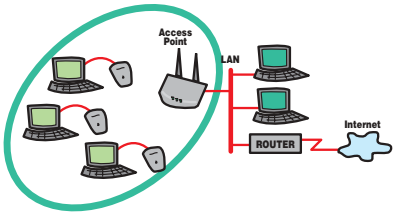
Una Wireless LAN è una rete di computer, comparabile ad una rete cellulare, che utilizza i segnali radio per far comunicare i computer tra loro, invece di veri e propri cavi.
La Wireless LAN può essere utilizzata sia in ufficio sia in casa e rende il lavoro più semplice grazie alla vera mobilità del computer che non è più "legato" ad un cavo di rete che ne limita di fatto l'ubicazione.
Gli utenti di una Wireless LAN possono utilizzare ed accedere alle stesse risorse a cui hanno accesso sulla normale rete Ethernet cablata. Le schede di rete o adattatori Wireless per computer portatili o desktop supportano gli stessi protocolli delle schede di rete Ethernet..
Generalmente un utente "Wireless" non nota alcuna differenza sostanziale nell'utilizzo della WLAN in confronto alla rete cablata, a parte il vantaggio di essere veramente "mobile".
In molte circostanze è necessario poter accedere a risorse come server, stampanti o accessi Internet raggiungibili sulla rete cablata. L'Access Point Wireless sarà il punto di accesso a tutte queste risorse per i computer Wireless.

L'utilizzo della tecnologia Wireless LAN porta molti vantaggi, tra cui la mobilità ed il basso costo di realizzazione (comparato ai costi di un cablaggio strutturato). Una rete WLAN mette a disposizione le informazioni in qualsiasi locazione coperta dal segnale. Una rete WLAN può essere gestita, modificata e rilocata in modo molto semplice e veloce.
L'interoperabilità con altri sistemi basati sulla tecnologia IEEE 802.11b e IEEE 802.11g permette di integrare ed espandere le possibilità di utilizzo in modo semplice ed efficace.

### 1.1.1. TIPOLOGIE DI RETI WIRELESS

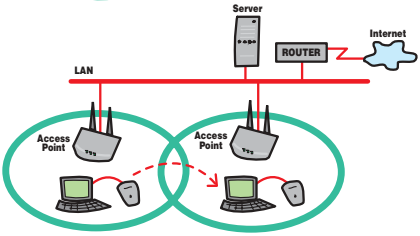
**Infrastructure**

Tipologia di rete Wireless a stella che prevede la presenza di un Access Point.
In questa modalità l'Access Point rappresenta l'equivalente di un hub o switch di rete, concentra le connessioni di una serie di client e permette la comunicazione tra essi. L'A.P. può anche svolgere le funzioni di gateway verso la LAN cablata.




**Infrastructure con Roaming**

WaveGate11 C supporta il Roaming 802.11 che permette alla stazione Wireless di muoversi all'interno di una area coperta da più Access Point, passando da un A.P. all'altro senza mai perdere la connessione con la rete Wireless.




## 1.2. CARATTERISTICHE

**LAN**

- Switch 10/100 BaseT integrato
  Fino a 4 stazioni di rete possono essere collegati direttamente al dispositivo. La velocità e modalità di funzionamento della LAN viene riconosciuta ed impostata automaticamente.
- Supporto DHCP Server
  Un server DHCP (Dynamic Host Configuration Protocol) interno è in grado di assegnare gli indirizzi IP ai computer della rete che ne fanno richiesta.
- Supporto RIP e Tabelle di Routing statiche
  E' supportato il protocollo RIP ed è possibile configurare le tabelle di routing statiche per interagire con altri router connessi in LAN.

**WLAN**

- Access Point Wireless IEEE 802.11g & IEEE 802.11b
- Velocità Supportate:
  - 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
  - 802.11b: 11, 5.5, 2, 1Mbps
- WEP: 64, 128 bit
- MAC Filtering
- Possibilità di restringere l'accesso solo alla LAN o solo alla WAN

**WAN**

- Porta WAN 10/100BaseT
  A questa porta è possibile connettere il Modem xDSL.
- Supporto protocollo PPPoE e PPTP
  FireGate Wave 54 è in grado di generare una chiamata automatica verso il provider Internet (se necessario), utilizzando il protocollo PPP over Ethernet integrato e supportare il protocollo PPTP.
- Connessione diretta al provider Internet
  FireGate Wave 54 può effettuare una "connessione diretta", senza protocollo PPPoE, se il provider Internet richiede questo tipo di funzionamento o se si collega il dispositivo ad un router intermedio.

### Accesso ad Internet

- Accesso condiviso ad Internet
  Tutti i PC connessi alla LAN oppure alla WLAN (se opportunamente configurati) potranno accedere in modo sicuro ad Internet, contemporaneamente ed in modo trasparente.
- Abbonamento per singolo utente
  Grazie alle funzionalità di NAT, tramite un abbonamento Internet per singolo utente tutti i PC potranno navigare contemporaneamente.

### Restrizioni accesso WLAN

- Accesso controllato alla LAN
  Se necessario è possibile abilitare l'accesso alla LAN solamente ai client Wireless abilitati.
- Accesso controllato alla WAN
  Se necessario è possibile abilitare l'accesso alla WAN (Internet) solamente ai client Wireless abilitati.

### Funzioni Internet Avanzate

- Virtual Servers.
  Permette a utenti Internet di accedere a computer presenti sulla propria LAN
- User-Defined Virtual Servers.
  Permette a utenti Internet di accedere a servizi speciali messi a disposizione sulla propria LAN.
- Special Internet Applications.
  Permette di utilizzare applicazioni Internet speciali come Internet Videoconferencing*, Telephony, Games Servers ecc.
- Multi-DMZ.
  E' possibile rendere direttamente visibili (esporre) da Internet tutti i servizi offerti da una o più macchine, senza applicare alcuna restrizione.
  Il numero di macchine che possono utilizzare questo servizio (max 7) è in relazione al numero di Indirizzi IP pubblici a disposizione (per abbonamenti multi utente).

### Configurazione e Monitor

- Configurazione semplice ed immediata attraverso un comune browser (Explorer, Netscape, ecc.) I Gestione e monitoraggio da una qualsiasi stazione di LAN locale o remota
- Supporto protocollo UpnP (Universal Plug and Play) per Windows XP, 2000 e Me.

### Sicurezza e protezione dei dati

- Accesso alla configurazione protetto da password
- Access List. Creazione di gruppi di utenti ai quali restringere o negare l'utilizzo di Internet con log visualizzabiile. Filtro su URL in uscita.
- Tutti i pacchetti di dati provenienti dal link WAN vengono controllati e verificati. Tutte le richieste di accesso a stazioni presenti in LAN sono automaticamente filtrate e bloccate.
- Ogni accesso non autorizzato proveniente da Internet è bloccato proteggendo la sicurezza dei dati presenti in LAN. Protezione automatica da attacchi di tipo Denial of Service.
- Supporto VPN Passthrough per i protocolli L2TP, PPTP e IPSEC.
- Log delle operazioni ed eventi diretto, via e-mail o syslog

### Prerequisiti

- Computer con schede di rete Ethernet 10/100 Megabit/s, connettori UTP
- Driver software per le schede di rete installati su ogni computer
- Cavi di rete diritti, connettori RJ45 su entrambe le estremità
- Modem xDSL per l'accesso ad Internet dotato di porta LAN 10Mbit/s e connettore UTP RJ45
- Abbonamento Internet per singolo utente stipulato con un ISP (Internet Service Provider)

**Contenuto della confezione**

- 1 FireGate Wave 54
- 1 Alimentatore
- 1 CD-ROM contenente il Manuale
- 1 Manuale di configurazione rapida

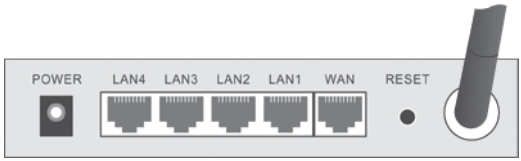
## 1.2. DESCRIZIONE PORTE, LED E DIP SWITCH


*Fig. 1.1. Vista dei Led*

### 1.2.1. DESCRIZIONE DEI LED

| | |
|---|---|
| **Power** | Acceso – Dispositivo Acceso<br>Spento – Dispositivo Spento |
| **Status (Rosso)** | Acceso – Condizione di errore<br>Spento – Stato normale<br>Lampeggiante - Durante il selftest di accensione |
| **LAN** | 2 led per ogni porta<br>● Link/Act<br>● Acceso – Porta LAN attiva<br>● Spento – Porta Lan non attiva<br>● Lampeggiante - Attività dati sulla porta<br>● 100<br>● Acceso - La porta sta operando a 100Mbit/s<br>● Spento - La porta sta operando a 10Mbit/s (se Link/Act acceso) |
| **WAN** | Acceso - connessione con il modem xDSL sulla porta WAN stabilita e attiva<br>Lampeggiante - Attività dati sulla porta WAN |
| **WIRELESS** | Acceso – Access Point Wireless attivo<br>Spento – Access Point Wireless disattivato<br>Lampeggiante – Attività sulla rete WLAN |

### 1.2.2. POSTERIORE




**Reset** Pulsante di Reset. Ha due funzioni:
- Reboot. Premendo e rilasciando il pulsante si effettua un riavvio del dispositivo.
- Reset di tutte le impostazioni. Per riportare tutte le impostazioni al default di fabbrica:

1. Spegnere il dispositivo.
2. Tenere premuto il pulsante e riaccendere il dispositivo.
3. Mantenere il pulsante premuto per circa 10 secondi o finche il led di status sarà acceso per 2 volte.
4. Rilasciare il pulsante. Il dispositivo è ora tornato alle impostazioni di fabbrica.

**WAN (10/100BaseT)** Porta per la connessione del modem xDSL. Usare il cavo fornito con il modem o un normale cavo di LAN.

**LAN1-4 (10/100BaseT)** Porte LAN. Usare normali cavi LAN (CAT5 per 100Mbit/s). tutte le porte sono in grado di trasformarsi in porte di "Uplink (MDI)" in modo automatico.
Quando rilasciato, la porta LAN1 è una normale porta dello switch (MDI).

**Power** Ingresso per il cavo proveniente dall'alimentatore. Utilizzare unicamente l'alimentatore fornito nella confezione. L'utilizzo di alimentatori diversi può comportare il danneggiamento del dispositivo con conseguente invalidazione delle condizioni di garanzia.

# 2. CONFIGURAZIONE

2

## 2.1. DESCRIZIONE

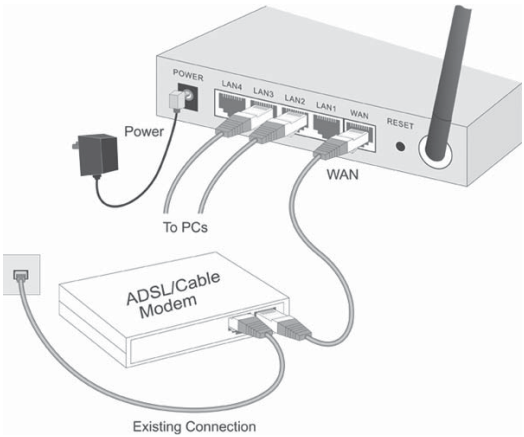
La configurazione dell'intero sistema comprende:
- Installazione e cablaggi
- Configurazione FireGate Wave 54
- Configurazione stazioni di rete

## 2.2. INSTALLAZIONE E CABLAGGI

1. **Scelta della locazione di installazione**
   Scegliete una locazione che sia vicina:
- al modem o router xDSL.
- Alla presa di alimentazione 220V.
- Ad un hub o presa di rete 10BaseT o 100BaseT.
- in una posizione centrale rispetto alla rete Wireless che volete creare.

2. **Connessione del router alla rete LAN**
   Utilizzate un normale cavo LAN RJ45-RJ45.
   Collegate un'estremità del cavo alla porta LAN1 presente sul posteriore del dispositivo.
   Collegate l'altra estremità del cavo ad una porta di un Hub/Switch o alla presa di rete LAN.
   Il router rileverà e imposterà la velocità di funzionamento 10/100 e la modalità half/full duplex in modo automatico.
   Se preferite potete collegare il dispositivo direttamente ad un PC.

***Nota! Per la configurazione del dispositivo si consiglia du utilizzare una normale connessione di rete Ethernet e di passare successivamente ad utilizzare anche la rete WLAN.***




3. **Connessione del router al modem xDSL**
   Utilizzate il cavo RJ45-RJ45 fornito con il modem oppure un normale cavo di LAN.
   Collegate un'estremità del cavo alla porta Ethernet del modem xDSL.
   Collegate l'altra estremità del cavo alla porta WAN di FireGate Wave 54.

4. **Accensione del router**
   Collegate il cavetto di alimentazione alla presa Power.
   Inserite l'alimentatore fornito nella confezione nella presa di alimentazione 220V.
   Non utilizzate alimentatori diversi da quello fornito nella confezione, pena il possibile danneggiamento del dispositivo e conseguente invalidazione delle condizioni di garanzia.
5. **Verifica stato led**
   Una volta acceso il dispositivo, i led WAN, WIRELESS e LAN (solo per le porte collegate) devono essere accesi.

***Nota: La lunghezza di ogni cavo deve essere inferiore a 100mt. Se la rete LAN opera a 100Mbit/s é necessario l'uso di cavi di rete in categoria 5.***

## 2.3. LA CONFIGURAZIONE

FireGate Wave 54 supporta il servizio HTTP server permettendovi di accedere alla sua configurazione tramite un comune browser (tipo Explorer o Netscape) che supporti tabelle e form HTML. Il vostro browser deve supportare i Javascript (Netscape 4.08 o superiore, Internet Explorer 4 o superiore).

In alternativa potete utilizzare il protocollo UpnP se il vostro sistema operativo lo supporta.

### 2.3.1. PREPARAZIONE DEL COMPUTER

Per accedere alla configurazione di FireGate Wave 54 è indispensabile che il vostro computer utilizzi il protocollo TCP/IP dopodichè il metodo più semplice è quello di utilizzare il servizio di DHCP server di FireGate Wave 54; l'alternativa è quella di modificare manualmente l'indirizzo IP del vostro computer.
Di seguito sono riportate le indicazioni per entrambe le modalità.

#### IMPOSTAZIONE COME CLIENT DHCP

**Windows® XP**

1. Dal menù Start selezionate -> **Pannello di Controllo -> Rete e Connessioni Internet , Risorse di rete** e selezionate **Visualizza risorse di rete**.
2. Selezionate **Connessione alla rete locale (LAN)** e visualizzate le **Proprietà**, selezionate **Protocollo Internet (TCP/ IP)** e premete sul pulsante **Proprietà**.
3. Per impostare il Computer come client DHCP dovete selezionare **Ottieni automaticamente un Indirizzo IP**, a questo punto potete chiudere le finestre confermando con **OK**.
4. Riavviate Windows® per rendere attive le nuove impostazioni.

**Macintosh®**

1. Dal menu Mela selezionate **Pannello di Controllo (Control Panels) e TCP/IP**.
   Potete utilizzare il menu **File:Configurazioni:Esporta** per salvare le impostazioni attuali e richiamarle successivamente (Importa).
2. Selezionate **Ethernet** nella sezione **Connetti via e Usa DCHP Server** in **Configura**.
3. Chiudete la finestra **TCP/IP** e salvate.
4. Riavviate il Mac per rendere attive le impostazioni ed ottenere un indirizzo IP da Michelangelo OFFICE.
5. Dopo il riavvio potete verificare l'indirizzo assegnato al Mac da Pannello di controllo:**TCP/IP:File:Get Info**.

**Linux**

Di seguito verranno date alcune informazioni su come configurare le risorse di rete utilizzando il Centro di Controllo KDE, con la distribuzione Suse 6.2.

1. Attivate il Control Center.
2. Selezionate **Configurare la scheda di rete** nel menù **Network Basic**.
3. Selezionate Assegnazione automatica degli indirizzi (via DHCP) .
4. Confermate con **Termina**.

### INDIRIZZI IP STATICI

#### Windows® XP

1. Dal menù Start selezionate -> **Pannello di Controllo -> Rete e Connessioni Internet , Risorse di rete** e selezionate **Visualizza risorse di rete**.
2. Selezionate **Connessione alla rete locale (LAN)** e visualizzate le **Proprietà**, selezionate **Protocollo Internet (TCP/ IP)** e premete sul pulsante **Proprietà**.
3. Per impostare un indirizzo IP dovete selezionare **Utilizza il seguente indirizzo IP**: ed inserite Indirizzo IP 192.168.0.2, la Subnet mask 255.255.255.0 ed il Gateway 192.168.0.1. Confermate con **OK** le nuove impostazioni.
4. Riavviate Windows® per rendere attive le nuove impostazioni.

#### Macintosh®

1. Dal menu Mela selezionate **Pannello di Controllo** (Control Panels) e **TCP/IP**.
2. Potete utilizzare il menu **File:Configurazioni:Esporta** per salvare le impostazioni attuali e richiamarle successivamente (Importa).
3. Selezionate **Ethernet** nella sezione **Connetti via** e **Manuale** (Manually) in b.
4. Inserite Indirizzo IP 192.168.0.2, la Subnet mask 255.255.255.0 ed il Gateway 192.168.0.1.
5. Chiudete la finestra TCP/IP e salvate.
6. Riavviate il Mac per rendere attive le impostazioni.

#### Linux

Di seguito verranno date alcune informazioni su come configurare le risorse di rete utilizzando il Centro di Controllo KDE, con la distribuzione Suse 6.2.

1. Attivate il Control Center.
2. Selezionate **Configurare la scheda di rete** nel menù **Network Basic**.
3. Selezionate Impostazione degli indirizzi statici, ed inserite Indirizzo IP 192.168.0.2, la Subnet mask 255.255.255.0.
4. Per impostare il gateway, cliccate su Routing e inserite l'indirizzo 192.168.0.1 nel campo Gateway predefinito.

## 2.4. CENNI PRELIMINARI PER LA CONFIGURAZIONE

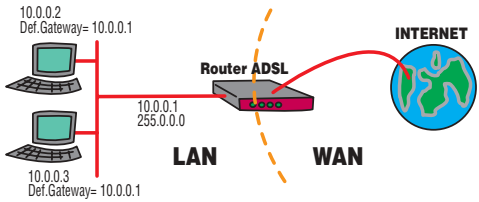
### CONFIGURAZIONE FIREWALL

Questa sezione descrive gli scenari della vostra rete LAN, prima e dopo l'inserimento del Firewall, fornendovi le indicazioni principali necessarie alla corretta impostazione dell'intero sistema.

***Nota: Nel nostro esempio assumiamo che gli indirizzi IP siano stati configurati in modalità fissa e non tramite DHCP (Indirizzi assegnati automaticamente, solitamente dal router ADSL). La descrizione generale è comunque valida. Fate riferimento alle sezioni DHCP e DNS per le descrizioni specifiche.***

### PRIMA

Ipotizziamo la tipica situazione di una rete LAN che accede ad Internet tramite un router ADSL. Tutto il sistema è già installato, configurato e funzionante.



### Gli indirizzi IP e la Subnet Mask

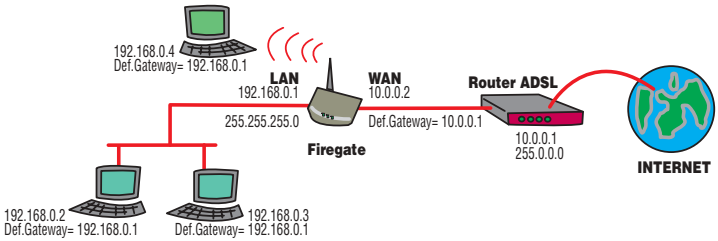
Nell'esempio illustrato, tutti i computer della rete LAN hanno un indirizzo IP appartenente alla stessa classe 10.0.0.x con Subnet Mask 255.0.0.0.
Affinchè i computer possano comunicare tra di loro tramite il protocollo TCP/IP, gli indirizzi e Subnet Mask assegnati alle stazioni di rete devono necessariamente appartenere alla stessa classe.
In questo contesto anche il Router ADSL fa parte della rete LAN e pertanto ha anch'esso un indirizzo appropriato.

### Il Default Gateway

Il **Router ADSL** svolge la funzione fondamentale di fornire l'accesso ad Internet a tutti i componenti della rete LAN, pertanto ne è la "porta di uscita" verso il mondo esterno, in altre parole, il **Gateway** della rete.
Per questo motivo, tutti i computer che debbano poter accedere ad Internet dovranno avere **l'indirizzo IP del Router ADSL** impostato nel campo **Default Gateway** (o Gateway) delle impostazioni di rete TCP/IP.

## DOPO

La caratteristica principale del Firewall è quella di interporre una "barriera" a protezione della rete locale, tra la LAN (Local Area Network) ed il mondo esterno, convenzionalemte chiamato "WAN" (Wide Area Network).
Il Firewall considera i due network LAN e WAN come due reti separate e distinte aventi indirizzi diversi.
Per questo motivo, inserendo il Firewall nella nostra rete sarà necessario modificare gli indirizzi IP della parte LAN come di seguito descritto (1).




### Gli indirizzi IP di LAN

Nell'esempio illustrato, tutti i computer della rete LAN dovranno modificare le proprie impostazioni per "passare" alla nuova classe di indirizzi 192.168.0.x e Subnet Mask 255.255.255.0.

### Il Default Gateway

Il **Firewall** svolgerà ora la funzione di punto di accesso verso il mondo esterno e pertanto diventerà il nuovo **Gateway** della rete.
Per questo motivo, tutti i computer che debbano poter accedere ad Internet dovranno avere l'indirizzo IP del Firewall impostato nel campo **Default Gateway** (o Gateway) delle impostazioni di rete TCP/IP.

Resta ora da configurare il "**lato WAN" del Firewall** per farlo comunicare con il Router ADSL.
Lasciando invariata la configurazione del router ADSL, l'impostazione della porta WAN del Firewall andrà a "sostituire" quella che era l'impostazione di una stazione di rete LAN, prima dell'inserimento del Firewall stesso.
Essendo 10.0.0.1 l'indirizzo IP del Router ADSL assegneremo alla porta WAN del Firewall un indirizzo IP appartenente alla stessa classe, ad esempio 10.0.0.2 e Subnet mask 255.0.0.0.

Dovremo anche specificare un indirizzo per il **Default Gateway** della porta **WAN**. In questo caso sarà ancora l'indirizzo IP 10.0.0.1 del Router ADSL che è di fatto il Gateway di accesso ad Internet per il Firewall.

A questo punto le stazioni della rete rete LAN saranno in grado di navigare in Internet in virtù del fatto che, di default, il Firewall non limiterà alcun accesso dalla LAN verso l'esterno mentre qualsiasi tentativo di intrusione, proveniente dall'esterno ed indirizzato verso la LAN del Firewall, verrà automaticamente impedito e bloccato.

### DNS

Una volta che una stazione di rete ha la possibilità di accedere ad Internet, un'altra impostazione fondamentale è quella relativa ai DNS (Domain Name Server). In una rete TCP/IP il servizio DNS svolge la funzione di **tradurre gli URL** (ad esempio www.digicom.it) nei corrispondenti **indirizzi IP globali** (ad esempio 195.103.9.66).
Se le impostazioni DNS sono assenti o incorrette, di fatto le stazioni di rete non possono navigare in Internet.
Tutte le stazioni di rete dovranno avere **almeno un indirizzo IP configurato nel campo DNS** delle impostazioni di rete TCP/IP. Questo indirizzo è solitamente fornito dal provider Internet.
Nota: Se il router ADSL supporta la funzione di **DNS Autodiscovery/Proxy**, l'impostazione del server DNS sulle stazioni di LAN può essere l'indirizzo IP del router ADSL stesso (10.0.0.1 nel nostro esempio); sarà il router ad occuparsi di svolgere il servizio di risoluzione dei nomi DNS per la rete LAN.

### DHCP

La descrizione fin qui fornita fa riferimento alle impostazioni degli indirizzi in modo "fisso" o statico.
E' possibile che una rete LAN si avvalga del servizio DHCP (Domain Host Control Protocol) per la configurazione automatica degli indirizzi. Questo servizio è svolto da un **DHCP server**, solitamente attivato sul Router ADSL, ed ha il compito di assegnare in modo automatico gli indirizzi IP, Subnet Mask, Default Gateway e DNS alle stazioni di LAN che ne fanno esplicita richiesta.

Una stazione di rete Microsoft Windows opera in **modalità DHCP** quando nelle impostazioni del protocollo TCP/IP della scheda di rete ha selezionato la voce "Ottieni automaticamente un indirizzo IP"; opera invece in modalità **fissa o statica** quando ha selezionato la voce "Utilizza il seguente indirizzo IP". La stessa cosa vale per le impostazioni dei server DNS.
Detto ciò, se la nostra rete LAN utilizzava il **servizio DHCP prima dell'inserimento del Firewall**, affinchè si possano lasciare invariate le impostazioni delle stazioni di LAN sarà necessario attivare il servizio DHCP anche nel Firewall. Si dovranno configurare un numero sufficientemente grande di indirizzi disponibili ma anche gli indirizzi dei server DNS da utilizzare in modo che, quando le stazioni di LAN ne faranno richiesta, il Firewall possa soddisfare tali richieste assegnando tutti i parametri necessari alla navigazione.

(1) Se avete libero accesso alla configurazione del Router ADSL ed avete ben compreso la descrizione della sezione "DOPO", potete anche optare per l'alternativa di lasciare invariata la configurazione dell'intera LAN ma modificare opportunamente l'indirizzo IP del Router ADSL.

## 2.5. ACCESSO ALLA CONFIGURAZIONE

### Configurazione via Browser

1. Avviate il vostro Browser (Explorer, Netscape, ecc.)
2. Nel campo Indirizzo URL inserite "HTTP://" e l'indirizzo IP (usando l'indirizzo impostato di fabbrica: HTTP://192.168.0.1)

Se non vedete apparire la schermata iniziale verificate che:

- Il dispositivo sia acceso ed il cavo di LAN è correttamente collegato.
- Il dispositivo ed il computer dal quale state tentando di accedere alla configurazione si trovino sullo stesso segmento di rete
- Nessun altro computer o dispositivo di rete stia utilizzando l'indirizzo 192.168.0.1. Se così fosse, scollegate la stazione dalla rete e modificatene l'indirizzo IP prima di ricollegarla alla rete oppure spegnetela finchè non avrete assegnato un diverso indirizzo IP Il dispositivo.
- Il vostro computer abbia un indirizzo IP compatibile. Per verificare quale sia l'indirizzo IP attualmente utilizzato dal vostro computer, dalla barra di Avvio di Windows® selezionate Esegui, inserite winipcfg (Win98) o ipconfig (WinMe/2000/XP) e cliccate OK.
  Verificate che sia selezionata la vostra scheda di rete. Verificate che l'indirizzo IP sia compreso tra 192.168.0.2 e 192.168.0.254 e il Subnet Mask sia uguale a 255.255.255.0

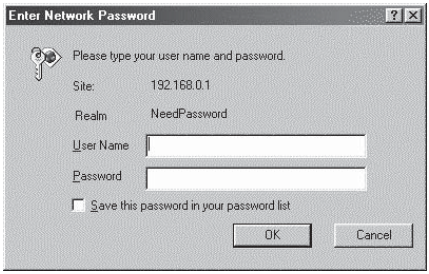
- Il vostro browser non sia configurato per utilizzare un Proxy server.
  Se utilizzate Internet Explorer verificate il menu Visualizza -> Opzioni -> Connessione.
  Se utilizzate Netscape verificate Opzioni -> Preferenze di rete -> Proxy.

### Configurazione via UPnP

Se il vostro sistema operativo supporta UPnP, una icona per il vostro Router apparirà nel system tray notificandovi che un nuovo dispositivo di rete è stato trovato e proponendovi un collegamento.

- Se non intendete cambiare l'indirizzo IP potete accettare di creare il collegamento.
- Che accettiate o meno di creare il collegamento il router sarà raggiungibile dalle Risorse di Rete.
- Fate doppio click sull'icona del Router (Collegamento o Risorse di Rete) per iniziare la configurazione.

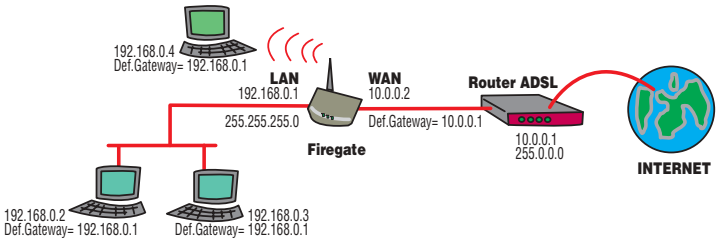
Se è stata impostata una password vedrete la seguente schermata:




- Lasciate il campo "**User Name**" vuoto ed inserite la password per il router.

## 2.6. CONFIGURAZIONE DI BASE

### Nuova struttura di rete con Firewall




Il Firewall avrà come indirizzi di WAN un indirizzo del tipo 10.0.0.x per poter comunicare correttamente con il Router e come Gateway avrà l'indirizzo del Router (nell'esempio 10.0.0.1).

Il Firewall avrà come indirizzo di LAN un indirizzo appartenente ad unaclasse **diversa** da quella di WAN (nell'esempio 192.168.0.1).
Tutti i PC hanno un indirizzo 192.168.0.x per poter comunicare correttamente con il Firewall ed hanno come indirizzo di Gateway l'indirizzo del Firewall (nell'esempio 192.168.0.1)
Di seguito un riassunto delle tipologie più comuni:

### Modem xDSL (ADSL, HDSL, SDSL, ecc)

| Tipo | Dettagli | Dati ISP richiesti |
|---|---|---|
| Dynamic IP address | Indirizzo IP dinamico.<br>L'indirizzo IP è allocato automaticamente quando ci si connette con l'ISP | Nessuno |
| Static (Fixed) IP Address | Indirizzo IP assegnato staticamente. | Indirizzi e Subnet mask a voi assegnate. |
| PPPoE | Connessione all'ISP in modalità PPP over Ethernet.<br>L'assegnazione dell'indirizzo è automatica. | User name e password. |
| PPTP | Connessione all'ISP in modalità Point to Point Tunneling.<br>L'assegnazione dell'indirizzo è solitamente dinamica ma può essere statica. | - Indirizzo IP del PPTP Server<br>- User name e password<br>- Indirizzi e Subnet mask a voi assegnate (se statico) |

### Other Modems (Altri modem, Router o Wireless)

| Tipo | Dettagli | Dati ISP richiesti |
|---|---|---|
| Dynamic IP Address | Indirizzo IP dinamico.<br>L'indirizzo IP è allocato automaticamente quando ci si connette con l'ISP | Nessuno |
| Static (Fixed) IP Address | Indirizzo IP assegnato staticamente. | Indirizzi e Subnet mask a voi assegnate. |

### Cable Modems

| Tipo | Dettagli | Dati ISP richiesti |
|---|---|---|
| Dynamic IP Address | Indirizzo IP dinamico.<br>L'indirizzo IP è allocato automaticamente quando ci si connette con l'ISP | Generalmente nessuno.<br>L'ISP potrebbe richiedere delle impostazioni come Hostname, Domain name, o MAC Address. |
| Static (Fixed) IP Address | Indirizzo IP assegnato staticamente. | Indirizzi e Subnet mask a voi assegnate.<br>L'ISP potrebbe richiedere delle impostazioni come Hostname, Domain name, o MAC Address. |

### Big Pond (Australia) e SingTel RAS

- Non utilizzati in Europa

Selezionate la modalità in base alla vostra tipologia di collegamento e proseguite nella configurazione cliccando su Next. Inserite i dati nelle apposite caselle.

*Esempi di configurazione:*

- **Accesso Internet tramite modem (Bridge) ADSL* e protocollo PPPoE:**
  Selezionate DSL/ADSL modem, selezionate PPPoE, inserite User name e password, deselezionate le voci "Connect automatically…" e "Disconnect after idle…", selezionate "Dynamic" per gli accessi con IP dinamico, selezionate "Static" se l'indirizzo IP è statico, inserite l'IP di WAN e l'indirizzo del DNS (fornito dall'ISP) in DNS.

- **Accesso ad Internet tramite Router ADSL* con NAT e IP dinamico:**
  Se la vostra LAN (e di conseguenza il Router ADSL) sta utilizzando gli indirizzi IP del range 192.168.0.x, modificate l'IP del router ADSL (ad esempio 10.0.0.1/255.0.0.0).
  Selezionate Other, selezionate "Static" IP address, inserite un indirizzo IP libero appartenente al range assegnato al router ADSL, Subnet mask e Gateway (ad esempio rispettivamente 10.0.0.2, 255.0.0.0 e 10.0.0.1. Inserite l'indirizzo del DNS (fornito dall'ISP) in DNS.

- **Accesso ad Internet tramite Router ADSL* con IP pubblico:**
  Selezionate Other, selezionate "Static" IP address, inserite uno degli indirizzi IP pubblici disponibili in IP address, inserite la Subnet mask, inserite l'indirizzo IP del router ADSL in Gateway, inserite l'indirizzo del DNS (fornito dall'ISP) in DNS.

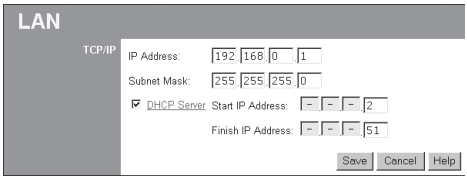
**** La porta LAN del Bridge o Router ADSL deve essere collegata alla porta WAN del dispositivo***

Al termine cliccate su **Finish**. Se avete selezionato "Test Internet connection" verrà verificata la raggiungibilità della parte WAN.

Cliccate su **Close** per chiudere il Wizard.

## LAN

Cliccate su LAN per accedere ai parametri della sezione LAN.




**TCP/IP IP Address**
**Network Mask**
Queste impostazioni dipendono dalle impostazioni della vostra LAN:
**Se utilizzate il DHCP server (consigliato):**
Generalmente nessun cambiamento è richiesto per queste impostazioni.
Comunque tutti i dispositivi in rete devono essere impostati come DHCP Client oppure utilizzare un indirizzo IP e Subnet mask compatibile.
**Se in LAN è già presente un DHCP server:**
Deselezionate il DHCP server interno per non incorrere in conflitti
**Se la LAN utilizza indirizzi IP statici:**
Impostate per il router un indirizzo IP tra quelli non utilizzati della LAN.
La Network Mask deve essere la stessa utilizzata per i PC in rete.

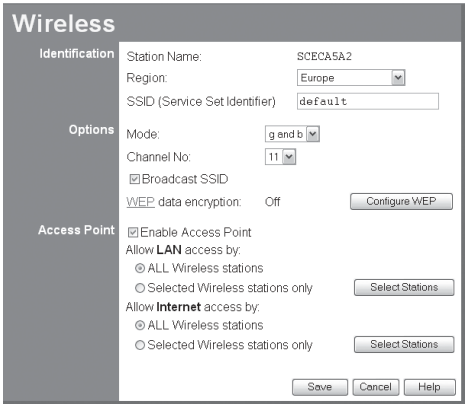
**DHCP Server**
Se abilitato (default), il router fornirà gli indirizzi IP e dati relativi ai computer DHCP client che ne faranno richiesta.
Se necessario modificate i campi Start IP Address e Finish IP Address per adattarlli alla vostra LAN.
Queste impostazioni determinano anche quanti client saranno gestiti.

**Save**
Salva nel dispositivo le modifiche apportate.

**Cancel**
Ignora le modifiche apportate e ricarica I parametri dal dispositivo.

## WIRELESS

Cliccate su Wireless per la configurazione della rete WLAN.




**Region:** Selezionate il paese dove l'AP deve operare, quest'impostazione disabilita i parametri NON utilizzabili nella regione selezionata.

**SSID** Inserite il nome della rete Wireless che volete configurare.
Per utilizzare le funzionalità di Roaming tutti gli Access Point devono avere lo stesso SSID.

**Mode** Selezionate la modalità di funzionamento dell'AP.
-**g and b** Abilita il funzionamento dell'AP in modalità IEEE 802.11g e IEEE 802.11b
-**b only** Solo modalità IEEE 802.11b
-**g only** Solo modalità IEEE 802.11g

**Channel No** Selezionate il canale Wireless da utilizzare. Verificate che il canale NON sia già utilizzato da altri dispositivi Wireless e se possibile mantenete sempre una distanza di 5 canali tra due applicazioni Wireless differenti.

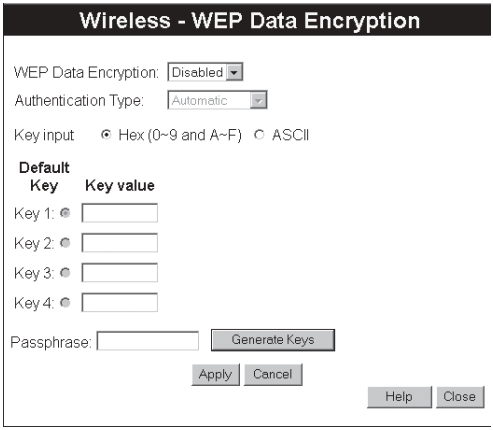
**Broadcast SSID:** disabilitate quest'opzione per nascondere la vostra rete Wireless, effettuando una scansione la rete NON sarà visibile.

**WEP** Selezionate il tasto Configure WEP per abilitare e configurare la crittografia WEP.

**Enable Access Point:** disabilitate quest'opzione per disabilitare tutte le funzionalità Wireless del dispositivo.

Selezionando l'opzione **Selected Wireless stations only** è possibile indicare le uniche stazioni Wireless (Client) possono avere accesso alla **LAN** cablata oppure ad **Internet** (WAN).
Selezionando **ALL Wireless stations** non viene applicata nessuna restrizione.

## Configure WEP




### WEP Data Encryption

Selezionate il tipo di crittografia da utilizzare:

- **Disabled** Nessuna Crittografia abilitata.
- **64 bit** Crittografia con chiave a 64bit
- **128 bit** Crittografia con chiave a 128bit

### Authentication Type

Selezionate il tipo di autenticazione:

**Open System**
**Shared Key**
**Automatic**

E' consigliabile lasciare questa impostazioni su Automatic, in alternativa verificate che questa autenticazione sia impostata su tutti i client Wireless.

### Key input

Selezionate la codifica con cui viene inserita la Key.

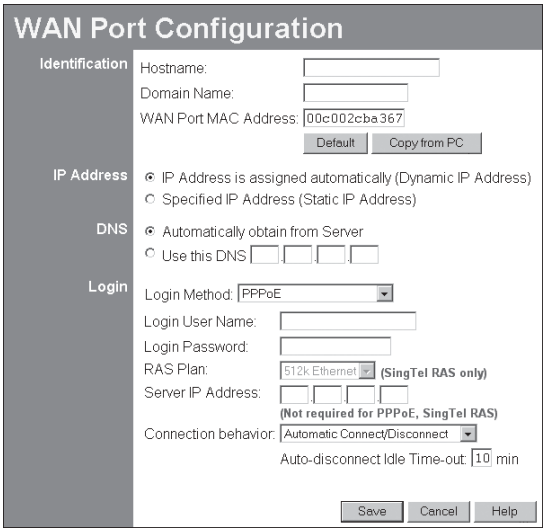
| | Lenght | |
|---|---|---|
| **Format** | **64-bit** | **128-bit** |
| **ASCII** | 5 characters | 10 hexadecimal codes |
| **HEX** | 13 characters | 26 hexadecimal codes |

La Key da utilizzare deve essere inserita in uno dei 4 campi Key1 / 2 / 3 / 4; la chiave scelta deve essere abilitata cliccando sul cerchio a fianco della Key.

### Passphrase

Se preferite è possibile generare automaticamente le Key partendo da una parola / frase a vostra scelta, utilizzando questa funzione.
Verificate prima che tutti i client Wireless supportino questo tipo di generazione delle Key.

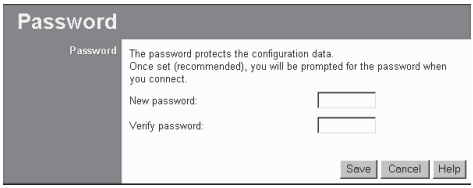
## INTERNET - WAN PORT



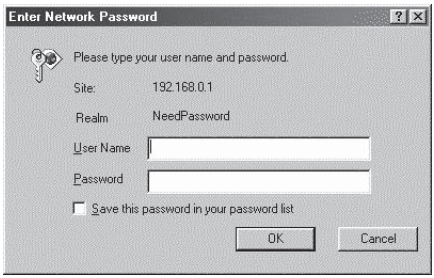

In questa finestra è possibile configurare tutte le impostazioni della porta di WAN con le stesse regole già descritte nel Wizard di configurazione.

## Password

Questa pagina permette di assegnare una password per l'accesso alla configurazione del dispositivo.




Una volta assegnata una password nella finestra sopra indicata, ogni volta che vorrete accedere alla configurazione del dispositivo, verrà visualizzata una finestra simile alla seguente:



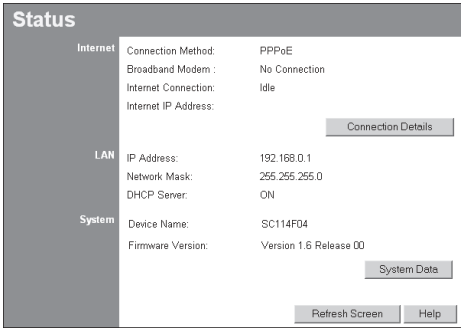

- Lasciate vuoto il campo "User Name"
- Inserite la password e cliccate OK.



digicom

## Status

La finestra di Status permette di verificare lo stato della connessione WAN, della sezione LAN e del Sistema.




### Internet

| | |
|---|---|
| **Connection Method** | Indica il metodo di connessione, come impostato nel Wizard |
| **Broadband Modem** | Stato della connessione (WAN) |
| **Internet Connection** | Stato della connessione Internet:<br>- Active (attivo)<br>- Idle (a riposo)<br>- Unknown (sconosciuto)<br>- Failed (fallito)<br>In caso di errori potete cliccare "Connection Details" per maggiori dettagli. |
| **Internet IP Address** | L'indirizzo IP assegnato dall'ISP (Internet Service Provider). |
| **"Connection Details"** | Descrizione dettagliata della connessione corrente |

### LAN

| | |
|---|---|
| **IP Address** | Indirizzo IP del dispositivo |
| **Network Mask** | Network Mask (Subnet Mask) associata all'indirizzo IP |
| **DHCP Server** | Stato del DHCP Server interno: "Enabled" (abilitato) o "Disabled" (disabilitato). |

### System

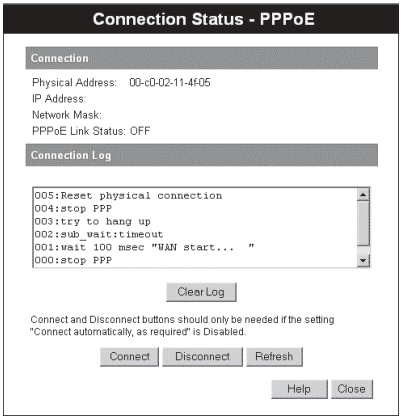
| | |
|---|---|
| **Device Name** | Identificativo del dispositivo |
| **Firmware Version** | Versione del firmware attualmente a bordo del dispositivo. |
| **System Data** | Informazioni varie di sistema. |

### Bottoni

| | |
|---|---|
| **Connection Details** | Finestra dei dettagli relativi alla connessione |
| **System Data** | Visualizza ulteriori informazioni varie di sistema |
| **Refresh Screen** | Aggiorna le informazioni visualizzate. |

## Connection Status - PPPoE

Log di connessione quando si utilizza PPPoE (PPP over Ethernet).




### PPPoE Connection

| | |
|---|---|
| **Physical Address** | Il Mac address (lato WAN) del dispositivo |
| **IP Address** | L'indirizzo IP con il quale il dispositivo viene identificato sulla WAN (Attenzione, non è l'indirizzo IP lato LAN del dispositivo) |
| **Network Mask** | La Network Mask (Subnet Mask) per l'indirizzo sopra |
| **PPPoE Link Status** | Indica lo stato attuale della connessione<br>Se la connessione non è attiva, il pulsante Connect permette di iniziarne una<br>- Se la connessione è attiva il pulsante Disconnect termina la connessione in corso |

### Connection Log

| | |
|---|---|
| **Connection Log** | Fornisce una serie di messaggi inerenti l'attività di connessione/negoziazione del protocollo PPPoE e del dispositivo sulla porta WAN. |

### Bottoni

| | |
|---|---|
| **Connect** | Se non collegato, attiva una connessione verso l'ISP. |
| **Disconnect** | Se connesso, termina la connessione. |
| **Clear Log** | Cancella il contenuto del log di connessione |
| **Refresh** | Aggiorna le informazioni visualizzate. |

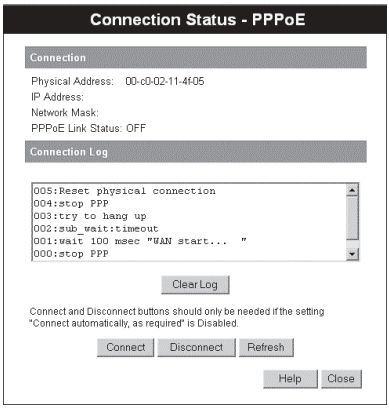
### Descrizione messaggi di Log:

| **Messaggio** | **Descrizione** |
|---|---|
| Connect on Demand | La connessione è stata attivata per "Connect on Demand" |
| Manual connection | La connessione è stata attivata premendo il pulsante "Connect" |
| Reset physical connection | Preparazione per la connessione |
| Connecting to remote server | Inizio connessione verso il remoto (provider o LAN) |
| Remote Server located | Il server remoto ha risposto alla richiesta di connessione |
| Start PPP | Inizio della negoziazione PPP con il server remoto |
| PPP up successfully | Negoziazione PPP completata con successo |
| Idle time-out reached | La connessione viene terminata per inattività dati superiore al valore impostato in "Idle Time-out". |
| Disconnecting | La connessione viene terminata per inattività o sconnessione manuale |

| | |
|---|---|
| Error: Remote Server not found | Il server remoto non ha risposto. Può dipendere dal server remoto stesso o da problemi sul link di connessione |
| Error: PPP Connection failed | Impossibile stabilire una corretta negoziazione PPP con il server remoto. Può dipendere dal server stesso o da errata impostazione di user id e password. |
| Error: Connection to Server lost | La connessione con il server remoto è stata persa. Potrebbe essere stata causata da caduta accidentale del link, mancanza di alimentazione o blocco del server remoto. |
| Error: Invalid or unknown packet type | I dati ricevuti dal server remoto sono incompatibili, incomprensibili o sconosciuti. Potrebbe essere causato da dati corrotti a causa di una connessione inaffidabile o instabile oppure il server remoto utilizza un protocollo non supportato dal dispositivo. |

## Connection Status - PPTP

Log di connessione quando si utilizza PPTP (Peer-to-Peer Tunneling Protocol).




### PPTP Connection

| | |
|---|---|
| **Physical Address** | Il Mac address (lato WAN) del dispositivo |
| **IP Address** | L'indirizzo IP con il quale il dispositivo viene identificato sulla WAN (Attenzione, non è l'indirizzo IP lato LAN del dispositivo) |
| **PPTP Status** | Indica lo stato attuale della connessione<br>- Se la connessione non è attiva, il pulsante Connect permette di iniziarne una<br>- Se la connessione è attiva il pulsante Disconnect termina la connessione in corso |

### Connection Log

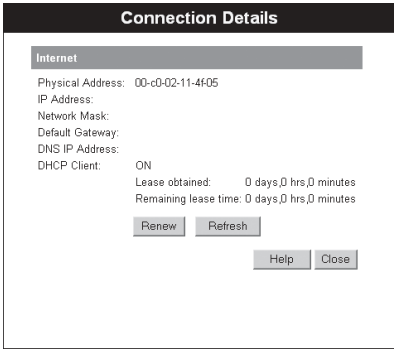
| | |
|---|---|
| **Connection Log** | Fornisce una serie di messaggi inerenti l'attività di connessione/negoziazione del protocollo PPTP. |

### Bottoni

| | |
|---|---|
| **Connect** | Se non collegato, attiva una connessione verso l'ISP. |
| **Disconnect** | Se connesso, termina la connessione. |
| **Clear Log** | Cancella il contenuto del log di connessione |
| **Refresh** | Aggiorna le informazioni visualizzate. |

## Connection Details - Fixed/Dynamic IP Address

Log di connessione quando si utilizza il metodo "Direct" (senza login).




### Fixed/Dynamic IP address
### Internet

| | |
|---|---|
| **Physical Address** | Il Mac address (lato WAN) del dispositivo |
| **IP Address** | L'indirizzo IP con il quale il dispositivo viene identificato sulla WAN (Attenzione, non è l'indirizzo IP lato LAN del dispositivo). |
| **Network Mask** | La Network Mask (Subnet Mask) per l'indirizzo sopra |
| **Default Gateway** | L'indirizzo IP del Gateway o Router associato con l'indirizzo sopra. |
| **DNS IP Address** | L'indirizzo IP del Domain Name Server attualmente in uso. |
| **DHCP Client** | Mostra "Enabled" (attivo) o "Disabled" (disattivo) a seconda dell'impostazione DHCP client. Se "Enabled" il tempo mostrato da "Remaining lease time" indica quando l'indirizzo IP allocato dal DHCP Server non sarà più valido. Allo scadere del tempo l'indirizzo sarà automaticamente rinnovato. Usare il bottone "Renew" per rinnovarlo manualmente. |

### Bottoni

| | |
|---|---|
| **Release/Renew** | - Premendo questo bottone l'indirizzo IP viene rinnovato o rilasciato. Non attivo se l'impostazione è Fixed (Static) IP address.. |
| **Refresh** | Aggiorna le informazioni visualizzate. |

## 2.7. CONFIGURAZIONE AVANZATA - ADVANCED

Cliccando sul bottone “Advanced” nel menù principale si accede ai menù delle Advanced Features.
Selezionando uno dei link presenti nella barra a sinistra è possibile configurare le seguenti funzionalità:

- Advanced Internet
  - Communication Applications, per dirigere delle “sessioni” di comunicazione entranti, quando la destinazione non è conosciuta, verso specifici PC di LAN
  - Special Applications, per mappare in modo specifico “porte UDP/TCP” interne ed esterne in uso da applicazioni particolari
  - Multi-DMZ, per permettere l’accesso “trasparente” ad un singolo PC di LAN dall’esterno.
    Con un abbonamento singolo utente (1 indirizzo IP) è possibile effettuare una sola esportazione DMZ (DMZ 1).
    Per abbonamenti multi-utente (n indirizzi IP) è possibile effettuare fino a 7 esportazioni DMZ.
  - URL filter, per bloccare la navigazione e accesso a siti internet “non autorizzati”
- Access Control, per restringere l’uso di Internet e di applicazioni a singoli o gruppi di PC
- DoS attack Firewall, per essere protetti dai più comuni attacchi di hacker e buontemponi.
- VPN passthrough, per realizzare connessioni protette attraverso Internet
- Virtual Servers, per “esportare” dei servizi presenti sui computer di LAN e renderli accessibili da Internet (Web server, FTP server, ecc)
- Dynamic DNS, per associare l’IP dinamico ad un URL (nome di dominio) virtuale, anche se l’IP cambia da connessione a connessione

## Access Control

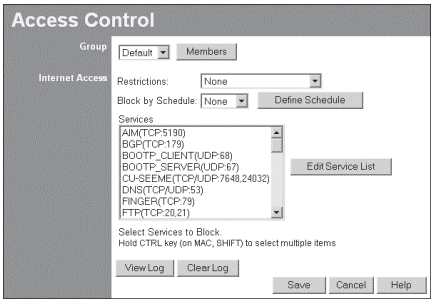
La funzione Access Control permette all'amministratore di implementare delle restrizioni all'accesso Internet alle singole stazioni (PC). Il criterio è quello del "Packet Filtering" per bloccare o scartare pacchetti di dati. E' possibile utilizzare i filtri predefiniti o crearne di propri.

Per default, i filtri sono disabilitati; nessun pacchetto viene bloccato o scartato

Per usare la funzione Access Control:

1. Applicate le restrizioni desiderate al gruppo "Everyone" (Tutti) e cliccate su "Setup". Per default, tutti i computer fanno parte del gruppo "Everyone" finchè non esplicitamente spostati in un gruppo diverso.
2. Applicate le restrizioni desiderate agli altri gruppi ("Group 1", "Group 2", ecc).
3. Per ogni Workstation che intendete spostare dal gruppo "Everyone", inserite i dati e selezionate il gruppo di destinazione.

***E' possibile impedire l'accesso ad Internet a TUTTI i computer senza specificare alcun dato, ma semplicemente applicando le restrizioni al gruppo "Default".***




### Access Control Group

| | |
|---|---|
| **Group** | Seleziona il gruppo di PC, denominati "Default", "Group 1", "Group 2", "Group 3", e "Group 4". Questi nomi non possono essere modificati. |
| **"Members"** | Aggiunge o rimuove dei PC dal Gruppo selezionato<br>- Il gruppo "Default" non può essere modificato. Questo gruppo definisce tutti I PC non assegnati agli altri gruppi.<br>- Per rimuovere un PC dal gruppo "Default" assegnarlo ad un gruppo differente, assign them to another Group.<br>- Per aggiungere un PC dal gruppo "Default" rimuoverlo dal gruppo al quale è attualmente assegnato.<br>Maggiori dettagli nella sezione *Group Members* |

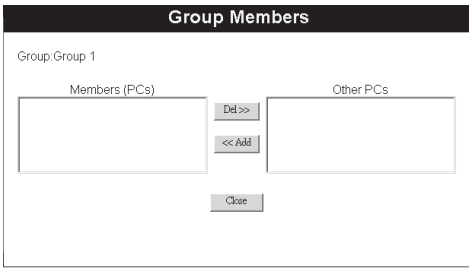
### Internet Access

| | |
|---|---|
| **Restrictions** | Restrizioni da applicare al gruppo selezionato:<br>- None – Nessuna restrizione.<br>- Block all Internet access – Tutto il traffico via porta WAN è bloccato.<br>- Block selected Services – Blocca solamente I servizi selezionati, in modo selettivo. |
| **Block by Schedule** | Per le restrizioni definite è possibile applicarle solamente in determinati orari del giorno. (Non ha effetto se non sono definite restrizioni) |
| **Define Schedule** | Permette di definire gli orari di scheduling delle restrizioni. |
| **Services** | Lista dei servizi definiti. Permette di selezionare I servizi da bloccare. Per selezionare entry multiple tenere premuto il tasto CTRL (SHIFT su Macintosh). |
| **Edit Service List** | Manutenzione della lista dei servizi. Permette di aggiungere o rimuovere dei servizi. |

## Bottoni

| | |
|---|---|
| **Members** | Manutenzione della lista dei membri di un gruppo. Permette di aggiungere o rimuovere membri. Il gruppo "Default" non può essere modificato. Questo gruppo definisce tutti I PC non assegnati agli altri gruppi. |
| **Save** | Salva le modifiche apportate |
| **Cancel** | Annulla le modifiche apportate |
| **View Log** | Visualizza il log degli accessi ad Internet che sono stati bloccati dalla funzione Access Control. |
| **Clear Log** | Cancella il log degli accessi ad Internet che sono stati bloccati dalla funzione Access Control. |

## Group Members

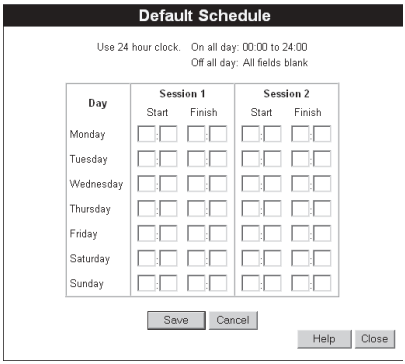



- Il bottone "Del >>" rimuove il PC selezionato dal gruppo (Members) e lo pone in Other PCs.
- Il bottone "<< Add" aggiunge il PC selezionato dal gruppo Other PCs nel gruppo corrente.

***I PC non assegnati ad alcun gruppo faranno parte del gruppo "Default".***
***I PC rimossi dai vari gruppi vanno ad aggiungersi al gruppo "Default".***

## Default Schedule

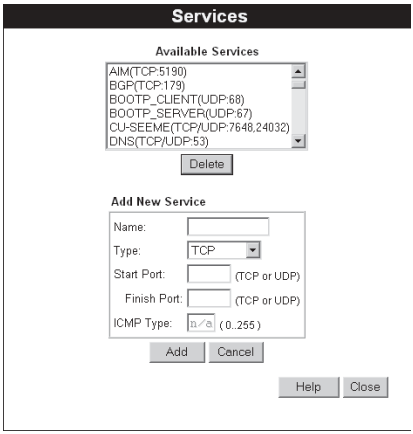
- Lo scheduling può essere (opzionalmente) applicato ad un gruppo Access Control.
- Il blocco dei servizi avverrà durante il periodo definito (tra "Start" e "Finish")
- Possono essere definiti due (2) sessioni o periodi differenti
- Il formato di inserimento è quello 24 ore.
- I campi vuoti non definiscono alcuno scheduling.



### Data - Default Schedule Screen

| | |
|---|---|
| **Day** | Giorno della settimana |
| **Session 1 Session 2** | Possono essere definiti due (2) sessioni o periodi differenti. La sessione 2 può essere lasciata vuota. |
| **Start Time** | Ora di inizio (24h) della restrizione. |
| **Finish Time** | Ora di termine (24h) della restrizione. |

## Services




### Services
### Available Services

| | |
|---|---|
| **Available Services** | Lista dei servizi disponibili |
| **"Delete"** | Cancella I servizi aggiunti manualmente. I servizi predefiniti non possono essere eliminati. |

### Add New Service

| | |
|---|---|
| **Name** | Nome mnemonico del servizio, senza spazi o punti. |
| **Type** | Selezionare il protocollo (TCP, UDP, ICMP) usato dal servizio. |
| **Start Port** | Inizio del range di porte utilizzato dal servizio. Se la porta è singola specificare lo stesso numero sia in "Start" che "Finish". |
| **Finish Port** | Fine del range di porte utilizzato dal servizio. Se la porta è singola specificare lo stesso numero sia in "Start" che "Finish". |
| **ICMP Type** | Per servizi basati su ICMP inserire il tipo (numero) del servizio |

### Bottoni

| | |
|---|---|
| **Delete** | Cancella il servizio selezionato dalla lista |
| **Save** | Aggiunge il servizio alla lista usando i dati presenti in "Add New Service". |
| **Cancel** | Azzera l'area "Add New Service " per l'aggiunta di una nuova entry. |

### Access Control Log

Questo log permette di visualizzare quali tentativi di accesso ad Internet sono stati bloccati e I relativi dettagli

| | |
|---|---|
| **Date/Time** | Data e ora del tentativo di accesso. |
| **Name** | Il nome del PC (se conosciuto), preso dalla lista PC database |
| **Source IP address** | Indirizzo IP del PC che ha effettuato il tentativo |
| **MAC address** | MAC address del PC che ha effettuato il tentativo. |
| **Destination** | URL o indirizzo IP di destinazione |



digicom

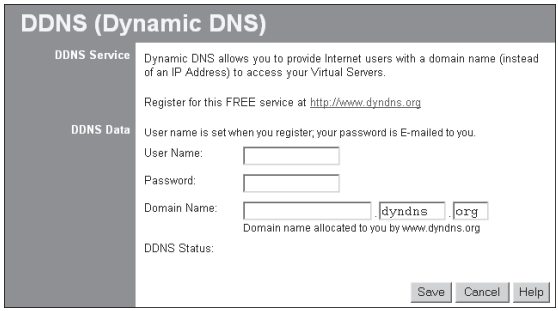
## Dynamic DNS (Domain Name Server)

Questa funzione si rivela utilissima in combinazione con la funzione di Virtual Server. DDNS permette agli utenti Internet di accedere ai vostri Virtual Servers utilizzando un URL invece di un indirizzo IP, risolvendo anche il problema dell'indirizzo dinamico che può cambiare da connessione in connessione.

### Come funziona il servizio DDNS:

1. Per poter utilizzare questo servizio dovete innanzitutto effettuare una registrazione (gratuita al momento della stesura di questo documento) all'indirizzo http://www.dyndns.org . La password vi sarà inviata via email.
2. Una volta effettuata la registrazione potrete usare l'opzione "Create New Host" (in www.dyndns.org) per richiedere la creazione di un vostro dominio virtuale, ad esempio mioweb.virtual.it.
3. Inserite I dati forniti dA www.dyndns.org nella funzione DDNS.
4. Il router farà si che l'indirizzo IP assegnatovi dall'ISP sia automaticamente registrato su http://www.dyndns.org.
5. Da Internet, gli utenti potranno accedere ai vostri Virtual Servers (o PC in DMZ) usando il nome di dominio, ad esempio http://mioweb.virtual.it

### Dynamic DNS



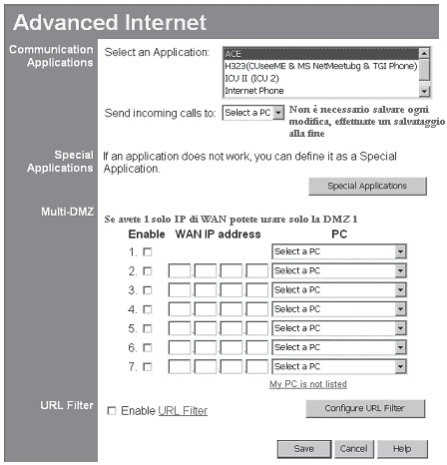

### Dynamic DNS
### DDNS Service

| | |
|---|---|
| **DDNS Service** | - E' necessario attivare un account prima di poter utilizzare il servizio.<br>- Cliccate su questo link per connettervi al sito www.dyndns.org<br>- Riceverete la user id e password iniziale via email. Potrete cambiarla in seguito.<br>- Una volta registrati, utilizzate il link "Create New Host" per richiedere un nome di dominio. |

### DDNS Data

| | |
|---|---|
| **User Name** | Inserire lo "User name" specificato in www.dyndns.org al momento della registrazione. |
| **Password** | Inserire la password corrente in www.dyndns.org |
| **Domain Name** | - Inserire il nome di dominio, come attivato in www.dyndns.org.<br>- Usare solamente caratteri e "-" per il nome di dominio. |
| **DDNS Status** | Messaggio proveniente dal server DDNS Server di www.dyndns.org<br>- Normalmente il messaggio deve riportare "Update successful" (l'indirizzo IP corrente è stato aggiornato sul server www.dyndns.org).<br>- Se il messaggio è "No host" il nome non è stato allocato per voi. Connettetevi al sito www.dyndns.org per verificare e correggere il problema. |

## Advanced Internet




### Communication Applications

La maggior parte delle applicazioni sono supportate in modo trasparente dal dispositivo, tuttavia alcune particolari situazioni possono non funzionare correttamente in presenza del protocollo NAT, per via dell'impossibilità di accettare connessioni iniziate dall'esterno. Spesso il router non è in grado di poter determinare chi è il destinatario in Lan di una data connessione. Per risolvere questo problema si può utilizzare la funzione ***Communication Applications***. Se il problema suddetto dovesse verificarsi è possibile associare un determinato PC in LAN, selezionandolo dal database (vedi apposita sezione) per far si che le quel tipo di connessioni venga rediretta sul PC selezionato.

### Communication Applications

**Select an Application** Lista della applicazioni che possono generare una connessione dall'esterno dove il destinatario non è determinabile dal router.

**Send incoming calls to** Lista dei PC in LAN.

- Se necessario è possibile aggiungere manualmente I PC nel "PC Database" (vedi apposita sezione).
- Per ogni applicazione della lista è possibile scegliere un PC di LAN PC.
- Cliccare "Save" dopo aver selezionato I vari PC, non per ogni singola scelta.

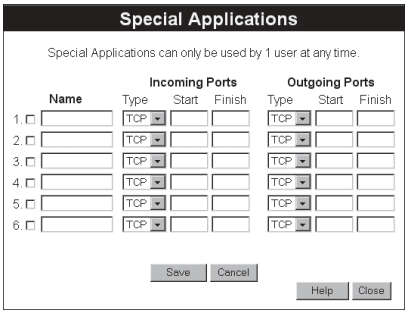
## Special Applications

Le applicazioni Internet che fanno uso di porte non standardizzate potrebbero non funzionare correttamente attraverso le funzioni di Firewall del dispositivo.

In questo caso è possibile inserire i parametri necessari nella sezione "Special Application" e permettere il funzionamento associando “porte entranti” a “porte uscenti”.

Per la corretta configurazione di questa sezione è necessario disporre di tutti I dettagli relativi all’uso delle porte TCP/UDP dell’applicazione in oggetto.

Le porte entranti "Incoming" e uscenti "Outgoing" sono riferite dal punto di vista del client (PC).




## Special Applications

| | |
|---|---|
| **Checkbox** | Abilita o Disabilita il supporto dell'applicazione |
| **Name** | Nome mnemonico descrittivo dell'applicazione |
| **Incoming Ports** | - Type - Il protocollo (TCP o UDP) usato per connettersi al servizio.<br>- Start - Inizio del range di porte utilizzato dal server dell'applicazione quando si ricevono i dati. Se la porta è singola specificare lo stesso numero sia in "Start" che "Finish".<br>- Fine del range di porte utilizzato dal server dell'applicazione quando si ricevono i dati. |
| **Outgoing Ports** | - Type - Il protocollo (TCP o UDP) usato per connettersi al servizio.<br>- Start - Inizio del range di porte utilizzato dal server dell'applicazione quando si inviano i dati. Se la porta è singola specificare lo stesso numero sia in "Start" che "Finish".<br>- Fine del range di porte utilizzato dal server dell'applicazione quando si inviano i dati. |

### Uso di Special Application

- Configurare le varie entry some necessario
- Lato PC utilizzare l’applicazione normalmente.

***NOTA: Solamente un PC alla volta potrà utilizzare una determinata Special application. Una volta che un PC ha terminato di usare una Special App. un timeout di circa 3 minuti viene attivato prima che la stessa Special App. possa essere utilizzata nuovamente da un altro PC.***

***Se una applicazione non dovesse comunque funzionare provare ad utilizzare la funzione "Multi-DMZ".***

### Multi-DMZ

Questa funzione, se abilitata, permette di rendere disponibili dall'esterno fino a 7 PC, associandoli a 7 indirizzi IP pubblici (che devono essere disponibili sul lato WAN).
Questo permette di rendere disponibili dei server collegati con indirizzo privato (LAN) all'esterno (da Internet / WAN).
Se l'abbonamento utilizzato per la connessione Internet è "singolo utente", con un unico indirizzo IP è possibile utilizzare solo la prima DMZ.
Per utilizzare questa funzione, il PC interessato deve essere già inserito nel Database PC.
E' consigliabile configurare questi PC con indirizzo IP fisso, in alternativa l'indirizzo deve essere riservato nel server DHCP.
***I PC interessati hanno una protezione limitata, il firewall è comunque in grado di proteggere queste macchine dagli attacchi base (DOS, IP Spoofing...).***
***Utilizzate la funzione Multi-DMZ solo se necessario, è preferibile utilizzare sempre i Virtual Server o le Special Application.***

### URL Filter

La funzione di URL Filter permette di bloccare l'accesso a siti Web non desiderati.

- La funzione si basa su stringhe di filtro. Se la stringa definita appare nell'URL del sito, la richiesta viene bloccata.
- L'abilitazione di *URL Filter* ha effetti su Internet *Access Log*. Se abilitato l'informazione di "Destination" appare in forma di URL, altrimenti in forma di indirizzo IP.

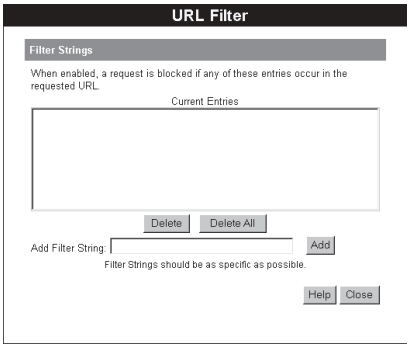



*Figure 1: URL Filter Screen*

### URL Filter
### Stringhe da filtrare

| | |
|---|---|
| **Current Entries** | Mostra le stringhe di filtro definite. Se vuoto, nessun filtro è attivo |
| **Add Filter String** | Per aggiungere una stringa di filtro, digitare la stringa e cliccare su "Add".<br>Una stringa può essere un dominio, ad esempio "www.trash.com" o una parte , ad esempio "ads"<br>Se la stringa inserita compare in una posizione qualsiasi dell'URL la richiesta verrà bloccata. |

### Bottoni

| | |
|---|---|
| **Delete/Delete All** | Cancella la entry selezionata o tutte le entry. Per selezionare entry multiple tenere premuto il tasto CTRL (SHIFT su Macintosh). |
| **Add** | Aggiunge la stringa inserita. |

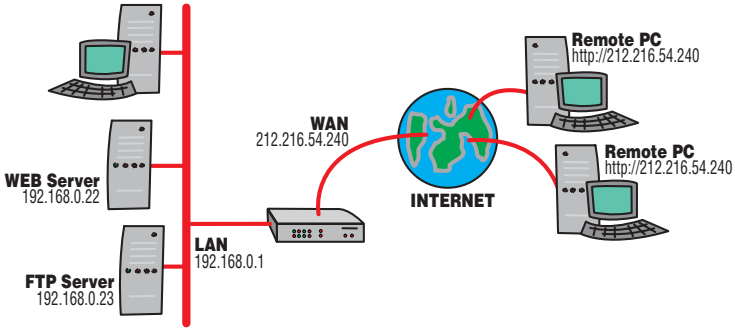
## Virtual Servers

La funzione Virtual Servers permette ad utenti localizzati in Internet di avere accesso a Server presenti in LAN attraverso il router.

Normalmente un'utente presente in Internet non ha accesso ai computer della vostra LAN perchè:

- Il computer non ha un indirizzo IP globale.
- Tentativi di accesso alla LAN vengono automaticamente bloccati dal protocollo NAT che "nasconde" qualsiasi computer ad esso collegato (l'intera LAN).

La funzione "Virtual Server" ha lo scopo di rendere "visibili" uno o più computer e far sì che possano essere raggiunti da Internet (se il router è connesso ad Internet).




### Indirizzi IP visibili agli utenti Internet

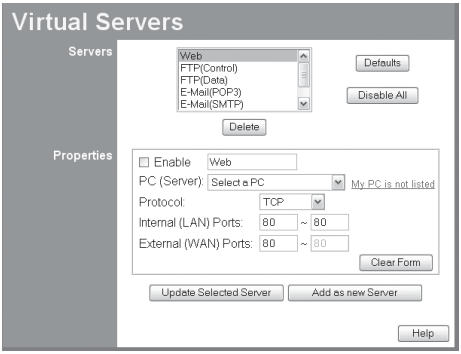
Notare che nell'esempio entrambi gli utenti Internet accedono allo stesso indirizzo IP ma utilizzando protocolli e servizi differenti.

**Per gli utenti Internet tutti i Virtual Servers della LAN avranno lo stesso indirizzo IP.**

**L'indirizzo IP di WAN** è quello specificato in Internet IP Address della finestra Status e può essere statico o dinamicamente assegnato dal provider Internet (diverso di connessione in connessione).

E' possibile utilizzare la funzione DDNS (Dynamic DNS) che permette agli utenti Internet di collegarsi ad un vostro Virtual Server utilizzando un URL invece di un indirizzo IP.

### Virtual Servers




Sono disponibili diversi Servers predefiniti, ma è possibile definire dei propri server. I dettagli sono visualizzati nella area "Properties".

## Virtual Servers

### Servers

| | |
|---|---|
| **Servers** | Lista dei server disponibili |

### Properties

| | |
|---|---|
| **Enable** | Abilitazione del Virtual server selezionato<br>- Se abilitato, le connessioni entranti saranno redirette al PC selezionato.<br>- Se disabilitato, le connessioni entranti saranno bloccate |
| **PC (Server)** | PC o computer associato al servizio (deve fornire il servizio in oggetto). |
| **Protocol** | Selezionare il protocollo (TCP o UDP) usato dal server. |
| **Internal (LAN) Ports:** | Inserire il range di porte utilizzato dal server per dare accesso al servizio |
| **External (WAN) Ports:** | Inserire il range di porte utilizzato dagli utenti Internet per accedere al servizio. Generalmente è lo stesso di Internal (LAN) Ports.<br>Potete eventualmente utilizzarne uno differente. Il router effettuerà automaticamente il "mapping" o "translation" del caso. |

### Bottoni

| | |
|---|---|
| **Defaults** | Cancella i server definiti dall'utente e reimposta quelli pre-definiti al default di fabbrica. |
| **Disable All** | Disabilita tutti i servizi abilitati |
| **Add** | Aggiunge una nuova entry nella lista Virtual Server usando I parametri presenti in "Properties". L'entry selezionata in lista è ignorata e non ha effetto. |
| **Update** | Aggiorna la entry selezionata nella lista Virtual Server usando I parametri presenti in "Properties". |
| **Delete** | Cancella la entry selezionata nella lista Virtual Server. Solamente i server definiti dall'utente possono essere cancellati. |
| **Clear Form** | Azzera l'area "Properties" per l'aggiunta di una nuova Virtual Server entry. |

### Virtual Servers definiti dall'utente

**Per creare una nuova entry:**

- Cliccare su Clear Form.
- Inserire i dati (vedi descrizione) necessari.
- Cliccare su Add.

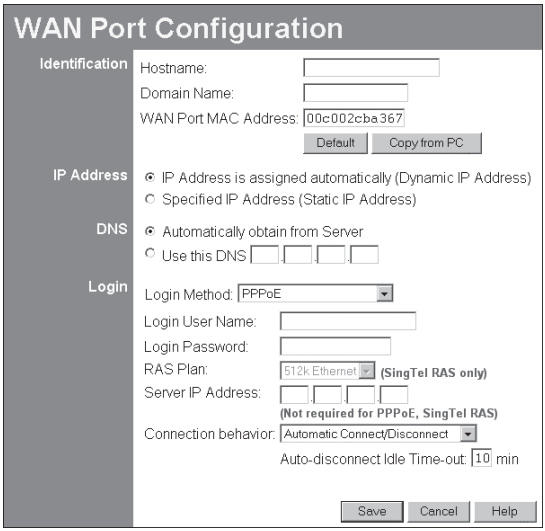
**Per cancellare una entry:**

- Selezionare la entry dalla lista
- Cliccare su Delete.

**Per modificare una entry:**

- Selezionare la entry dalla lista.
- Effettuare le modifiche
- Cliccare su Update.

## INTERNET - WAN PORT

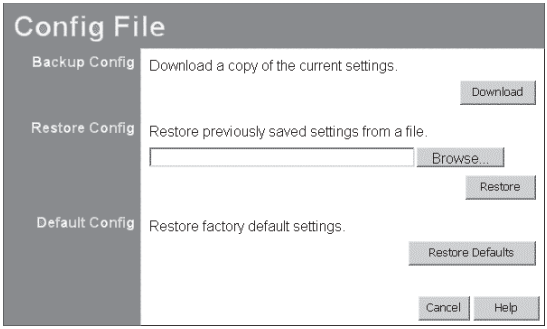



In questa finestra è possibile configurare tutte le impostazioni della porta di WAN con le stesse regole già descritte nel Wizard di configurazione.

## 2.8. CONFIGURAZIONE AVANZATA - ADMINISTRATION (Advanced Configuration)

| | |
|---|---|
| **Config File** | In questo menu è possible effettuare un salvataggio di backup della Configurazione, oppure di ripristinare le impostazioni precedentemente salvate. |
| **Logs** | Visualizzazione e impostazioni relative ai Log. |
| **Network Diagnostics** | Ping e DNS LookUp. |
| **Options** | Opzioni varie come Backup DNS, UPnP, etc.. |
| **PC Database** | Lista (database) dei PC di LAN, da selezionare successivamente nelle funzioni "DMZ PC" o "Virtual Server". Il database è mantenuto automaticamente e si possono aggiungere manualmente entry per indirizzi IP statici. |
| **Remote Administration** | Abilitazione delle configurazione da Internet. |
| **Routing** | Interazione con altri Router o Gateway in LAN. |
| **Security** | Impostazioni Firewall e di sicurezza. |
| **Firmware Upgrade** | Aggiornamento Firmware del dispositivo. |

### Config File

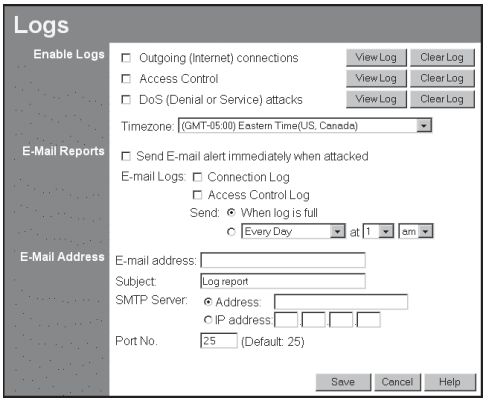



| | |
|---|---|
| **Backup Config** | Selezionate il tasto **Default** per salvare la configurazione attuale su file. |
| **Restore Config** | Selezionate **Browse** per indicare il percoso del file di configurazione da caricare e successivamente selezionate **Restore**. |
| **Default Config** | Selezionate **Restore Default** per caricare tutte le impostazioni di fabbrica del dispositivo. |

## Logs

I log tracciano e registrano vari tipi di attività svolte dal dispositivo. L'utilità dei log è fondamentale per la determinazione e risoluzione di eventuali problemi, ma può generare un gran numero di dati e influire sulle prestazioni generali del dispositivo.

Date le basse capacità di memorizzazione del dispositivo stesso, i log possono essere inviati via email ad un indirizzo predeterminato.




### Logs
### Enable Logs

| | |
|---|---|
| **Outgoing Connections** | Se selezionato, le connessioni verso Internet vengono inserite nel log, normalmente con un indirizzo IP. |
| **Access Control** | Se selezionato, le connessioni verso Internet bloccate da "Access Control" vengono inserite nel log. |
| **DoS Attacks** | Se selezionato le informazioni relative ad attacchi DoS (Denial of Service) bloccate dal Firewall vengono inserite nel log. |
| **Timezone** | Selezionare la corretta Timezone, per una corretta visualizzazione di data e ora nei log. |

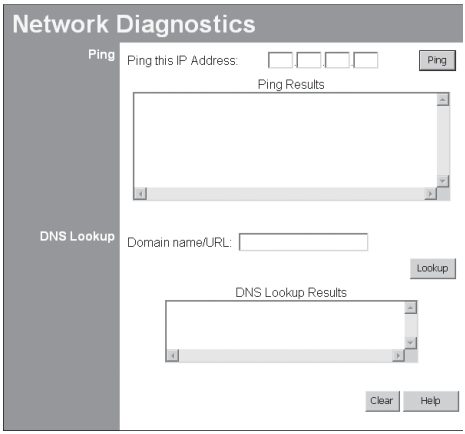
### E-Mail Reports

| | |
|---|---|
| **Send E-mail alert** | Se selezionato una E-mail viene inviata immediatamente in caso di un attacco DoS (Denial of Service). |
| **E-mail Logs** | Selezionare quali log si desidera ricevere via e-mail |
| **Send** | Selezionare quando si desidera ricevere I log via e-mail.<br>- When log is full – Quando il log raggiunge la massima capacità di memorizzazione.<br>- Every day, Every Monday ... – Il log viene inviato agli intervalli selezionati.<br>- Selezionando "Every day" il log verrà inviato all'ora selezionata.<br>- Selezionando un giorno specifico, il log verrà inviato una volta alla settimana.<br>- Se il log si riempie prima della data/ora specificata, questo verrà inviato comunque subito. |

### E-Mail Address

| | |
|---|---|
| **E-mail Address** | Inserire l'indirizzo e-mail al quale inviare il log. Questo indirizzo comparirà anche come mittente. |
| **Subject** | Inserire il "soggetto" per l'e-mail. |
| **SMTP Server** | Inserire l'indirizzo IP del server SMTP (Simple Mail Transport Protocol) per la posta in uscita. |
| **Port No.** | Inserire il numero di porta del server SMTP, generalmente 25. |

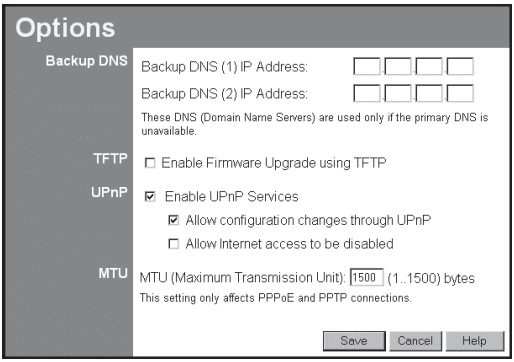
## Network Diagnostic




**Ping**
**DNS Lookup**

Inserite l'indirizzo IP da "pingare" nelle 4 caselle predisposte e selezionate **Ping** per avviare il test. Inserite il nome dominio o l'URL nell'apposito campo e selezionare **Lookup** per verificare la risoluzione del nome tramite i DNS impostati nel dispositivo.

## Options




### Options

### Backup DNS

**IP Address** Inserire gli indirizzi IP dei DNS (Domain Name Servers). Questi DNS saranno usati nel caso il primary DNS fosse irraggiungibile.

### TFTP

**Enable Firm-ware Upgrade using TFTP**

- Se abilitato, permette l'aggiornamento del firmware via TFTP (Trivial FTP) seguendo le istruzioni allegate al file di aggiornamento via TFTP

### UPnP

**Enable UPnP Services**
- UPnP (Universal Plug and Play) permette la rilevazione automatica e configurazione del dispositivo connesso in LAN. UpnP è supportato da Windows ME/XP.
- Se Enabled, il dispositivo è visibile via UPnP.
- Se non Enabled, il dispositivo non è visibile via UPnP.

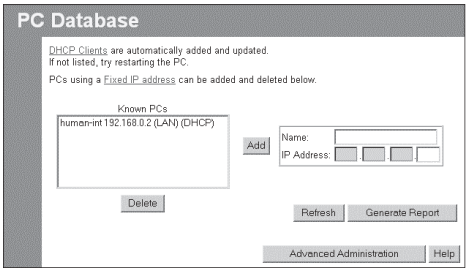
**Allow Configuration...**
- Se selezionato, si potrà modificare la configurazione via UPnP.
- Se non selezionato gli utenti potranno solamente visualizzare la configurazione via UPnP.

**Allow Internet access to be disabled**
- Se selezionato, si potrà disabilitare l'accesso ad Internet via UPnP.
- Se non selezionato, non si potrà disabilitare l'accesso ad Internet via UPnP

### MTU

**MTU size** Il valore di MTU (Maximum Transmission Unit) non deve essere modificato salvo diverse indicazioni del supporto tecnico
- Inserire un valore compreso tra 1 e 1500.
- Il dispositivo negozierà comunque il valore più basso con il remoto.
- Per connessioni dirette (non PPPoE o PPTP) l'MTU utilizzato è sempre 1500.

## PC Database




- I PC configurati come "DHCP Clients" (Ottieni un indirizzo IP automaticamente) vengono inseriti automaticamente nel database.
- Il dispositivo utilizza il MAC address per identificare ogni PC, non il nome o l'indirizzo IP in quanto questi possono variare.
- Il database non contiene I PC che operano con indirizzi IP statici a meno che non vengano manualmente inseriti.

### PC Database

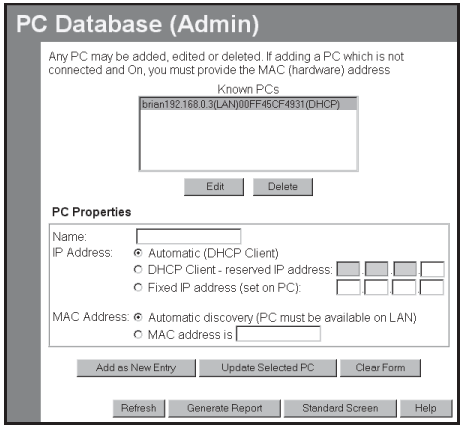
| | |
|---|---|
| **Known PCs** | Lista delle entry correnti. Sono visualizzati nome, indirizzo IP e tipo. |
| **Name** | Per aggiungere un nuovo PC alla lista inserire un nome mnemonico, possibilmente il nome dell'host per comodità. |
| **IP Address** | Inserire l'indirizzo IP del PC. Al PC verrà inviato un PING per determinarne il MAC Address. Se il PC non è raggiungibile non sarà possibile inserirlo nella lista. |

### Bottoni

| | |
|---|---|
| **Add** | Aggiunge il PC alla lista. |
| **Delete** | Cancella il PC dalla lista |
| **Refresh** | Aggiorna i dati visualizzati |
| **Generate Report** | Visualizza una lista completa e dettagliata. |
| **Advanced Administration** | Visualizza il menu in modalità Advanced. |

## PC Database (Admin)

Visualizzazione in modalità "Advanced Administration"




## PC Database ( Admin)

**Known PCs** Lista delle entry correnti. Sono visualizzati nome, indirizzo IP e tipo.

## PC Properties

**Name** Per aggiungere un nuovo PC alla lista inserire un nome mnemonico, possibilmente il nome dell'host per comodità.

**IP Address** Selezionare l'opzione appropriata:
- Automatic – Il PC è impostato come DHCP client. Il dispositivo allocherà un indirizzo per il PC quando questo ne farà. L'indirizzo potrebbe cambiare.
- DCHP Client - Reserved IP Address - Il PC è impostato come DHCP client. Il dispositivo allocherà sempre lo stesso indirizzo IP per il PC quando questo ne farà richiesta.
- Fixed IP Address – Il PC è impostato con un indirizzo IP statico.

**MAC Address** Select the appropriate option
- Automatic discovery – Il dispositivo cercherà in LAN il PC per scoprirne il MAC address. Il PC deve essere raggiungibile in LAN.
- MAC is – Inserire il MAC address del PC. Il MAC address è anche chiamato "Hardware Address", "Physical Address", o "Net-work Adapter Address".

## Bottoni

**Add as New Entry** Aggiunge l'indirizzo IP del PC usando i dati in "Properties" . Se "Automatic discovery" è selezionato al PC verrà inviato un PING per determinarne il MAC Address, pertanto il PC deve essere raggiungibile in LAN.

**Update Selected PC** Aggiunge (modifica) l'indirizzo IP del PC usando i dati in "Properties"

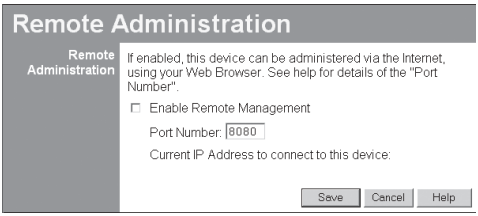
**Clear Form** Azzera l'area " Properties per l'aggiunta di una nuova entry.

**Refresh** Aggiorna i dati visualizzati

**Generate Report** Visualizza una lista completa e dettagliata.

**Standard Screen** Visualizza il menu in modalità Standard.

## Remote Administration




Selezionate l'opzione "**Enable Remote Managment**" per attivare il server di configurazione sulla porta WAN del dispositivo. Per poter accedere alla configurazione è necessario collegarsi all'indirizzo di WAN del Router sulla porta indicata.

L'URL deve essere scritto nel seguente modo:

http://xxx.xxx.xxx.xxx:yyyy cioè http:// indirizzo IP : porta

## Routing

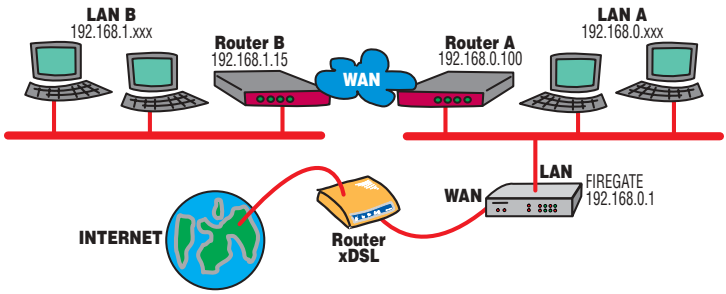
Questa sezione può essere ignorata se sulla vostra LAN non sono presenti Router.

Se invece sulla vostra rete sono presenti altri Router, sarà necessario intervenire sulla configurazione di FireGate Wave 54 e su quella dei Router, per permettere il corretto funzionamento dell'intero sistema.

Se i computer serviti da FireGate Wave 54 non devono accedere alla rete remota o se i computer sulla rete remota non devono accedere ad Internet potete ignorare questa sezione.
Se gli altri router in LAN utilizzano il protocollo **RIP** potete abilitarlo anche sul dispositivo ed ignorare la sezione di Routing statico.
Se preferite assegnare manualmente ed in modo **statico** tutti gli instradamenti dovrete configurare la sezione di Routing statico.
Per effettuare correttamente questo tipo di operazioni fatevi assistere dall'amministratore di rete o dal personale preposto all'installazione e manutenzione dei Router. Per comodità e maggiore chiarezza disegnate uno schema dell'attuale impostazione della rete, riportando gli indirizzi IP delle reti e dei router connessi.

### Esempio di Routing

L'esempio che segue prevede l'inserimento di FireGate Wave 54 in un sistema composto da due LAN (LAN A, 192.168.0.x e LAN B 192.168.1.x) indipendenti ed interconnesse da due router (ROUTER A e ROUTER B)



In questa situazione le tabelle di routing dei due router contengono le informazioni su come raggiungere le rispettive reti remote.
Esemplificando, il ROUTER A connesso alla propria rete 192.168.0.x , sa che per raggiungere una qualsiasi stazione della rete 192.168.1.x deve inoltrare i pacchetti dati all'indirizzo 192.168.1.15, ovvero il ROUTER B.
Il ROUTER B a sua volta sa che se dalla propria rete 192.168.1.x si deve raggiungere una qualsiasi stazione della rete 192.168.0.x, esso deve inoltrare i pacchetti dati all'indirizzo 192.168.0.100, ovvero il ROUTER A.

All'inserimento del dispositivo nel sistema, affinchè tutto continui a lavorare correttamente, i vari componenti dovranno disporre delle seguenti informazioni:

### FireGate Wave 54
La rete remota 192.168.1.x (Destination IP Address) è raggiungibile attraverso il router all'indirizzo 192.168.0.100 (Gateway Address).

### ROUTER A (Router locale)
La rete remota 192.168.1.x è raggiungibile attraverso il router all'indirizzo 192.168.1.15 (Informazione già presente nella routing table).
Ogni altra destinazione (Default route, Internet in questo caso) è raggiungibile attraverso il router all'indirizzo 192.168.0.1 (Informazione da aggiungere).

### ROUTER B (Router remoto)
La rete remota 192.168.0.x è raggiungibile attraverso il router all'indirizzo 192.168.0.100, informazione già presente nella routing table. Ogni altra destinazione (Default route, Internet in questo caso) è raggiungibile attraverso il router all'indirizzo 192.168.0.100 (Informazione da aggiungere).

In questo caso specifico è possibile configurare la tabella di routing del ROUTER B con un'unica entry che contenga l'informazione che qualsiasi destinazione (LAN A e Internet) sono raggiungibili attraverso un'unica default route che punta all'indirizzo 192.168.0.100.

Riassumendo, le tabelle di routing dei tre dispositivi dovranno contenere le seguenti informazioni:

| **FireGate Wave 54** | | **Note** |
|---|---|---|
| Destination IP Address | 192.168.1.0 | LAN B |
| Network Mask | 255.255.255.0 | |
| Gateway IP Address | 192.168.0.100 | Router A |
| Metric | 1 | |

| **ROUTER A** | | Note |
|---|---|---|
| Destination IP Address | 192.168.1.0 | LAN B |
| Network Mask | 255.255.255.0 | |
| Gateway IP Address | 192.168.0.15 | Router B |
| Default Route | | |
| Destination IP Address | 0.0.0.0 | * |
| Network Mask | 0.0.0.0 | * |
| Gateway IP Address | 192.168.0.1 | FireGate Wave 54 |

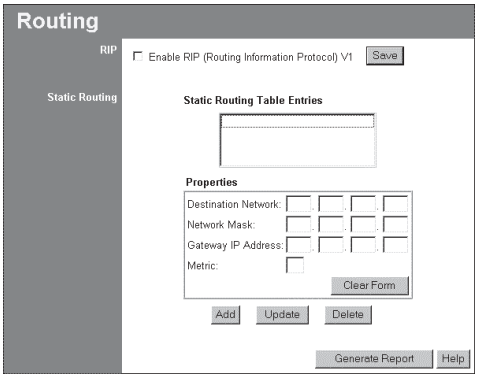
| **ROUTER B** | | Note |
|---|---|---|
| Destination IP Address | 192.168.0.0 | LAN A |
| Network Mask | 255.255.255.0 | |
| Gateway IP Address | 192.168.0.100 | Router A |

| **Default Route**** | | |
|---|---|---|
| Destination IP Address | 0.0.0.0 | * |
| Network Mask | 0.0.0.0 | * |
| Gateway IP Address | 192.168.0.100 | Router A |

**Questa è la sintassi normalmente utilizzata per indicare una default route. Verificate che sia valida anche per i vostri router.*
***In questo esempio potrebbe essere l'unica entry nella routing table del Router B.*

## Routing

E' preferibile utilizzare il protocollo RIP oppure in alternativa le tabelle di routing statico, anche se è possibile usare entrambe le modalità simultaneamente.




### Routing
### RIP

**Enable RIP** Abilita la funzione RIP (Routing Information Protocol) del dispositivo.
Questo dispositivo supporta solamente il protocollo RIP 1.

### Static Routing

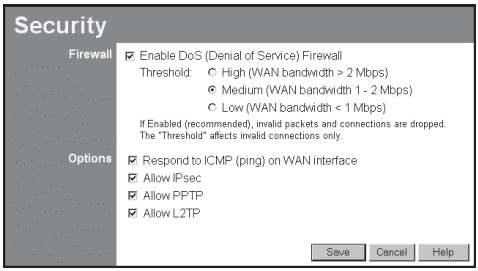
**Static Routing Table Entries** Lista della route statiche attualmente inserite
- I dettagli della route sono mostrati in "Properties".
- Modificare i parametri come desiderato e cliccare "Update" per salvare le modifiche.

**Properties**
- Destination Network – L'indirizzo di rete della LAN remota. Per una LAN in classe C standard, i primi tre campi identificano l'indirizzo di rete, il quarto va lasciato a zero, ad esempio 192.168.1.0.
- Network Mask – La Subnet Mask della LAN remota. Per una LAN in classe C standard, questa è 255.255.255.0
- Gateway IP Address – Indirizzo IP del Gateway o Router in LAN (locale) al quale il dispositivo deve far riferimento per raggiungere la rete remota)
- Metric – Numero di salti o "hops" (routers) da attraversare per raggiungere la LAN remota. Verrà utilizzata la via più breve. Il default è 1.

### Buttons

**Save** Salva l'impostazione RIP. Non ha effetto sulle tabelle di routing statiche.
**Add** Aggiunge una nuova entry alla tabella di routing statica con I parametri presenti in "Properties".
**Update** Aggiorna una nuova entry alla tabella di routing statica con I parametri presenti in "Properties".
**Delete** Cancella la entry corrente
**Clear Form** Azzera I parametri in "Properties" per l'inserimento di una nuova entry.
**Generate Report** Visualizza una lista completa e dettagliata.

## Security




### Security Firewall

**Enable DoS Firewall** Se abilitato gli attacchi di tipo DoS (Denial of Service) saranno intercettati e bloccati. Si raccomanda di lasciare questa opzione abilitata..

***Note:***

- Un attacco DoS non mira a penetrare le difese e carpire dati ma piuttosto a saturare la banda disponibile sulla connessione Internet rendendola di fatto inutilizzabile.
- Il dispositivo utilizza la tecnologia "Stateful Inspection" in grado di determinare quando singoli pacchetti TCP/IP possono essere validi ma in situazioni particolari e ben precise, questi rappresentano un DoS attack.

**Threshold** Questa impostazione interviene sul numero massimo di connessioni “half-open" accettate e permesse.

- Una connessione “half-open" si verifica quando un client remoto apre una sessione con il server senza poi proseguire a fronte delle richieste del server.
- Mentre il numero ottimale delle connessioni "half-open" permesse può dipendere da molti fattori, il fattore primario è la capacità di banda della vostra connessione Internet.
- Selezionare l’opzione che corrisponde alla vostra bada per la connessione Internet.

### Options

**Respond to ICMP** Il protocollo ICMP è utilizzato da programmi tipo "ping" e "traceroute", di monitor o discovery.

- Se selezionato il dispositivo risponderà a pacchetti ICMP provenienti da Internet.
- Se non selezionato il dispositivo non risponderà a pacchetti ICMP provenienti da Internet, ignorandoli e accrescendo la sicurezza.

**Allow IPsec** Il protocollo IPSec è largamente utilizzato per stabilire connessioni protette attraverso Internet dai programmi VPN (Virtual Private Networking).

- Se selezionato, le connessioni IPSec sono permesse.
- Se non selezionato, le connessioni IPSec non sono permesse

**Allow PPTP** Il protocollo PPTP è largamente utilizzato dai programmi VPN (Virtual Private Networking).

- Se selezionato, le connessioni PPTP sono permesse.
- Se non selezionato, le connessioni PPTP non sono permesse.

**Allow L2TP** Il protocollo L2TP è spesso utilizzato dai programmi VPN (Virtual Private Networking).

- Se selezionato, le connessioni L2TP sono permesse.
- Se non selezionato, le connessioni L2TP non sono permesse.

## Firmware Upgrade

Il firmware del dispositivo può essere aggiornato dal browser.
Scaricate sul PC il file di aggiornamento, poi selezionate Upgrade dal menu Advanced.


**Per effettuare un aggiornamento del firmware:**

1. Cliccate su "Browse".
2. Selezionate il file di aggiornamento.
3. Cliccate su "Start Upgrade" per iniziare l'aggiornamento.

***Durante l'aggiornamento il dispositivo non è operativo ed effettuerà un restart a fine procedura. Ogni connessione attiva sarà.***

## 2.9. COME CONFIGURARE LE STAZIONI DI RETE

### 2.9.1. CONFIGURAZIONE DEL TCP/IP

**Se utilizzate il servizio DHCP Server:**

- Configurate ogni computer come DHCP client, cioè per ottenere automaticamente un indirizzo IP dalla rete.

**Se sulla vostra rete é già presente un DHCP server:**

- Configurate il vostro DHCP server per assegnare alle stazioni l'indirizzo IP di FireGate Wave 54 come "Default Gateway" o "Router".
- Riportate il computer utilizzato per la configurazione al suo stato originale.

**Se sulla vostra rete é già presente uno o più Router:**

- Non modificate le impostazioni delle stazioni di rete
- Fate riferimento al capitolo Routing del manuale completo.

**Se sulla vostra utilizzate indirizzi IP statici:**

**Su tutte le stazioni di rete:**

- Inserite l'indirizzo IP di FireGate Wave 54 nel campo Default Gateway
- Inserite lo stesso indirizzo IP del DNS inserito nella configurazione di FireGate Wave 54 nel campo DNS.

### 2.9.2. IMPOSTAZIONI INTERNET

Ogni stazione di rete deve essere configurata per accedere ad Internet tramite la LAN (non attraverso una connessione modem).

**In Windows® 95/98/Me/2000/XP:**

- Dal menu di Avvio – Programmi – Accessori, (Comunicazioni) oppure Internet Explorer.
- Selezionate Connessione guidata (Internet Connection Wizard).
- Selezionate "rete locale (LAN)" quando richiesto.

***NOTA: Tutte le configurazioni che regolano il passaggio di dati tra WAN e LAN, hanno effetto anche sulla WLAN.***

### 2.9.3. ACCESSO INTERNET – LA NAVIGAZIONE

Una volta terminata la configurazione della stazione di rete per accedere ad Internet tramite la LAN, è sufficiente utilizzare il vostro browser per accedere ad un sito Internet, ad esempio www.digicom.it.

# 3. RISOLUZIONE DEI PROBLEMI

3

In questa sezione troverete le soluzioni ai problemi più comuni e le indicazioni per individuare le cause dei malfunzionamenti, nel caso si verificassero.

### Problema 1: Non riesco ad accedere alla configurazione del dispositivo

***Soluzione 1: Verificare che:***

- Il dispositivo sia accesso e le connessioni LAN siano corrette.
- Che il PC utilizzato abbia il protocollo di rete TCP/IP installato,e che sia associato alla scheda di rete. Se mancante cliccate su Aggiungi, protocollo, Microsoft, TCP/IP, OK. Potrebbe essere necessario riavviare il PC.
- Che il PC e il dispositivo siano connessi allo stesso segmento di rete.
- Che gli indirizzi IP siano corretti, come definiti nella parte di configurazione di questo manuale.

### Problema 2: Inserendo un indirizzo URL o indirizzo IP ricevo un errore di time out

***Soluzione 2: Verificate che le impostazioni TCP/IP del computer siano corrette (indirizzo IP, Default gateway e DNS).***

Effettuate un Ping verso il dispositivo. Da prompt di DOS digitare
Ping xxx.xxx.xxx.xxx
dove xxx.xxx.xxx.xxx è l'indirizzo IP del dispositivo.
In caso di risposta negativa verificare che il router sia connesso alla LAN e acceso. Se cos'è, il problema è dovuto alla rete LAN.
Nelle finestre di Status esaminate il log. Fate riferimento alla sezione Connection Log.
Verificate che il modem xDSL sia acceso e correttamente connesso.
Verificate le impostazioni "Proxy Server" del PC.
Il dispositivo non è un Proxy Server e il PC non necessità di un "Proxy Server" per utilizzarlo.
Se è presente un Proxy Server in LAN, disabilitatelo e disabilitate le impostazioni "Proxy Server" del PC.
Se il provider ha un Proxy Server seguite le istruzioni da esso fornite.

### Problema 3: Alcune applicazioni non funzionano correttamente quando utilizzano il dispositivo

***Soluzione 3: Il dispositivo processa i dati che lo attraversano e non è trasparente.***

La finestra Advanced Internet mette a disposizione alcune funzionalità per le applicazioni non standard:
Special Internet Applications
Exposed Computer
Utilizzare Special Internet Applications quando possibile.
Ricordare che ad ogni modo un solo utente alla volta può usare un'applicazione speciale.
Se non si riesce ad ottenere un buon funzionamento utilizzare la funzione Exposed Computer.

***Attenzione, questa funzione scavalca qualsiasi sicurezza ed espone la LAN ad accessi indiscriminati dall'esterno.***

digicom

21010 Cardano al Campo VA
via A. Volta 39