

# Michelangelo Office Pro V



Manuale Operativo  
rev. 1.0 06/2004

# Indice

<b>PREMESSA</b>	<b>4</b>
<b>CONDIZIONI AMBIENTALI</b>	<b>4</b>
<b>AVVERTENZE GENERALI</b>	<b>4</b>
<b>PULIZIA</b>	<b>4</b>
<b>VIBRAZIONI</b>	<b>4</b>
<b>DICHIARAZIONE CE DI CONFORMITÀ</b>	<b>4</b>
<b>1 INTRODUZIONE</b>	<b>5</b>
PREREQUISITI	5
CONTENUTO DELLA CONFEZIONE	5
<b>1.1 CARATTERISTICHE</b>	<b>6</b>
ADSL	6
LAN	6
WIRELESS (SOLO MODELLO WAVE)	6
FIREWALL	6
APPLICAZIONI AVANZATE	6
<b>1.2 DESCRIZIONE PORTE E LED</b>	<b>7</b>
<b>2 INSTALLAZIONE</b>	<b>8</b>
ALIMENTAZIONE	8
CONNESSIONE ADSL	8
CONNESSIONE LAN	8
<b>3 CONFIGURAZIONE</b>	<b>9</b>
<b>3.1 CONFIGURAZIONE DEL COMPUTER</b>	<b>9</b>
<b>3.2 CONFIGURAZIONE ROUTER</b>	<b>9</b>
3.2.1 REGOLE GENERALI DI CONFIGURAZIONE:	9
3.2.2 ACCESSO ALLA CONFIGURAZIONE DEL ROUTER	9
<b>3.3 CONFIGURATION – LAN</b>	<b>11</b>
3.3.1 ETHERNET	11
3.3.2 WIRELESS (SOLO MODELLO WAVE)	11
3.3.3 WIRELESS SECURITY (SOLO MODELLO WAVE)	12
3.3.4 WIRELESS (SOLO MODELLO WAVE) WEP	12
3.3.5 WIRELESS (SOLO MODELLO WAVE) WPA PRE-SHARED KEY	12
3.3.6 PORT SETTING	13
3.3.7 DHCP SERVER	13
DHCP SERVER MODE	13
<b>3.4 CONFIGURATION – WAN</b>	<b>16</b>
3.4.1 LINEA PPOA / PPPOE	16
3.4.2 LINEA RFC 1483 ROUTED CON 1 INDIRIZZO IP STATICO	17
3.4.3 LINEA RFC 1483 ROUTED CON PIÙ INDIRIZZI IP STATICI	17
3.4.4 DNS	18

3.4.5	ADSL	18
<b>3.5</b>	<b>CONFIGURATION SYSTEM</b>	<b>19</b>
3.5.1	TIMEZONE	19
3.5.2	REMOTE ACCESS	19
3.5.3	FIRMWARE UPGRADE	19
3.5.4	BACKUP/RESTORE	20
3.5.5	RESTART ROUTER	20
3.5.6	USER MANAGEMENT	21
<b>3.6</b>	<b>CONFIGURATION – FIREWALL</b>	<b>22</b>
3.6.1	GENERAL SETTINGS	22
3.6.2	PACKET FILTER	22
3.6.3	INTRUSION DETECTION	25
3.6.4	MAC ADDRESS FILTER	26
3.6.5	URL FILTER	26
3.6.6	FIREWALL LOG	28
<b>3.7</b>	<b>CONFIGURATION VPN</b>	<b>29</b>
3.7.1	VPN PPTP	29
3.7.2	VPN PPTP - REMOTE ACCESS	29
3.7.3	VPN PPTP - LAN TO LAN	30
3.7.4	VPN IPSEC	30
3.7.5	VPN L2TP	32
3.7.6	VPN L2TP - REMOTE ACCESS	32
3.7.7	VPN L2TP - LAN TO LAN	33
<b>3.8</b>	<b>CONFIGURATION – QOS</b>	<b>34</b>
3.8.1	PRIORITIZATION	34
3.8.2	IP THROTTLING	34
<b>3.9</b>	<b>CONFIGURATION – VIRTUAL SERVER</b>	<b>36</b>
<b>3.10</b>	<b>CONFIGURATION ADVANCED</b>	<b>37</b>
3.10.1	STATIC ROUTE	37
3.10.2	DYNAMIC DNS	37
3.10.3	CHECK EMAILS	37
3.10.4	DEVICE MANAGEMENT	38
3.10.5	SNMP ACCESS CONTROL	38
<b>3.11</b>	<b>STATUS</b>	<b>40</b>
3.11.1	STATUS – ARP TABLE	40
3.11.2	STATUS – DHCP TABLE	40
3.11.3	STATUS – PPTP STATUS, IPSEC STATUS, L2TP STATUS	40
3.11.4	STATUS – EMAIL STATUS	40
3.11.5	STATUS – EVENT LOG, ERROR LOG	40
<b>4</b>	<b>APPENDICE</b>	<b>41</b>
<b>4.1</b>	<b>PORTE TCP/UDP MAGGIORMENTE UTILIZZATE</b>	<b>41</b>
<b>4.2</b>	<b>ELENCO SERVER DNS</b>	<b>42</b>
<b>4.3</b>	<b>ACCESSO DA REMOTO CON VPN PPTP</b>	<b>44</b>

## 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 è 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 da -5 a +45°C

Umidità relativa 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

---

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

## VIBRAZIONI

---

Attenzione a non causare vibrazioni o urti.

## Dichiarazione CE di conformità

---

# 1 INTRODUZIONE

---

## ***Gentile Cliente,***

la ringraziamo per la fiducia accordataci nell'acquistare un prodotto Digicom.

Michelangelo Office Pro V riunisce in un unico dispositivo tutte le funzionalità e le caratteristiche necessarie a realizzare un efficiente accesso ad Internet via ADSL, fornendo nel contempo la protezione della rete LAN locale da attacchi provenienti dal mondo esterno, tramite un firewall integrato.

Il supporto VPN (Virtual Private Network) offre la possibilità di fornire l'accesso alla rete LAN locale anche ad utenti remoti (client o LAN) in modo sicuro e protetto da crittografia dei dati.

Il modello Michelangelo Office **Wave** Pro V integra inoltre un Access Point Wireless 802.11b, permettendo di estendere la rete locale anche ad utenti Wireless.

## **Prerequisiti**

- Computer con schede di rete Ethernet 10/100 Mbps o wireless 802.11b
- Protocollo TCP/IP installato su ogni macchina
- Cavi di rete dritti, connettori RJ45 su entrambe le estremità
- Linea ADSL su linea analogica, connettore RJ11
- Abbonamento ADSL singolo utente o multiutente stipulato con un ISP
- Dati relativi all'abbonamento

## **Contenuto della confezione**

- 1 Michelangelo Office Pro V o Michelangelo Office Pro Wave V
- 1 Alimentatore
- 1 CD-ROM completo di manuali
- Manuale di configurazione rapida
- 1 cavo RJ45-RJ45 dritto
- 1 cavo di linea RJ11-RJ11

## 1.1 CARATTERISTICHE

---

### ADSL

- Velocità dati asimmetrica
- Velocità massima Ricezione (downstream) : 8Mbit/s
- Velocità massima Trasmissione (upstream) : 1Mbit/s
- Standard ADSL:
  - ANSI T1.413 Issue 2
  - ITU G.922.1 (G.dmt)
  - ITU G.992.2 (G.lite)
- Protocolli Supportati :
  - RFC 2364 (PPP over ATM)
  - RFC 2516 (PPP over Ethernet)
  - RFC 1483 (Bridged e Routed Ethernet over ATM)
- Supporto ATM UNI3.1/4.0 PVC, ATMSAR, ATM AAL5 e OAM F5
- Interfaccia WAN ADSL: Connettore RJ11

### LAN

- Switch 4 porte 10/100 Mbit/s
- Funzione MDI / MDI-X su tutte le 4 porte
- Supporto IP Alias (2 indirizzi IP di LAN)
- DHCP Server e Relay

### WIRELESS (solo modello Wave)

- Access Point wireless 802.11b
- Supporto crittografia dei dati WEP 64 e 128bit
- Supporto crittografia WPA-PSK (Pre Shared Key)
- Supporto funzione Hide SSID

### FIREWALL

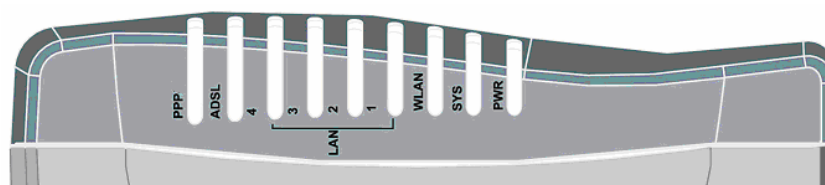
- Protocollo NAT
- Protezione Packet Filter
- Protezione MAC Address Filter
- Protezione URL Filter
- Intrusion Detection (Protezione da attacchi tipici, Denial of Service e Scan)

### APPLICAZIONI AVANZATE

- Client e Server VPN con protocollo PPTP e IPSEC
- QoS – Quality of Service Lan → Wan
- Esportazione servizi (Virtual Server)
- Supporto DMZ
- Dynamic DNS
- Check Emails

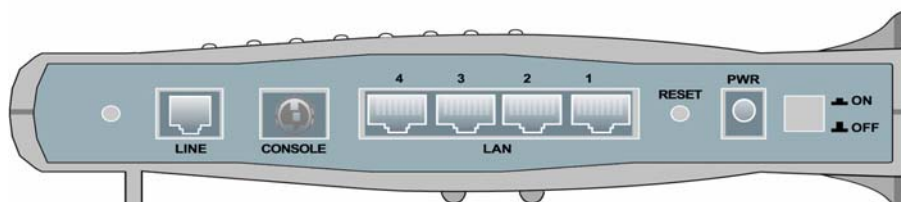
## 1.2 DESCRIZIONE PORTE E LED

### Descrizione Led



LED	Descrizione
<b>PPP</b>	Lampeggiante durante la negoziazione di una connessione PPPoA/PPPoE. Accesso a connessione avvenuta con successo.
<b>ADSL</b>	Lampeggiante durante la fase di training della linea ADSL. Acceso quando la sincronizzazione del livello fisico ADSL è avvenuta con successo.
<b>LAN 1—4</b>	Accesso quando la corrispondente porta Ethernet è connessa ad un dispositivo di rete LAN. Verde: 100Mbps, Arancio: 10Mbps. Lampeggiante quando dei dati sono trasmessi o ricevuti sulla corrispondente porta Ethernet.
<b>WLAN</b>	Accesso quando avviene una connessione wireless (WLAN). Flashes when sending/receiving data. Lampeggiante quando dei dati sono trasmessi o ricevuti sulla sezione wireless.
<b>SYS</b>	Lampeggiante durante la fase di start-up del dispositivo Accesso al termine della fase di start-up.
<b>PWR</b>	Accesso quando il dispositivo è alimentato.

### Descrizione Porte



	Descrizione
Interruttore ON OFF	Interruttore di accensione del dispositivo
<b>PWR</b>	Connettore per l'alimentatore. Nota: Utilizzare solamente l'alimentatore fornito nella confezione, pena il possibile danneggiamento del dispositivo e conseguente invalidazione delle condizioni di garanzia.
<b>RESET</b>	Pulsante di reset. Una volta acceso il dispositivo, premere il pulsante di reset per: - da 0 a 3 secondi: effettuare un reset del dispositivo. - più di 6 secondi above: ripristinare le impostazioni di fabbrica del dispositivo (inclusa la password di accesso alla configurazione)
<b>LAN 1—4</b>	Porta UTP RJ45 per la connessione di computer o altri dispositivi di rete LAN. Tutte le porte sono Autosensing 10/ 100Mbps e Auto MDI/MDI-X.
<b>CONSOLE</b>	Porta di console locale. Utilizzare il cavo PS2/RS-232 fornito nella confezione per accedere alla console. Vedi apposito manuale.
<b>LINE</b>	Connettore RJ-11 per la connessione della linea ADSL.

## 2 INSTALLAZIONE

---

### **Alimentazione**

Alimentate il Router utilizzando l'alimentatore fornito nella confezione quindi accendete il dispositivo tramite l'apposito interruttore di accensione **Power Switch**.

### **Connessione ADSL**

Collegate la linea ADSL al connettore **LINE** presente nel pannello posteriore.

### **Connessione LAN**

Collegate i Computer della vostra LAN (fino a quattro) direttamente al Router ad una delle porte LAN presenti nel pannello posteriore.

Se disponete di una rete LAN pre-esistente, collegate una delle porte LAN del router ad una porta del vostro HUB o Switch di rete LAN, tramite un cavo RJ45-RJ45 diritto (funzionalità MDI/MDI-X automatica effettuata dal router)

## 3 CONFIGURAZIONE

---

Per poter effettuare la configurazione del Router è necessario disporre di tutti i dati relativi al Vostro abbonamento ADSL. Questi dati vi devono essere forniti dal provider Internet con il quale avete stipulato il contratto di accesso ad Internet su ADSL.

I parametri richiesti solitamente sono:

- VPI / VCI (normalmente 8 / 35)
- Tipo di protocollo (PPP over ATM, PPP over Ethernet, RFC 1483.....)
- Indirizzi IP dei DNS utilizzati dal provider
- Username e Password oppure IP assegnati.

### 3.1 CONFIGURAZIONE DEL COMPUTER

---

Per accedere alla configurazione del router è indispensabile che il computer utilizzi il protocollo TCP/IP e che disponga di un comune Browser grafico (Explorer, Netscape, Opera ...).

Le impostazioni di fabbrica (default) del router sono:

**Indirizzo IP:** 192.168.1.254  
**Subnet Mask:** 255.255.255.0  
**DHCP Server:** Abilitato

Per accedere alla configurazione quindi occorre impostare sul computer un indirizzo IP della stessa rete del router; potete impostare l'indirizzo in modo statico oppure utilizzare l'assegnamento con DHCP Server.

#### Windows® XP

Dal menù **Start** selezionate -> **Pannello di Controllo** -> **Rete e Connessioni Internet** , **Risorse di rete** e selezionate **Visualizza risorse di rete**.

Selezionate **Connessione alla rete locale (LAN)** e visualizzate le Proprietà, selezionate **Protocollo Internet (TCP/IP)** e premete sul pulsante **Proprietà**.

Se volete utilizzare un indirizzo IP Statico inserite un indirizzo 192.168.1.x (con x compreso tra 1 e 253), Subnet Mask 255.255.255.0 e gateway 192.168.1.254

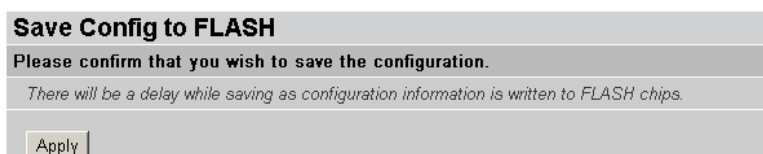
Se volete utilizzare un DHCP Server, impostate “**ottieni automaticamente un indirizzo IP**”.

### 3.2 CONFIGURAZIONE ROUTER

---

#### 3.2.1 Regole generali di configurazione:

1. Il PC dal quale eseguite la configurazione del Router deve essere privo di software proxy o firewall. Se utilizzate dei programmi di proxy, firewall o similari, disattivateli temporaneamente per poter effettuare la configurazione del Router.
2. In ogni finestra di configurazione premete **Apply** per attivare le impostazioni; le modifiche hanno effetto immediato.
3. Per salvare le impostazioni in modo definitivo (in modo che rimangano attive anche dopo uno spegnimento del router) selezionate l'opzione **Save Config to FLASH** e successivamente **Apply**.



#### 3.2.2 Accesso alla configurazione del Router

Aprire il vostro Browser e verificate che non sia impostato per utilizzare un proxy.

Digitate l'URL <http://192.168.1.254>

Nota: 192.168.1.254 è l'indirizzo IP di fabbrica del router



Vi verrà richiesto di autenticarvi per poter accedere alla configurazione del Router:



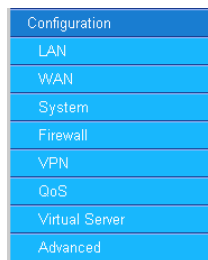
Inserite:

**Nome utente:** admin

**Password:** admin

Nota: admin è la username e password di fabbrica del router. Vi consigliamo di modificarle successivamente, una volta terminata la configurazione, per motivi di sicurezza.

Selezionate la voce **Configuration** per configurare tutte le funzionalità del dispositivo:



## 3.3 Configuration – LAN

### 3.3.1 Ethernet

Ethernet				
<b>Primary IP Address</b>				
IP Address	192	168	1	254
SubNetmask	255	255	255	0
RIP	<input type="checkbox"/> RIP v1 <input type="checkbox"/> RIP v2 <input type="checkbox"/> RIP v2 Multicast			
<b>Secondary IP Address</b>				
The Secondary IP Address should be on the same subnet as the Primary IP Address and uses the same Subnet Mask.				
IP Address	0	0	0	0
<input type="button" value="Apply"/>				

Michelangelo Office (Wave) Pro V è in grado di gestire 2 differenti indirizzi IP di LAN. Utilizzando questa funzionalità è possibile fornire accesso ad Internet a 2 reti distinte allo stesso tempo. Nel caso intendiate utilizzare un unico indirizzo di rete LAN, impostatelo con la relativa Subnet Mask in **Primary IP Address**.

Entrambi gli indirizzi IP sono utilizzabili tramite connessione Ethernet o Wireless.

Abilitate, se necessario l’invio e ricezione di pacchetti **RIP** versione 1, 2 ed il supporto Multicast.

Selezionate **Apply** per attivare le impostazioni effettuate

### 3.3.2 Wireless (solo modello Wave)

Nella finestra Wireless è possibile impostare i parametri di funzionamento per la sezione Wireless LAN.

Wireless	
<b>Parameters</b>	
WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	wlan-ap
ESSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Regulation Domain	Europe
Channel ID	Channel 1 (2.412 GHz)
Reset	false
Connected	true
Card Type	Prism 3
AP Firmware Version	2.0.5
Primary Firmware Version	1.1.1
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**WLAN Service:** Abilita o disabilita la funzionalità wireless.

**ESSID:** inserite una stringa alfanumerica, che identificherà il nome della vostra rete wireless. Lo stesso nome deve essere impostato in ogni client che dovrà accedere a questa rete WLAN. Per usufruire delle funzionalità di roaming 802.11b, lo stesso ESSID deve essere impostato anche negli altri Access Point.

**ESSID Broadcast:** Normalmente un client wireless può effettuare una ricerca degli access point disponibili nel suo raggio di azione. Disabilitando la funzione ESSID Broadcast, MICHELANGELO WAVE PRO V “nasconde” l’ESSID della rete wireless, impedendo ai Client di rilevare la sua presenza tramite una semplice ricerca (Site survey). I client dovranno conoscere (ed aver configurato) a priori il nome della rete (ESSID) per potersi collegare. Questa opzione di sicurezza permette di proteggere la rete da eventuali “sniffing” e attacchi indiscriminati.

**Regulation Domain:** Definisce il range di frequenze e canali ammessi in nel paese o continente in cui si utilizza il dispositivo. Selezionate *Europe* per abilitare solo l’utilizzo dei canali permessi in Italia.

**Channel ID:** Selezionate il canale da utilizzare, utilizzate un canale libero (non utilizzato da altri access point nelle vicinanze). Se sono attivi altri dispositivi Wireless, mantenete 5 canali “di distanza” da quelli già utilizzati.

**Reset:** Effettua un reset della connessione wireless, forza una temporanea sconnessione di tutti i client wireless.

### 3.3.3 Wireless Security (solo modello Wave)

In questa finestra è possibile abilitare la crittografia per proteggere l’accesso alla rete Wireless.

Selezionate da **Security Mode** il tipo di crittografia desiderato:

**Disable:** disabilita la crittografia

**WEP:** abilita la crittografia a 64 o 128bit.

**WPA Pre Shared Key:** abilita il nuovo standard di crittografia WPA.

### 3.3.4 Wireless (solo modello Wave) WEP

The screenshot shows the 'Wireless Security' configuration window. It has a title bar 'Wireless Security' and a 'Parameters' section. The 'Security Mode' is set to 'WEP'. Under 'WEP Encryption', 'WEP64' is selected with a radio button, and 'Hex' is selected in the dropdown menu. There is a 'Passphrase' field with a 'Generate' button next to it. Below that is the 'Default Used WEP Key' field, set to '0' with a '(0~3)' label. There are four rows for 'Key 0', 'Key 1', 'Key 2', and 'Key 3', each with a text input field containing '00-00-00-00-00'. At the bottom, there are 'Apply' and 'Cancel' buttons.

**WEP Encryption:** In questo campo è possibile selezionare il tipo di crittografia WEP; le Key possono essere a 64bit oppure 128bit e possono essere scritte in codice ASCII oppure esadecimale (HEX).

**Passphrase:** Questo campo può essere utilizzato per generare le 4 key WEP automaticamente, inserendo una stringa di testo; L’algoritmo che genera le Key è standard pertanto è sufficiente inserire la stessa stringa di testo anche negli altri dispositivi che dovranno collegarsi al Michelangelo Office Pro Wave V (se dispongono di questa funzione).

**Default Used WEP Key:** Indica il numero della Key (chiave WEP) da utilizzare se si abilita la crittografia WEP. Le chiavi disponibili sono le 4, da Key 0 a Key 3.

**Key (0~3):** In questo campo potete inserire le Key per la WEP encryption.

**Codifica HEX (esadecimale):** la KEY è composta da 5 coppie di caratteri (WEP 64bit) oppure da 13 coppie di caratteri (WEP 128bit), separate da separate “-”, ad esempio **0a-1b-2c-3d-4e**

**Codifica ASCII:** La KEY è composta da 5 caratteri (WEP 64bit) oppure 13 caratteri (WEP 128bit). I caratteri devono essere inseriti senza spazi o caratteri di separazione, ad esempio **p1A9a** per una KEY 64bit ASCII. Attenzione: la KEY ASCII è ‘case sensitive’, pertanto una ‘A’ è considerata differente dalla ‘a’.

### 3.3.5 Wireless (solo modello Wave) WPA Pre-Shared Key

Wireless Security	
Parameters	
Security Mode	WPA Pre-Shared Key
WPA Algorithms	TKIP
WPA Shared Key	<input type="text"/>
Group Key Renewal	600 seconds
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**WPA Shared Key:** Inserite in questo campo una stringa di testo con un minimo di 8 caratteri e un massimo di 63 caratteri.

**Group Key Renewal:** Inserite il numero di secondi prima del cambio automatico della chiave di crittografia. (il cambio avviene in modo automatico secondo l' algoritmo TKIP).

### 3.3.6 Port Setting

Questo menu permette di impostare i parametri di funzionamento delle porte LAN.

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

#### Port (1-4) Connection Type:

Ogni porta Ethernet può essere singolarmente configurata per operare in automatico, velocità fissa 10 o 100Mbit, Half o Full duplex.

Utilizzare l'impostazione 'auto' a meno che non si debba forzare la velocità o modalità di funzionamento per apparati non in grado di negoziarla correttamente.

#### IPv4 TOS priority Control:

Abilita il controllo del byte di TOS e delle priorità in esso impostate nel pacchetto IP.

### 3.3.7 DHCP Server

Questo menu permette di impostare i parametri relativi al servizio DHCP

DHCP Server	
Configuration	
DHCP Server Mode	<input type="radio"/> Disable <input checked="" type="radio"/> DHCP Server <input type="radio"/> DHCP Relay Agent
<input type="button" value="Next"/>	

#### DHCP Server Mode

**Disable:** Disabilita il DHCP Server.

**DHCP Server :** Abilita il DHCP Server interno del router.

**DHCP relay agent:** permette l'utilizzo di Server DHCP già presenti in rete. Le richieste DHCP che perverranno al router verranno reindirizzate al DHCP di rete impostato.

Selezionando NEXT è possibile modificare le impostazioni del server DHCP.

DHCP	
DHCP Server	
Allow Bootp	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Allow Unknown Clients	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Use Default Range	<input type="checkbox"/>
Starting IP Address	192.168.1.100
Ending IP Address	192.168.1.199
Default Lease Time	43200 seconds
Maximum Lease Time	86400 seconds
Use Router as DNS Server	<input checked="" type="checkbox"/>
Primary DNS Server Address	0.0.0.0
Secondary DNS Server Address	0.0.0.0
Use Router as Default Gateway	<input checked="" type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Fixed Host"/>	

Il DHCP Server può essere attivato solamente sul **Primary IP Address**.

**Allow Bootp:** se abilitato assegna l'indirizzo IP anche ai client che utilizzano il bootp

**Allow Unknown Client:** se abilitato assegna un indirizzo IP a tutti i client che ne fanno richiesta. Se disabilitato solo i client inseriti in **Fixed Host** potranno ricevere un indirizzo IP.

**Use Default Range:** imposta automaticamente il range utilizzando i primi 20 indirizzi della rete.

**Starting-Ending IP Address:** definiscono un range di indirizzi IP (inizio – fine) che il DHCP server può allocare ai vari client.

**Lease Time:** imposta il tempo di default e il tempo massimo di validità di un indirizzo IP, una volta assegnato tramite DHCP server. Non modificate questi valori se non avete esigenze particolari.

**Use Router as DNS Server:** assegna l'indirizzo IP del router come server DNS.

Il Router dovrà avere impostati gli indirizzi DNS nella apposita finestra di configurazione della sezione WAN per poter operare come DNS Proxy.

**Primary / Secondary DNS Server Address:** Se il DHCP server deve assegnare degli indirizzi di DNS prefissati, inseriteli in questi campi e disabilitate la funzione "Use Router as DNS Server Address".

**Use Router as Default Gateway:** assegna l'indirizzo IP del router come Gateway.

Disabilitate questa funzione solamente se volete fornire accesso alla rete LAN ai client DHCP senza permettere loro la navigazione.

E' possibile assegnare sempre lo stesso indirizzo IP ad una determinata macchina, creando degli IP riservati, tramite il menu **FixedHost**.

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

**Name:** Inserite un nome mnemonico per la macchina

**IP Address:** Inserite l'indirizzo IP che volete assegnare alla macchina.

**MAC Address:** Inserite l'indirizzo MAC della scheda di rete che identifica la macchina.

**Maximum Lease Time:** Tempo di validità dell'indirizzo IP assegnato.

Una volta creato un FixedHost è possibile visualizzare l'elenco degli host configurati:

Fixed Host					
Host Table					
Name	IP Address	MAC Address	Maximum Lease Time		
Aministrator	192.168.1.62	00:06:7b:03:07:79	86400	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>					

**Edit:** permette la modifica dell'Host

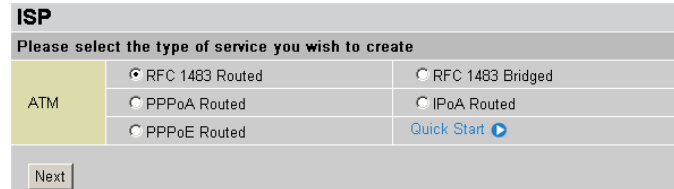
**Delete:** **cancella l'Host**

**Create:** visualizza la finestra 'FixedHost Create' per aggiungere un nuovo Host.

## 3.4 Configuration – WAN

In questo menu è possibile inserire i parametri di accesso alla linea ADSL,

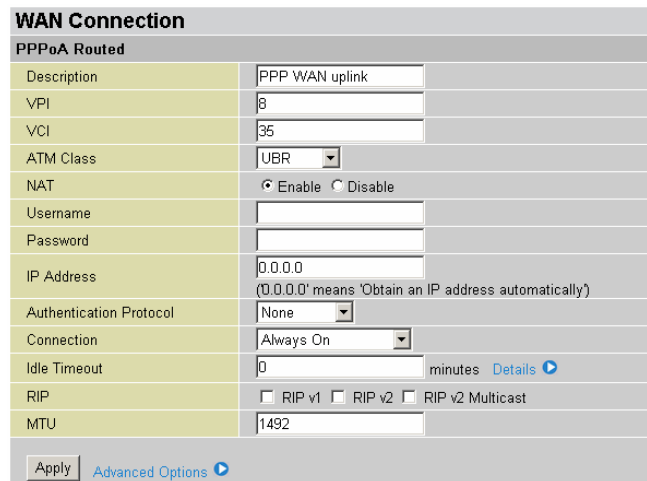
Nella sezione **ISP** (Internet Service Provider) selezionare il tipo di protocollo utilizzato dalla linea Adsl .



### 3.4.1 Linea PPPoA / PPPoE

Le linee con indirizzo IP dinamico utilizzano il protocollo PPPoA, oppure il protocollo PPPoE (quest'ultimo generalmente solo su richiesta). Questo tipo di linee prevedono un'autenticazione tramite un nome utente ed una password.

Selezionate **PPPoA router** se disponete di questo tipo di linea, selezionate **Next**:



**VPI e VCI:** se non diversamente indicati nel contratto di attivazione della linea Adsl, inserite rispettivamente **8** e **35** come nell'esempio.

**ATM Class:** Lasciate impostato UBR; impostate un altro valore solo se espressamente richiesto dal vostro Provider Adsl.

**NAT:** Impostate **Enable**

**Username e Password:** Inserite Username e Password forniti dal provider per la connessione alla linea Adsl.

**IP address:** lasciate 0.0.0.0 per utilizzare l'indirizzo IP dinamico che vi verrà assegnato dal provider al momento della connessione.

**Authentication Protocol:** selezionate **Chap(Auto)**

**Connection:** selezionate **Always On**

**Idle Timeout (in minutes):** impostate 0 per non forzare mai la disconnessione da Internet.

Se la linea è di tipo PPPoE selezionate **PPPoE router** e premete **Next**:

WAN Connection	
<b>PPPoE Routed</b>	
Description	PPPoE Routed
VPI	8
VCI	35
ATM Class	UBR
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	nome utente
Password	••••••••
Service Name	
IP Address	0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')
Authentication Protocol	Chap(Auto)
Connection	Always On
Idle Timeout	0 minutes
RIP	<input type="checkbox"/> RIP v1 <input type="checkbox"/> RIP v2 <input type="checkbox"/> RIP v2 Multicast
MTU	1492
Apply	

I parametri da impostare sono equivalenti a quelli descritti per la linea PPPoA.  
Nel campo Service name non inserite nulla, se non espressamente richiesto dal provider.

### 3.4.2 Linea RFC 1483 Routed con 1 indirizzo IP statico

Le linee con indirizzo IP statico generalmente utilizzano il protocollo RFC 1483 Routed con incapsulamento LLC.

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

**VPI e VCI:** se non diversamente indicati nel contratto di attivazione della linea Adsl, inserite rispettivamente **8** e **35** come nell'esempio.

**NAT:** Impostate **Enable**

**Encapsulation method:** selezionate **LLC Routed**

Selezionate l'opzione **Use the following IP address.**

Inserite in **IP Address** l'indirizzo IP che vi è stato assegnato dal provider.

Inserite in **Netmask** la Subnet Mask che vi è stata indicata dal provider

Inserite in **Gateway** l'indirizzo IP del Gateway che vi è stato assegnato dal provider.

### 3.4.3 Linea RFC 1483 Routed con più indirizzi IP statici

La configurazione del router è equivalente a quella per la linea ad un singolo indirizzo IP statico.

Per poter effettivamente utilizzare gli indirizzi IP pubblici che vi sono stati assegnati, dovrete disabilitare il NAT (**NAT: Disable**) e configurare il primo indirizzo IP utile del vostro range sull'interfaccia di LAN del router.

Tutte le macchine che dovranno lavorare con indirizzi IP pubblici dovranno essere configurate nel seguente modo:

IP: uno degli IP pubblici

Subnet Mask: la Subnet associata ai vostri indirizzi pubblici.

Gateway: l'indirizzo pubblico assegnato al router (sulla LAN)

DNS: Gli indirizzi dei DNS forniti dal provider.

### 3.4.4 DNS

I DNS sono fondamentali per la risoluzione dei nomi, pertanto è necessario che ogni macchina conosca gli indirizzi IP dei DNS.

Se non utilizzate il DHCP server dovete inserire manualmente gli indirizzi dei DNS nelle proprietà della scheda di rete di ogni PC. Avete due opzioni:

1. Inserite nella configurazione dei DNS di ogni PC quelli che vi ha fornito il provider.
2. Inserite nella configurazione dei DNS di ogni PC l'indirizzo IP di LAN del router ed inserite gli indirizzi IP dei DNS forniti dal provider nella finestra di configurazione WAN-DNS del router.

Nel secondo caso, ogni richiesta di risoluzione DNS verrà inviata al router che, grazie alla funzionalità di **DNS Proxy**, è in grado provvedere autonomamente alla risoluzione degli indirizzi.

DNS	
Parameters	
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

L'inserimento dei DNS in questa finestra è necessario anche per poter utilizzare correttamente il servizio di **Dynamic DNS**.

### 3.4.5 ADSL

In questa finestra di configurazione è possibile modificare alcune impostazioni relative alla collegamento con la linea ADSL.

ADSL	
Parameters	
Connect Mode	Multimode
Activate Line	true
Coding Gain	auto
Tx Attenuation	0
DSP FirmwareVersion	A.27.4.1
Connected	false
Operational Mode	Inactive
Annex Type	AnnexA
Upstream	0
Downstream	0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

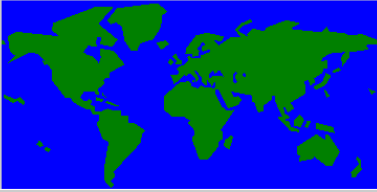
Non effettuate modifiche in questa pagina di configurazione, lasciate invariati i parametri come mostrati nell'immagine. Effettuate modifiche solo a fronte di un'esplicita richiesta del vostro provider o del supporto tecnico Digicom.

## 3.5 Configuration System

Questi menu permettono la configurazione dei parametri di sistema del router

### 3.5.1 TimeZone

Time Zone	
<b>Parameters</b>	
Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time Zone List	<input checked="" type="radio"/> By City <input type="radio"/> By Time Difference
Local Time Zone (+GMT Time)	(GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
SNTP Server IP Address	carl.css.gov time.nist.gov india.colorado.edu time-b.nist.gov
Daylight Saving	<input checked="" type="checkbox"/> Automatic
Resync Period	1440 minutes



Apply Cancel

Il router è in grado di regolare automaticamente l'ora, sfruttando i server SNTP pubblici disponibili in Internet.

**Time Zone:** Enable, abilita il servizio.

Selezionate il fuso orario corretto in **Local Time Zone**.

**Daylight Saving:** Abilitate questa funzione per gestire automaticamente il passaggio tra ora solare e legale.

### 3.5.2 Remote Access

Remote Access	
You may temporarily permit remote administration of this network device	
Allow Access for	30 minutes.
Enable	

Premendo **Enable** sarà possibile accedere alla configurazione del router da remoto, collegandosi all'indirizzo IP di WAN del router, per il tempo massimo impostato.

Eseguite un **Logout** prima di chiudere il Browser.

L'accesso è limitato nel tempo, se volete accedere liberamente al router per la configurazione in modo sicuro, create un profilo VPN PPTP per l'accesso alla LAN e quindi alla configurazione del Router.

### 3.5.3 Firmware Upgrade

Permette di aggiornare il firmware del dispositivo.

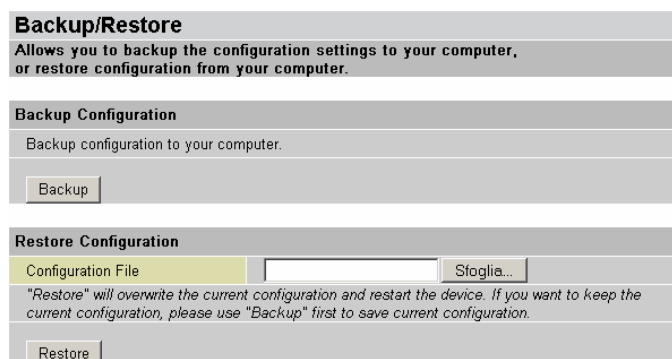
Firmware Upgrade	
You may upgrade the system software on your network device	
New Firmware Image	<input type="text"/> Sfoglia...
Upgrade	

Selezionate **Sfoglia** per indicare il file di aggiornamento e **Upgrade** per iniziare la procedura.

**Non tentare di effettuare un aggiornamento del firmware senza le adeguate istruzioni e i file forniti dal costruttore.**

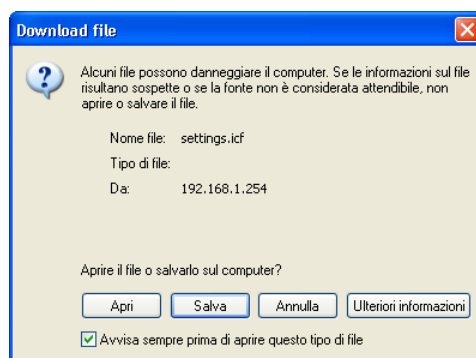
### 3.5.4 Backup/Restore

In questa finestra è possibile salvare la configurazione corrente del router per poterla poi ripristinare in un secondo momento.



### SALVATAGGIO CONFIGURAZIONE

Premete **Backup**



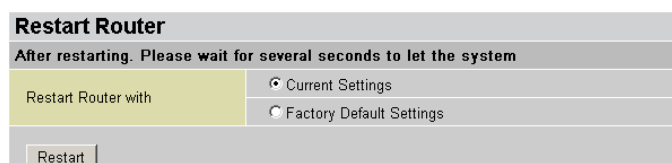
selezionate **Salva** per salvare il file di configurazione in una cartella sul vostro PC.

### RIPRISTINO CONFIGURAZIONE

Premete **Sfoggia** ed indicate il file di configurazione che avete salvato sul PC.

Premete **Restore** per caricare la nuova configurazione.

### 3.5.5 Restart Router



Al termine di tutte le configurazioni è consigliabile effettuare un “riavvio” del router.

Premete **Restart Router** per riavviare il dispositivo.

Se selezionate la voce **Reset to factory default settings** il router tornerà alla configurazione di fabbrica, **cancellando tutte le impostazioni** e dovrà poi essere riconfigurato.

Dopo un **Reset to factory default settings**, i parametri di accesso alla configurazione saranno:

indirizzo IP: 192.168.1.254

username: **admin**

password: **admin**

### 3.5.6 User Management

User Management				
Current Defined Users				
Valid	User	Comment		
true	<i>admin</i>	Default admin user	<a href="#">Edit</a>	

[Create](#)

In questa finestra è possibile modificare la password dell'amministratore del router e creare nuovi utenti in grado di accedere alla configurazione.

## 3.6 Configuration – Firewall

Il Firewall integrato sfrutta le tecniche di stateful packet inspection e packet filtering per fornire due diversi tipi di funzionalità:

1. Firewall: previene gli accessi non autorizzati da internet, con tre livelli di sicurezza:
  - NAT: nasconde gli indirizzi della rete privata LAN all'esterno rendendo difficile l'identificazione di una macchina privata ad un malintenzionato esterno.
  - Firewall Security and Policy: è possibile abilitare o bloccare il passaggio di particolari protocolli in Ingresso.
  - Intrusion Detection: previene o rileva un attacco proveniente dall'esterno.
2. Access Control: previene accessi Internet non autorizzati dalla rete LAN tramite:
  - Firewall Security and Policy: è possibile abilitare o bloccare il passaggio di particolari protocolli in Uscita.
  - MAC Filter rules: abilita o disabilita il passaggio di determinate stazioni in modo univoco (tramite l'indirizzo fisico della scheda di rete)
  - URL Filter: blocca l'accesso ad alcuni siti web, eventualmente in base ad orari prestabiliti.

### 3.6.1 General Settings

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

**Security:** Enable, abilita tutte le funzionalità del firewall.

**Policy:** Impostate “All blocked/user profile” per creare delle regole personalizzate. In alternativa potete selezionare “Low” o “Medium” o “High” per attivare alcuni profili già preconfigurati.

**Block WAN Request:** Se abilitato blocca tutte le richieste in arrivo al firewall da Internet.

### Una volta abilitato il firewall, TUTTI i pacchetti in ingresso o uscita verranno bloccati

Sarà necessario impostare delle regole per abilitare il passaggio dei pacchetti desiderati.

La selezione della Firewall Policy influenza solamente la configurazione del menù **Packet Filter**  
Per comprendere la creazione delle regole, trovate nell'APPENDICE DEL MANUALE l'elenco delle principali porte utilizzate (l'elenco completo è disponibile alla pagina Internet <http://www.iana.org/assignments/port-numbers>).

### 3.6.2 Packet Filter

Packet Filter		
Firewall Security		
Type	Configuration	Note
external < > internal	<a href="#">Port Filters</a> <input type="button" value="▶"/> <a href="#">Address Filters</a> <input type="button" value="▶"/>	1. By default, all protocol types and TCP/UDP ports are blocked. 2. Only the listed IP addresses are blocked

I filtri applicabili sui pacchetti che attraversano il firewall possono essere configurati in due modi differenti: in base alle porte utilizzate **Port Filters** e in base agli indirizzi IP interessati **Address Filters**.

## Port Filters

Questo menu visualizza l'elenco delle regole già impostate

Port Filters						
Filtering Rules						
<a href="#">Add TCP/UDP Filter</a>		<a href="#">Add Raw IP Filter</a>		<a href="#">Return</a>		
Filtering Table						
Type	Start Port	End Port	Inbound	Outbound		
TCP	80	80	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
UDP	53	53	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
TCP	53	53	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
TCP	21	21	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
TCP	23	23	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
TCP	25	25	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
TCP	110	110	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
TCP	119	119	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
UDP	7070	7070	Allow	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
ICMP	N/A	N/A	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
TCP	1720	1720	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
TCP	1503	1503	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
TCP	22	22	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
UDP	123	123	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>
TCP	443	443	Block	Allow	<a href="#">Edit</a>	<a href="#">Delete</a>

La tabella mostra l'elenco delle regole attive.

Analizziamo come esempio la prima regola:

**Type TCP** : regola abilitata per pacchetti TCP

**Start Port – End Port 80** : regola abilitata per pacchetti che hanno come destinazione la porta 80 (oppure nel caso in cui 'start' e 'end' abbiano numeri differenti, la regola interessa tutte le porta all'interno del range definito)

**Inbound Block** : I pacchetti TCP in arrivo da internet e destinati alla porta 80 vengono bloccati.

**Outbound Allow** : I pacchetti TCP in uscita verso Internet e destinati alla porta 80 vengono lasciati passare.

Questa regola quindi permette la navigazione WEB, essendo il protocollo HTTP associato alla porta 80.

Selezionando **Edit** è possibile modificare una regola

Selezionando **Delete** è possibile rimuovere una regola .

Per aggiungere nuovi filtri sono disponibili le seguenti funzioni:

### Add TCP/UDP filter

Port Filters		
Add TCP/UDP Filter		
Transport	Type	TCP
Port Range	Start Port	
	End Port	
Direction	Inbound	Allow
	Outbound	Allow
<input type="button" value="Apply"/> <a href="#">Return</a>		

Selezionate il tipo di pacchetto, **TCP, UDP**  
 Inserite il range di porte (inizio – fine) che volete controllare con questa regola in **Start Port / End Port**.  
 Selezionate i permessi in ingresso ed in uscita.  
 Selezionate **Apply** per aggiungere la regola.

### Add RAW IP filter

Port Filters		
Add Raw IP Filter		
Protocol Number		
Direction	Inbound	Allow
	Outbound	Allow
<input type="button" value="Apply"/> <a href="#">Return</a>		

Questo filtro offre la possibilità di controllare direttamente un protocollo.  
 Inserite il numero del protocollo da filtrare in **Protocol Number** e selezionate i permessi in ingresso e uscita.  
 Selezionate **Apply** per aggiungere la regola.

I principali protocolli sono:

- 1 ICMP
- 2 IGMP
- 4 IP
- 6 TCP
- 17 UDP
- 47 GRE
- 50 IPSEC ESP
- 51 IPSEC AH

L'elenco dei protocolli definito dall' RFC 1700 è disponibile nell'APPENDICE DEL MANUALE

### Address Filters

Questa tipologia di filtro, blocca tutto il traffico in ingresso o uscita (o in entrambi i sensi) di un indirizzo IP o di un gruppo di indirizzi.

Address Filters	
Filtering Rules	
<a href="#">Add Address Filter</a>	<a href="#">Return</a>
Filtering Table	
No Address Filter Defined	

Cliccate su **Add Address Filter** per aggiungere una nuova regola:

Address Filters	
Add Address Filter	
Host IP Address	
Host Subnet Mask	
Direction	outbound
<input type="button" value="Apply"/> <a href="#">Return</a>	

**Host IP Address:** Inserite l'indirizzo IP che volete filtrare.

**Host Subnet Mask:** Inserite la Subnet Mask associata all'indirizzo all'indirizzo o al gruppo di indirizzi che vogliamo filtrare

**Direction:**

**Inbound**-> Blocca tutto il traffico in ingresso.

**Outbound**-> Blocca tutto il traffico in uscita.

**Both**-> Blocca tutto il traffico generato dalla macchina identificata dall'host IP address.

Per indicare un singolo indirizzo IP inserite:

Host IP Address: xxx.xxx.xxx.xxx (l'indirizzo IP che volete bloccare)

Host Subnet Mask: 255.255.255.255 (questa Subnet Mask identifica un singolo indirizzo IP)

Se inserite una Subnet Mask differente da quella indicata nell'esempio, la regola verrà applicata a tutti i membri della Subnet Mask.

Indicando per esempio:

Host IP Address: 192.168.1.1

Host Subnet Mask: 255.255.255.248

La regola verrà applicata a tutti gli indirizzi IP tra 192.168.1.0 e 192.168.1.7 (range di indirizzi identificato dalla Subnet Mask inserita)

Nota: Questa tipologia di regola lavora semplicemente basandosi sull'indirizzo IP, pertanto bloccando il traffico in una sola direzione non può essere garantito il funzionamento di tutte le applicazioni nella direzione opposta (dipende dalla modalità di funzionamento dell'applicazione).

### 3.6.3 Intrusion Detection

Questa funzione ha lo scopo di proteggere la tua LAN da attacchi esterni, come per esempio attacchi DOS (Denial-of-Service) o port scan.

Lo scopo di questi attacchi è quello di saturare le risorse disponibili sul router e sui server per provocare una temporanea interruzione del funzionamento o in alcuni casi il blocco di tutta la rete LAN.

Il firewall è in grado di riconoscere e di interrompere un tentativo di attacco.

Inoltre è possibile abilitare la funzione di Blacklist, disabilitando per n secondi la ricezione di pacchetti dagli indirizzi IP che sono stati identificati come attaccanti.

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

**Intrusion Detection:** selezionate Enable per abilitare le funzioni di Intrusion Detection.

**Victim Protection Block Duration:** inserite il tempo in secondi, di disconnessione della nostra macchina di LAN, se vittima di un attacco.

**Scan Attack Block Duration:** questo tempo identifica la durata di permanenza di un indirizzo IP nella Blacklist se ritenuto colpevole di una scansione dei servizi attivi sulla LAN.

**DOS Attack Block Duration:** questo tempo identifica la durata di permanenza di un indirizzo IP nella Blacklist, quando ritenuto colpevole di un attacco DoS.

**Maximum TCP Open Handshaking Count:** numero massimo di richieste (SYN) che possono arrivare al router, o ad un server interno, in un secondo; superato questo valore viene abilitata la protezione per evitare il compimento di una attacco SYN flood.

**Maximum Ping Count:** numero massimo di pacchetti PING che il router può ricevere in un secondo; superata questa soglia il firewall attua le protezioni necessarie a proteggere la LAN da questo tipo di attacco.

**Maximum ICMP Count:** Inserite il massimo numero di pacchetti ICMP che il router può ricevere in un secondo; superate questa soglia il firewall attua le protezioni necessarie a proteggere la LAN da questo tipo di attacco.

Se siete indecisi sui valori da impostare, non modificate le impostazioni predefinite.

### 3.6.4 MAC Address Filter

Questa funzionalità permette di abilitare o disabilitare l'accesso ad Internet ad un elenco di host (max. 10) basandosi sull'indirizzo fisico (MAC Address) della scheda.

MAC Address Filter											
<b>Filtering Rules</b>											
MAC Address Filter	<input type="radio"/> Enable <input checked="" type="radio"/> Disable										
For LAN ethernet frames, only the following Source MAC Address(es) are	<input type="radio"/> Allowed <input checked="" type="radio"/> Blocked										
MAC Address	<table border="1"><tr><td>00:00:00:00:00:00</td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>	00:00:00:00:00:00									
00:00:00:00:00:00											
<input type="button" value="Apply"/>											

**MAC Address Filter:** abilita la funzionalità MAC Address Filter

**Allowed:** Il router è abilitato ad operare **solamente** con i MAC address inseriti nella tabella, tutte le altre schede di rete non possono comunicare con e attraverso il router.

**Blocked:** Il router comunica con tutte le macchine, **ad esclusione** di quelle con il MAC address inserito in tabella.

**MAC Address:** Inserite gli indirizzi MAC

### 3.6.5 URL Filter

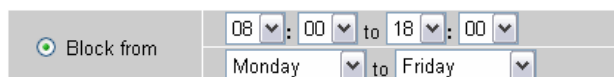
Questa funzione permette di limitare i siti WEB raggiungibili.

URL Filter															
<b>Configuration</b>															
URL Filtering	<input type="radio"/> Enable <input checked="" type="radio"/> Disable														
Block Mode	<input checked="" type="radio"/> Always Block														
	<input type="radio"/> Block from <table border="1"><tr><td>08</td><td>:</td><td>00</td><td>to</td><td>18</td><td>:</td><td>00</td></tr><tr><td>Monday</td><td></td><td></td><td>to</td><td>Friday</td><td></td><td></td></tr></table>	08	:	00	to	18	:	00	Monday			to	Friday		
08	:	00	to	18	:	00									
Monday			to	Friday											
Keywords Filtering	<input type="checkbox"/> Enable <a href="#">Details</a>														
Domains Filtering	<input type="checkbox"/> Enable <a href="#">Details</a>														
	<input type="checkbox"/> Disable all WEB traffic except for Trusted Domains														
Restrict URL Features	<input type="checkbox"/> Block Java Applet														
	<input type="checkbox"/> Block surfing by IP address														
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>															

**URL Filtering:** abilita la funzionalità URL Filter

**Always Block:** le regole impostate sono sempre attive.

**Block from** : permette di selezionare una fascia oraria in cui attivare queste regole, inoltre è possibile limitare l'applicazione di queste regole solo ad alcuni giorni della settimana.  
Per esempio, inserendo

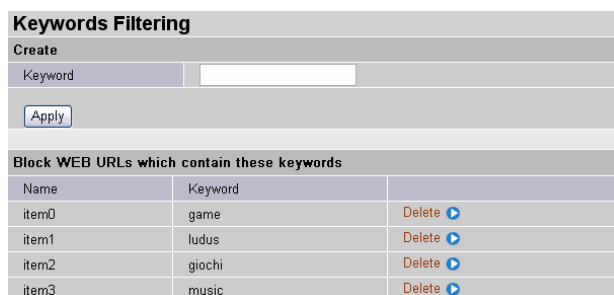


Block from 08:00 to 18:00 Monday to Friday

Questi filtri verranno impostati dal Lunedì al Venerdì, dalle 8:00 alle 18:00, in orari/giorni differenti sarà possibile raggiungere tutti i siti WEB.

**Keywords Filtering:** Se abilitato blocca l'accesso a tutti i siti WEB di cui l'URL contiene una delle stringhe inserite.

Selezionate **Details** per specificare l'elenco delle stringhe da bloccare.



Name	Keyword	
item0	game	Delete ▶
item1	ludus	Delete ▶
item2	giochi	Delete ▶
item3	music	Delete ▶

La tabella mostra tutte le stringhe che verranno bloccate, selezionate **Create** per aggiungerne di nuove oppure **Delete** per rimuovere una parola dalla lista.

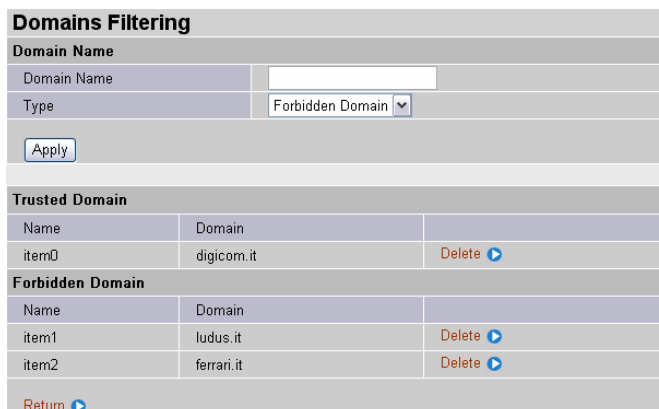
Come l'esempio mostrato sopra, ogni sito WEB che contiene nell'URL una delle stringhe in tabella non risulterà accessibile:

[www.ludus.it](http://www.ludus.it)  
[www.megagames.com](http://www.megagames.com)  
etc. etc.

Il controllo viene effettuato sull'intero URL, pertanto non sarà possibile nemmeno effettuare una ricerca (per esempio da [www.google.it](http://www.google.it)) che abbia come argomento una delle stringhe impostate. Infatti l'URL che verrà utilizzato per effettuare la ricerca di "giochi" da un qualsiasi motore di ricerca sarà di questo tipo:  
<http://www.google.it/search?hl=it&ie=UTF-8&oe=UTF-8&q=giochi&btnG=Cerca+con+Google&lr=>

**Domains Filtering:** Se abilitato applica il filtro basato su domini.

Selezionate **Details** per specificare l'elenco di domini da utilizzare.



Name	Domain	
item0	digicom.it	Delete ▶

Name	Domain	
item1	ludus.it	Delete ▶
item2	ferrari.it	Delete ▶

Return ▶

La tabella mostra in **Trusted Domain** l'elenco di domini permessi ed in **Forbidden Domain** l'elenco di quelli da bloccare.

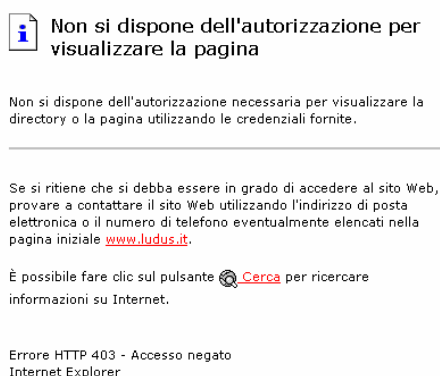
Selezionate **Create** per aggiungere nuovi domini oppure **Delete** per cancellarne uno.

Il dominio deve essere scritto come nell'esempio, per [www.ferrari.it](http://www.ferrari.it) inserite **ferrari.it** (senza www.)

Se invece di scrivere delle regole per bloccare alcuni siti, preferite indicare gli unici domini raggiungibili, selezionate l'opzione **Disabile all WEB traffic except for Trusted Domains**.

In questo caso sarà possibile raggiungere **solamente** i domini inseriti nella tabella **Trusted Domains**.

Se un PC cerca di raggiungere un sito "bloccato" ottiene solo una pagina di questo tipo



**Block Java Applet:** Se selezionata, vengono bloccate tutte le applet java.

**Block Surfing by IP Address:** Se selezionate blocca l'accesso a pagine web raggiunte senza una richiesta DNS.

### 3.6.6 FIREWALL LOG

In questa finestra è possibile abilitare o disabilitare i log.

Firewall Log	
Event will be shown in the Status - Event Log	
Filtering Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Intrusion Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
URL Blocking Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply

Il log abilitati saranno visibili nel menù **Status – Event Log**

## 3.7 Configuration VPN

Il router supporta delle funzionalità VPN per stabilire connessioni sicure e protette in Internet con altre reti LAN o Client VPN

Il tunnel VPN può utilizzare il protocollo PPTP oppure il protocollo IPSEC.  
Il router riesce a gestire fino a 8 connessioni contemporanee, 4 PPTP e 4 IPSEC.

### 3.7.1 VPN PPTP

Questo menu permette la creazione delle policy per il tunneling VPN basato su protocollo PPTP

The screenshot shows the PPTP configuration interface. It has a header 'PPTP' and two main sections: 'VPN/PPTP for Remote Access Application' and 'VPN/PPTP for LAN-to-LAN Application'. Each section contains a table with columns for 'Enable', 'Disable', 'Name', 'Type', and 'Status'. Below these tables are 'Create' and 'Apply' buttons.

Esistono due differenti tipi di connessione PPTP:

**Remote Access:** permette la connessione alla LAN locale di un singolo client remoto connesso in Internet.

**LAN-to-LAN:** permette la creazione di un tunnel VPN PPTP tra la LAN locale ed una rete LAN remota.

Selezionate **Create...** per creare una nuova policy VPN PPTP

### 3.7.2 VPN PPTP - REMOTE ACCESS

The screenshot shows the 'PPTP Configuration' screen. Under 'Connection Type', there are two radio button options: 'Remote Access' (which is selected) and 'LAN to LAN'. A 'Next' button is located at the bottom of the screen.

Premete **Next** per continuare.

The screenshot shows the 'PPTP Remote Access Connection' configuration screen. It includes fields for 'Connection Name', 'Type' (with 'Dial out' selected), 'Username', 'Password', 'Auth. Type' (set to 'Chap(Auto)'), 'Data Encryption' (set to 'Auto'), 'Key Length' (set to 'Auto'), 'Mode' (set to 'stateful'), and 'Idle Timeout' (set to '0 minutes'). There are also input fields for 'Server IP Address (or Hostname)' and 'Private IP Address Assigned to Dialin User'. An 'Apply' button is at the bottom.

**Connection Name:** inserite il nome mnemonico da associare a questa policy, il nome non deve contenere spazi.

**Type:**

**Dial out:** selezionate questo tipo di connessione se volete che sia il router ad attivare la connessione verso un server PPTP remot raggiungibile in Internet. Nel campo **Server IP Address** inserite l'indirizzo IP del server remoto oppure il suo Hostname.

**Dial in:** selezionate questa modalità se volete fornire l'accesso alla LAN ad un client remoto connesso in Internet. Nel campo **Private IP Address..** inserite l'indirizzo IP di LAN che volete assegnare al client, una volta connesso.

**Username, Password:** inserite username e password per il collegamento PPTP.

**Auth. Type:** selezionate il tipo di autenticazione.

**Data Encryption:** abilita l'algoritmo di cifratura MPPE. Di default il parametro è impostato su Auto, quindi negoziato all'instaurarsi della connessione.

**Key Length:** Imposta la lunghezza della Key utilizzata dall'algoritmo MPPE; se lasciato in Auto la Key viene negoziata all'instaurarsi della connessione.

**Mode:** La Key viene cambiata ogni 256 pacchetti (**stateful**) oppure ad ogni pacchetto (**stateless**).

**Idle time:** inserite il tempo di inattività dati per disconnettere il tunnel VPN PPTP; impostando 0 minuti la connessione rimarrà sempre attiva.

Nell'appendice del manuale è disponibile una sezione che illustra un esempio di configurazione.

### 3.7.3 VPN PPTP - LAN to LAN

PPTP Configuration	
Connection Type	<input type="radio"/> Remote Access <input checked="" type="radio"/> LAN to LAN
<input type="button" value="Next"/>	

Premete **Next** per continuare.

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

Tutti i parametri sono equivalenti a quelli descritti nella configurazione del Remote Access PPTP.

**Peer Network IP / Netmask:** identifica la rete LAN remota o una parte della rete remota raggiungibile tramite la connessione PPTP.

Esempio: Per indicare tutta la rete 192.168.2.x inserite:  
**Peer Network IP:** 192.168.2.0  
**Netmask:** 255.255.255.0

### 3.7.4 VPN IPSEC

Questo menu permette la creazione delle policy per il tunneling VPN basato su protocollo IPSEC

IPSec						
VPN Tunnels						
Enable	Disable	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal
Create						
Apply						

Selezionate **Create...** per creare una nuova policy.

IPSec						
Create						
Connection Name <input type="text"/>						
Local						
NetWork	<input checked="" type="radio"/> Single Address	IP Address	<input type="text"/>			
	<input type="radio"/> Subnet	IP Address	<input type="text"/>	Netmask	<input type="text"/>	
	<input type="radio"/> IP Range	IP Address	<input type="text"/>	End IP	<input type="text"/>	
Remote						
Secure Gateway Address(or Hostname) <input type="text"/>						
NetWork	<input checked="" type="radio"/> Single Address	IP Address	<input type="text"/>			
	<input type="radio"/> Subnet	IP Address	<input type="text"/>	Netmask	<input type="text"/>	
	<input type="radio"/> IP Range	IP Address	<input type="text"/>	End IP	<input type="text"/>	
Proposal						
<input checked="" type="radio"/> ESP	Authentication		None			
	Encryption		NULL			
<input type="radio"/> AH	Authentication		MD5			
	Perfect Forward Secrecy		None			
	Pre-shared Key		<input type="text"/>			
Apply						

**Connection Name:** inserite il nome mnemonico da associare a questa policy, il nome non deve contenere spazi.

#### Local

**NetWork:** identifica la rete LAN locale o la parte di essa che può utilizzare il tunnel VPN IPSEC.

**Single Address:** singolo indirizzo IP locale

**Subnet:** una rete LAN

**IP Range:** un range d indirizzi IP locali (inizio – fine)

#### Remote

**Secure Gateway Address:** Indica l'end point, cioè l'indirizzo IP di WAN del router remoto.

**NetWork:** identifica la rete LAN remota o una parte della rete remota raggiungibile tramite il tunnel VPN IPSEC

**Single Address:** singolo indirizzo IP remoto

**Subnet:** una rete LAN remota

**IP Range:** un range d indirizzi IP remoti (inizio – fine)

#### Proposal

In questa sezione dovete impostare i vari parametri di crittografia della connessione IPSEC.

Verificate che tutti i paramentri impostati corrispondano esattamente a quelli configurati nel router remoto.

**AH Authentication:** AH (Authentication Header) specifica l'algoritmo di crittografia da utilizzare per l'header VPN.

**ESP:** ESP (Encapsulating Security Payload) provvede alla sicurezza dei dati (payload) inviati attraverso il tunnel VPN.

ESP si divide in due parti **Encryption** ed **Authentication** per entrambe è possibile selezionare un algoritmo di crittografia differente.

**Perfect Forward Security:** se abilitata forza un continuo cambio delle chiavi IPSEC durante la sessione, garantendo che le nuove chiavi non siano in alcun modo in relazione con le precedenti, evitando che dopo aver eventualmente scoperto una chiave, un malintenzionato sia in grado di generarsi tutte le successive.

**Pre-Shared Key:** inserite la stringa utilizzata come password per generare la crittografia.

Nota: **Perfect Forward Security** incrementa il grado di sicurezza ma richiede maggior elaborazione dei dati, a discapito delle prestazioni.

### 3.7.5 VPN L2TP

Questo menù permette la creazione delle policy per il tunneling VPN basate sul protocollo L2TP.

The screenshot shows the 'L2TP' configuration menu. It has two sections: 'L2TP for Remote Access Application' and 'L2TP for LAN-to-LAN Application'. Each section contains a table with columns for 'Enable', 'Disable', 'Name', 'Type', and 'Status'. Below these tables are 'Create' and 'Apply' buttons.

Esistono due differenti tipi di connessione L2TP:

**Remote Access:** permette la connessione alla LAN locale di un singolo client remoto connesso in Internet.

**LAN-to-LAN:** permette la creazione di un tunnel VPN PPTP tra la LAN locale ed una rete LAN remota.

Selezionate **Create...** per creare una nuova policy VPN L2TP

### 3.7.6 VPN L2TP - REMOTE ACCESS

The screenshot shows the 'L2TP Configuration' screen. Under 'Connection Type', the 'Remote Access' radio button is selected, and the 'LAN to LAN' radio button is unselected. A 'Next' button is at the bottom.

Premete **Next** per continuare.

The screenshot shows the 'L2TP Remote Access Connection' configuration screen. Fields include: 'Connection Name' (text input), 'Type' (radio buttons for 'Dial out' and 'Dial in'), 'Server IP Address (or Hostname)' (text input), 'Private IP Address Assigned to Dialin User' (text input), 'Username' (text input), 'Password' (text input), 'Auth. Type' (dropdown menu with 'Chap(Auto)' selected), 'Idle Timeout' (text input with '0 minutes'), 'IPSec' (checkbox), 'Authentication' (dropdown menu with 'None' selected), 'Encryption' (dropdown menu with 'NULL' selected), 'Perfect Forward Secrecy' (dropdown menu with 'None' selected), and 'Pre-shared Key' (text input). An 'Apply' button is at the bottom.

**Connection Name:** inserite il nome mnemonico da associare a questa policy, il nome non deve contenere spazi.

**Type:**

**Dial out:** selezionate questo tipo di connessione se volete che sia il router ad attivare la connessione verso un server L2TP remoto raggiungibile in Internet. Nel campo **Server IP Address** inserite l'indirizzo IP del server remoto oppure il suo Hostname.

**Dial in:** selezionate questa modalità se volete fornire l'accesso alla LAN ad un client remoto connesso in Internet. Nel campo **Private IP Address..** inserite l'indirizzo IP di LAN che volete assegnare al client, una volta connesso.

**Username, Password:** inserite username e password per il collegamento L2TP.

**Auth. Type:** selezionate il tipo di autenticazione.

**Idle time:** inserite il tempo di inattività dati per disconnettere il tunnel VPN L2TP; impostando 0 minuti la connessione rimarrà sempre attiva.

**IP Sec:** Se abilitato viene utilizzata la crittografia IPSec.

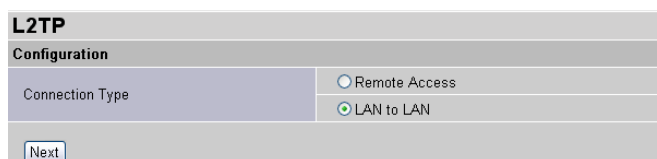
**Authentication:** Selezionate l'algoritmo di crittografia per la fase di autenticazione IpSec.

**Encryption:** Selezionate l'algoritmo di crittografia d utilizzare per i dati

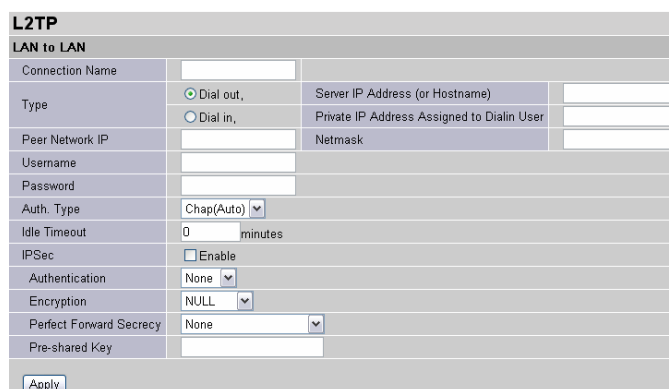
**Perfect Forward Secrecy:** se abilitata forza un continuo cambio delle chiavi IPSEC durante la sessione, garantendo che le nuove chiavi non siano in alcun modo in relazione con le precedenti, evitando che dopo aver eventualmente scoperto una chiave, un malintenzionato sia in grado di generarsi tutte le successive.

**Pre-Shared Key:** inserite la stringa utilizzata come password per generare la crittografia.

### 3.7.7 VPN L2TP - LAN to LAN



Premete **Next** per continuare.



Tutti i parametri sono equivalenti a quelli descritti nella configurazione del Remote Access L2TP.

**Peer Network IP / Netmask:** identifica la rete LAN remota o una parte della rete remota raggiungibile tramite la connessione L2TP.

Esempio: Per indicare tutta la rete 192.168.2.x inserite:  
**Peer Network IP:** 192.168.2.0  
**Netmask:** 255.255.255.0

## 3.8 Configuration – QoS

La funzione QoS (Quality of Service) permette di gestire l'utilizzo della banda in uscita in base alle sessioni e agli indirizzi IP interessati.

### 3.8.1 Prioritization

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

Esistono tre livelli di priorità che ripartiscono la banda disponibile:

**High 60%**

**Normal 30%** (tutti i pacchetti hanno questa priorità al default)

**Low 10%**

**Enable:** Abilita la regola inserita sulla stessa riga.

**Application:** inserite un nome mnemonico per l'applicazione.

**Priority:** Selezionate High o Low per aumentare o diminuire la priorità.

**Protocol:** Selezionate il tipo di protocollo utilizzato nell'applicazione

**Source Port:** inserite le porte sorgenti utilizzate dall'applicazione da priorizzare

**Destination Port:** inserite le porte di destinazione utilizzate dall'applicazione da priorizzare

**Source IP Address:** inserite il gruppo di indirizzi IP sorgenti utilizzati nell'applicazione da priorizzare

**Destination IP Address:** inserite il gruppo di indirizzi IP di destinazione utilizzati nell'applicazione da priorizzare

### 3.8.2 IP Throttling

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

Apply

**Enable:** Abilita la regola inserita sulla stessa riga.

**Application:** inserite un nome mnemonico per l'applicazione.

**Protocol:** Selezionate il tipo di protocollo utilizzato nell'applicazione

**Source Port:** inserite le porte sorgenti utilizzate dall'applicazione da priorizzare

**Destination Port:** inserite le porte di destinazione utilizzate dall'applicazione da priorizzare

**Source IP Address:** inserite il gruppo di indirizzi IP sorgenti utilizzati nell'applicazione da priorizzare

**Destination IP Address:** inserite il gruppo di indirizzi IP di destinazione utilizzati nell'applicazione da priorizzare

**Upstream Rate Limit:** Inserite il limite massimo di banda utilizzabile dall'applicazione, il valore deve essere espresso in multipli di 32 kbps

## 3.9 Configuration – Virtual Server

La funzione **Virtual Server** permette l'accesso a Server e servizi presenti nella LAN locale, da parte di utenti remoti connessi in Internet.

I servizi selezionati verranno resi disponibili sull'indirizzo IP di WAN del router.

Normalmente questi Server NON sono raggiungibili da Internet perché:

1. Il Server ha un indirizzo IP privato
2. Il protocollo NAT nasconde la LAN interna.

Nella finestra di configurazione **Virtual Server**, è possibile selezionare quali servizi rendere disponibili all'esterno.

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

Il router è già preconfigurato per facilitare l'esportazione dei principali servizi, è sufficiente completare l'indirizzo IP del Server interno alla nostra LAN in **IP Address** e selezionare la corrispondente casella nella colonna **Enable**.

E' inoltre possibile configurare 10 esportazioni (virtual server) aggiuntive:

<input type="checkbox"/>	Nome del Servizio	tcp	Range di porte utilizzate	192.168.1. [ ]
--------------------------	-------------------	-----	---------------------------	----------------

Michelangelo Office (Wave) Pro V offre inoltre la possibilità di utilizzare una funzione chiamata **DMZ (De Militarized Zone)**

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

Abilitando questa opzione, tutti i pacchetti destinati a porte (servizi) non definiti nelle altre regole verranno indirizzati al PC impostato in **DMZ**.

**Utilizzare questa impostazione solamente se non si hanno a disposizione altre opzioni oppure se non si conoscono le porte di funzionamento di un dato servizio.**

Il router supporta le funzionalità **Virtual Server** solamente sull'indirizzo Ethernet primario.

Al termine di ogni modifica selezione **Apply** a fondo pagina per attivare la nuova configurazione.

## 3.10 Configuration Advanced

Questo menu permette di impostare alcuni parametri e funzioni avanzate

### 3.10.1 Static Route

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

Se Michelangelo Office (Wave) Pro V non è l'unico router presente nella rete LAN potrebbe essere necessario creare delle route statiche (regole di instradamento) per indirizzare i pacchetti verso le altre reti (e altri Gateway).

### 3.10.2 Dynamic DNS

La maggior parte degli abbonamenti Adsl utilizzano un indirizzo IP dinamico, pertanto l'indirizzo di WAN del router può cambiare ad ogni connessione.

Per risolvere questo problema sono disponibili in Internet dei servizi denominati **Dynamic DNS (DDNS)**.

Questi servizi DDNS permettono di associare un nome di dominio ad un indirizzo IP in modo dinamico, dopo aver effettuato una registrazione gratuita oppure a pagamento.

Dynamic DNS	
Parameters	
Dynamic DNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Dynamic DNS Server	<input type="text" value="www.dyndns.org (dynamic)"/>
Domain Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Period	<input type="text" value="25"/> <input type="text" value="Day(s)"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Dynamic DNS:** Selezionate Enable per abilitare il servizio.

Selezionate il vostro server del servizio da **Dynamic DNS** ed inserite i dati del vostro account.

In **Period** selezionate ogni quanti giorni volete effettuare un aggiornamento dell'indirizzo.

Ogni qualvolta il router rileva un nuovo indirizzo IP sulla WAN, effettua automaticamente una nuova registrazione al server DDNS (nell'esempio [www.dyndns.org](http://www.dyndns.org)) impostato, aggiornando così l'indirizzo IP di WAN corrente.

Un host, o altro router, che da internet faccia riferimento al dominio attivato, otterrà come risultato l'indirizzo IP attuale, e potrà così raggiungere i servizi eventualmente messi a disposizione sulla porta WAN. (tramite Virtual Server)

### 3.10.3 Check Emails

Michelangelo Office (Wave) Pro V è in grado di controllare periodicamente un account di posta e di indicare con l'apposito led sul frontale la presenza di e-mail nella casella di posta.

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

### 3.10.4 Device Management

Device Management			
<b>Device Host Name</b>			
Host Name	<input type="text" value="home.gateway"/>		
<b>Embedded Web Server</b>			
* HTTP Port	<input type="text" value="80"/>	(80 is default HTTP port)	
Management IP Address	<input type="text" value="0.0.0.0"/>	(0.0.0.0 means Any)	
Expire to auto-logout	<input type="text" value="180"/>	seconds	
<b>Universal Plug and Play (UPnP)</b>			
UPnP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
* UPnP Port	<input type="text" value="2800"/>		
<b>SNMP Access Control</b>			
<b>SNMP V1 and V2</b>			
Read Community	<input type="text" value="public"/>	IP Address	<input type="text" value="0.0.0.0"/>
Write Community	<input type="text" value="password"/>	IP Address	<input type="text" value="0.0.0.0"/>
Trap Community	<input type="text"/>	IP Address	<input type="text"/>
<b>SNMP V3</b>			
Username	<input type="text"/>	Password	<input type="text"/>
Access Right	<input checked="" type="radio"/> Read <input type="radio"/> Read/Write		IP Address <input type="text"/>
* : This setting will become effective after you save to flash and restart the router.			
<input type="button" value="Apply"/>			

In questa finestra è possibile modificare le proprietà del Web Server interno per la configurazione dell'hardware.

**Host Name:** Inserite l'Host name da associare al router.

**HTTP Port:** permette la modifica della porta sulla quale è attivo il Web Server. Se modificate la porta, inserite un valore **superiore a 1024**.

Per entrare in configurazione del router è quindi necessario collegarsi alla porta scelta; se impostate la porta 8080, nel browser dovrete scrivere <http://192.168.1.254:8080>.  
Selezionate sempre la porta 80 (HTTP) oppure in alternativa una porta superiore a 1024.

**Management IP Address:** lasciate impostato 0.0.0.0 se volete permettere la configurazione del router da un qualsiasi indirizzo IP di LAN.

In alternativa potete limitare l'accesso alla configurazione ad un solo indirizzo IP, inserendone il valore .

**Expire to auto-logout:** nella configurazione del dispositivo può accedere un solo utente alla volta.

Se l'utente non effettua il logout, cliccando sull'apposito pulsante, mantiene impegnata la sessione di configurazione impedendo l'accesso ad altri utenti. Per ovviare a questo problema è possibile impostare un logout automatico allo scadere di n secondi di inattività.

**Universal Plug and Play (UPnP)**

**UPnP:** Abilitate la configurazione tramite il protocollo UPnP selezionando Enable sulla porta **UPnP Port**.

### 3.10.5 SNMP Access Control

Michelangelo Office (Wave) Pro V supporta il protocollo SNMP.

E' possibile configurare la password di accesso alle tre Community e l'indirizzo IP abilitato ad accedere (0.0.0.0 per permettere l'accesso da tutti gli indirizzi)

Al default la password per la **Read Community** è **public**, per la **Write Community** è **password** e la **Trap Community** è disabilitata.

## 3.11 Status

---

Il menù **Status** mostra un riepilogo della configurazione del router.

In particolare:

**Software Version** è la versione Firmware caricata nel dispositivo

**LAN e WAN** riepilogano le configurazioni di LAN e WAN.

### 3.11.1 Status – ARP Table

In questa finestra è possibile controllare gli indirizzi IP e i MAC Address di tutte le macchine che sono entrate in contatto con il Router.

### 3.11.2 Status – DHCP Table

Questa finestra mostra tutti gli indirizzi IP che sono stati assegnati via DHCP Server in associazione al MAC Address e al nome della scheda di rete che ha richiesto l'indirizzo.

**Expiry** rappresenta il tempo di validità dell'indirizzo.

### 3.11.3 Status – PPTP Status, IPSEC Status, L2TP Status

Questa due finestre mostrano un riassunto delle eventuali connessioni PPTP o IPSEC configurate e ne visualizzano lo stato.

### 3.11.4 Status – Email Status

In questa finestra è possibile verificare il numero di Email che il router ha rilevato sulla casella di posta da controllare.

**Reset Status:** azzerà il contatore (e quindi spegne anche il led MAIL)

**Check Now !** forza un controllo del numero di Email nella casella di posta configurata.

### 3.11.5 Status – Event Log, Error Log

Queste finestra mostrano i Log di sistema.

Se abilitate i log nella configurazione del firewall, verranno tutti riportati nella pagina **Event Log**.

## 4 Appendice

---

### 4.1 Porte TCP/UDP maggiormente utilizzate

---

Nome	Numero	Descrizione
ftp-data	20/tcp	File Transfer (Default Data)
ftp-data	20/udp	File Transfer (Default Data)
ftp	21/tcp	File Transfer (Control)
ftp	21/udp	File Transfer (Control)
ssh	22/tcp	SSH Remote Login Protocol
ssh	22/udp	SSH Remote Login Protocol
telnet	23/tcp	Telnet
telnet	23/udp	Telnet
smtp	25/tcp	Simple Mail Transfer
smtp	25/udp	Simple Mail Transfer
domain	53/tcp	Domain Name Server
domain	53/udp	Domain Name Server
http	80/tcp	World Wide Web HTTP
http	80/udp	World Wide Web HTTP
www	80/tcp	World Wide Web HTTP
www	80/udp	World Wide Web HTTP
www-http	80/tcp	World Wide Web HTTP
www-http	80/udp	World Wide Web HTTP
pop3	110/tcp	Post Office Protocol - Version 3
pop3	110/udp	Post Office Protocol - Version 3
nntp	119/tcp	Network News Transfer Protocol
nntp	119/udp	Network News Transfer Protocol
ntp	123/tcp	Network Time Protocol
ntp	123/udp	Network Time Protocol
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
snmp	161/tcp	SNMP
snmp	161/udp	SNMP
snmptrap	162/tcp	SNMPTRAP
snmptrap	162/udp	SNMPTRAP
pptp	1723/tcp	pptp
pptp	1723/udp	pptp
ms-wbt-server	3389/tcp	
ms-wbt-server	3389/udp	MS WBTerminal Server

## 4.2 Elenco Server DNS

---

Gli indirizzi riportati in questa pagina hanno lo scopo di aiutare nella configurazione del router, qualora questi dati non siano stati specificati dal provider.

La gestione di questi indirizzi dipende solo dai rispettivi provider, pertanto non è possibile garantirne la funzionalità nel tempo.

### TIN

dns1.village.tin.it	195.14.96.135
dnsca2.tin.it	212.216.172.222
dnscache2.tin.it	212.216.172.162
dns2.tin.it	194.243.154.51
dnscache1.tin.it	212.216.172.62
dns1.fullcompany.telecomitalia.it	212.131.30.42
dnsca.tin.it	212.216.112.112
dnsca.tin.it	195.31.190.31
dns.tin.it	194.243.154.62

### Interbusiness

r-dns.interbusiness.it	151.99.125.1
dns2.interbusiness.it	151.99.125.3
dns.interbusiness.it	151.99.125.2
server-b.cs.interbusiness.it	151.99.250.2

### Infostrada

ns2.libero.it	193.70.192.100
ns1.libero.it	195.210.91.100
cns-a.libero.it	193.70.192.25
cns-b.libero.it	193.70.152.25

### Wind

dns.wind.it	212.245.255.2
dns2.wind.it	212.245.158.66
dns.inwind.it	212.141.53.123
dns2.wind.it	212.245.158.66

### Atlanet

ns1.atlanet.it	213.234.128.211
ns2.atlanet.it	213.234.132.130
ns1.its.it	151.92.2.35
ns.telexis.it	213.199.1.132

### McLink

dns.mclink.it	195.110.128.1
---------------	---------------

### Flashnet

dns.flashnet.it	194.247.160.1
dns2.flashnet.it	194.247.160.8

### Albacom

ns2.albacom.net	212.17.192.209
-----------------	----------------

### I.Net

urano.inet.it	194.20.8.1
venere.inet.it	194.20.8.4

### Elitel

elitel.it	212.34.224.193
ns.elitel.it	212.34.224.132
ns2.elitel.it	217.146.65.7
ns3.elitel.it	217.146.65.80

### Tiscali

ns.tiscali.it	195.130.224.18
sns.tiscali.it	195.130.225.129

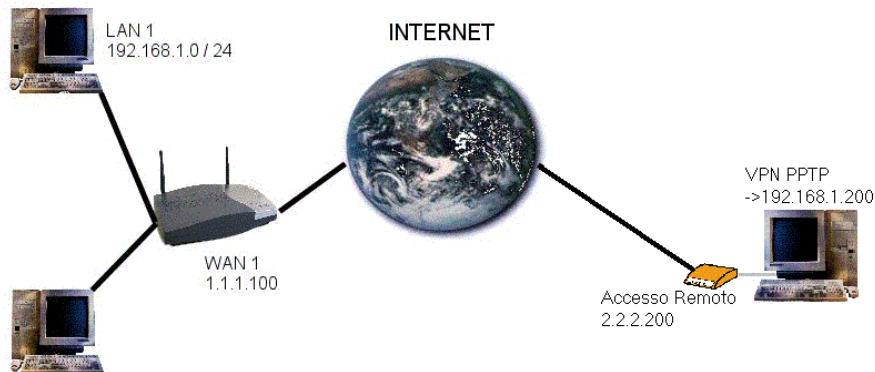
### Jumpy

-	212.17.192.216
-	212.17.192.56

### Public DNS

dns.nic.it	193.205.245.5
dns2.nic.it	193.205.245.8
nameserver.cnr.it	194.119.192.34

## 4.3 Accesso da remoto con VPN PPTP



Da una qualsiasi postazione remota connessa in Internet, è possibile accedere alla rete locale LAN1 utilizzando la connessione VPN PPTP fornita da Windows®.

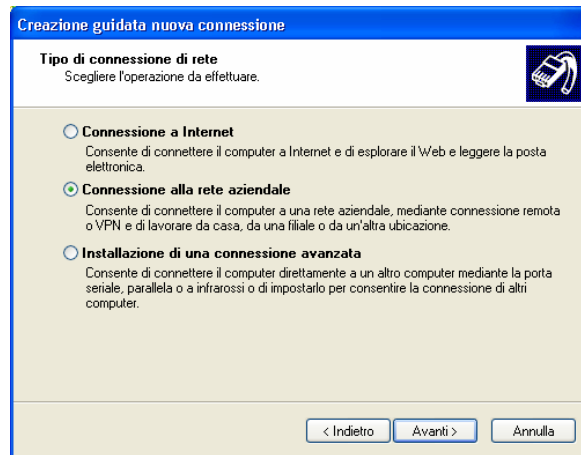
Michelangelo Office (Wave) Pro V deve essere configurato nel seguente modo:

PPTP			
Remote Access Connection			
Connection Name	Accesso01	Server IP Address (or Hostname)	
Type	<input type="radio"/> Dial out,	Private IP Address Assigned to Dialin User	192.168.1.200
	<input checked="" type="radio"/> Dial in,		
Username	pippo		
Password	*****		
Auth. Type	Chap(Auto)		
Data Encryption	Auto	Key Length	Auto
		Mode	stateful
Idle Timeout	0 minutes		
Apply			

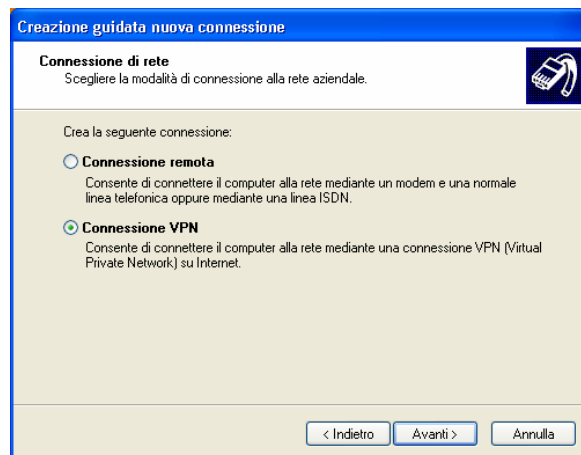
Con questa configurazione si abilita un host remoto ad accedere direttamente alla nostra LAN, l'host remoto riceverà un indirizzo IP da noi specificato (in questo caso 192.168.1.200).

La configurazione di windows deve essere effettuata nel seguente modo.

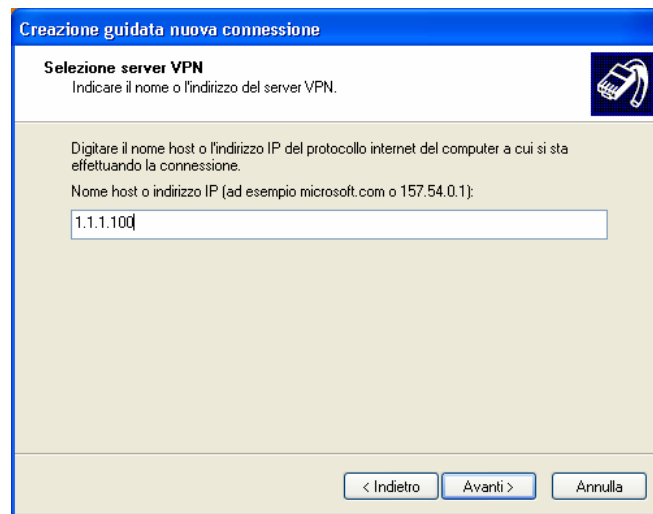
Create una **Connessione alla rete aziendale**



Selezionate il tipo **Connessione VPN**



Inserite l'indirizzo IP di WAN del router Michelangelo Office (Wave) Pro V .



Attivate la vostra connessione Internet classica e eseguite la connessione appena creata:



Al termine della connessione, potrete accedere a tutte le risorse disponibili nella rete LAN 1.