

# MICHELANGELO Office WAVE C



Manuale Operativo  
rev. 1.0 del 01/2004



**INDICE**

<b>PREMESSA</b>	<b>II</b>
<b>DICHIARAZIONE CE DI CONFORMITA'</b>	<b>II</b>
<b>1. INTRODUZIONE</b>	<b>1.1</b>
1.1. CARATTERISTICHE	1.1
1.2. DESCRIZIONE PORTE E LED	1.2
<b>2. INSTALLAZIONE</b>	<b>2.1</b>
<b>3. CONFIGURAZIONE</b>	<b>3.1</b>
3.1. CONFIGURAZIONE DEL COMPUTER	3.1
3.1.1. INDIRIZZI IP STATICI	3.1
3.1.2. IMPOSTAZIONE COME CLIENT DHCP	3.5
3.2. ACCESSO ALLA CONFIGURAZIONE	3.8
3.3. WIZARD SETUP	3.9
3.3.1. FASE 1	3.10
3.3.2. FASE 2	3.11
3.3.3. FASE 3	3.12
3.3.4. FASE 4 (CHANGE LAN CONFIGURATION)	3.13
<b>4. ADVANCED SETUP</b>	<b>4.1</b>
4.1. PASSWORD	4.1
4.2. LAN	4.1
4.3. WIRELESS	4.3
4.4. WAN	4.6
4.5. NETWORK ADDRESS TRANSLATION (NAT)	4.7
4.5.1. COSA FA IL NAT	4.7
4.5.2. COME FUNZIONA IL NAT	4.8
4.5.3. TIPOLOGIE DI NAT MAPPING	4.9
4.5.4. SUA SERVER	4.10
4.5.4.1. <i>SUA Only</i>	4.11
4.5.4.2. <i>Full Features</i>	4.12
4.5.4.3. <i>Type One-to-One</i>	4.12
4.5.4.4. <i>Type Many-to-One</i>	4.13
4.5.4.5. <i>Type Many-to-Many Overload</i>	4.13
4.5.4.6. <i>Type Many-to-Many no Overload</i>	4.14
4.5.4.7. <i>Type Server</i>	4.14
4.6. SECURITY	4.15
4.7. DYNAMIC DNS	4.15
4.8. TIME ZONE	4.16
4.9. REMOTE MANAGMENT	4.17
4.9.1. LIMITAZIONI DEL REMOTE MANAGEMENT	4.17
4.9.2. REMOTE MANAGEMENT E NAT	4.17
4.9.3. TIMEOUT	4.17
4.10. UPNP	4.18
4.10.1. DESCRIZIONE	4.18
4.10.2. NAT TRAVERSAL	4.18
4.11. MAINTENANCE	4.19
4.11.1. SYSTEM STATUS	4.19
4.11.2. DHCP TABLE	4.19
4.11.3. WIRELESS	4.19
4.11.4. DIAGNOSTIC	4.19
4.11.5. FIRMWARE	4.19
4.12. IP ALIAS	4.20
4.13. IP POLICY ROUTING (IPPR)	4.20
<b>A. APPENDICE</b>	<b>A.1</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 0 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 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 fatelo 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 il prodotto, Nome: **Michelangelo Office Wave C** 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 55022
- EN 61000-3-2
- EN 61000-3-3
- EN 301 489-1
- EN 301 489-17
- EN 300 328
- EN 60950

## 1. INTRODUZIONE

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

Michelangelo Office Wave C le permetterà di collegare il suo ufficio o dipartimento aziendale ad Internet e di creare una rete Wireless LAN in modo semplice ed efficiente.

Le stazioni della sua rete locale LAN Wireless e cablata avranno la possibilità di accedere ad Internet per la navigazione (WWW, HTTP) o l'accesso alla posta elettronica (e-mail) o altri servizi Internet utilizzando la linea ADSL ed un abbonamento per singolo utente o multi-utente (con indirizzi IP globali).

Tutte le operazioni di instaurazione del link saranno gestite in modo completamente automatico e trasparente da Michelangelo Office Wave C, senza intervento alcuno da parte degli utilizzatori della rete.

Potrà inoltre sfruttare le funzionalità avanzate del Router per gestire in modo efficiente l'accesso ad Internet dei suoi computer, realizzando se necessario, l'esportazioni di servizi interni.

In questo manuale troverà tutte le informazioni necessarie per collegare Michelangelo Office Wave C alla rete di computer e configurare opportunamente l'insieme in pochi minuti.

### Prerequisiti

- Computer con scheda di rete Ethernet o compatibile 802.11b
- Protocollo Tcp/Ip installato su ogni macchina
- Cavi di rete UTP Cat.5 con connettori RJ45 su entrambe le estremità
- Linea ADSL su linea analogica con connettore RJ11
- Abbonamento ADSL singolo o multi utente
- Dati abbonamento ADSL

### Contenuto della confezione

- 1 Michelangelo Office Wave C
- 1 Alimentatore 12VDC
- 1 cavo di linea RJ11 – RJ11
- 1 cavo di rete RJ45 - RJ45
- 1 cavo di console PS2/RS232
- 1 Cd-rom con il manuale completo
- 1 Guida rapida di installazione

## 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)
  - ENET ENCAP (MAC Encapsulated Routing Link Protocol)
  - Supporto ATM UNI3.1/4.0 PVC, ATMSAR, ATM AAL5 e OAM F5
- Interfaccia WAN ADSL: Connettore RJ11

**LAN**

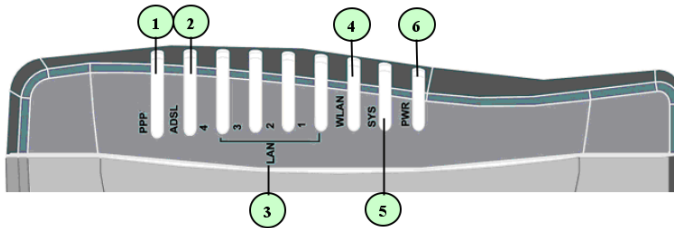
- Switch 4 porte 10/100 Mbit/s
- MDI / MDI-X su tutte le porte

**WIRELESS**

- Tecnologia Wireless IEEE 802.11b 2.4GHz
- DSSS Direct Sequence Spread Spectrum
- 13 canali
- Velocità Wireless: Automatic, 11, 5.5, 2,1 Mbit/s
- Antenna esterna
- Supporto crittografia dati WEP 64 e 128 bit
- Interoperabile Wi-Fi e Airport®

**1.2. DESCRIZIONE PORTE E LED**

**Descrizione Led**

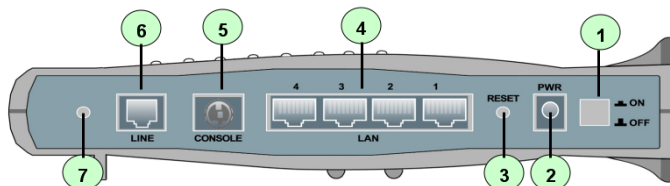


**LED**

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



## Descrizione Porte



Porta	Descrizione
1	Interruttore
2	PWR
3	RESET
4	LAN 1—4
5	CONSOLE
6	LINE

Interruttore di accensione del dispositivo

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.

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)

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.

Porta di console locale. Utilizzare il cavo PS2/RS-232 fornito nella confezione per accedere alla console. Vedi apposito manuale.

Connettore RJ-11 per la connessione della linea ADSL.





## 2. INSTALLAZIONE

# 2

Il dispositivo è interamente configurabile tramite un'interfaccia HTTP - WEB.

Per effettuare la prima configurazione del dispositivo, si consiglia di utilizzare un PC connesso al router tramite rete cablata Ethernet.

Le impostazioni di fabbrica del dispositivo sono le seguenti:

<b>Indirizzo IP di LAN</b>	192.168.1.254
<b>Subnet Mask</b>	255.255.255.0

<b>User Name</b>	admin
<b>Password</b>	admin

### 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

# 3

### 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

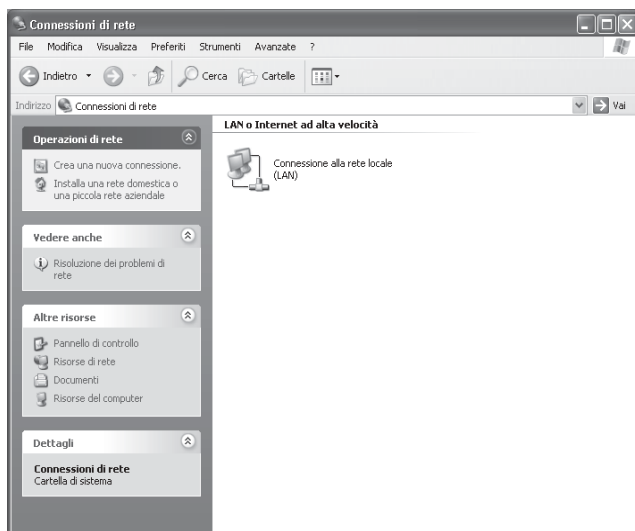
DHCP Server: Abilitato

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.

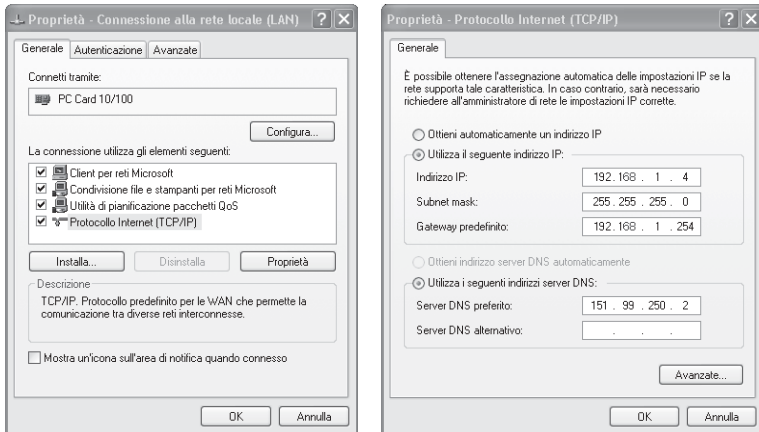
#### 3.1.1. INDIRIZZI IP STATICI

##### Windows® XP

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



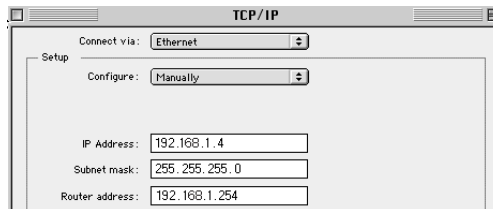
2. Selezionate **Connessione alla rete locale (LAN)** e visualizzate le **Proprietà**, selezionate **Protocollo Internet (TCP/IP)** e premete sul pulsante **Proprietà**.



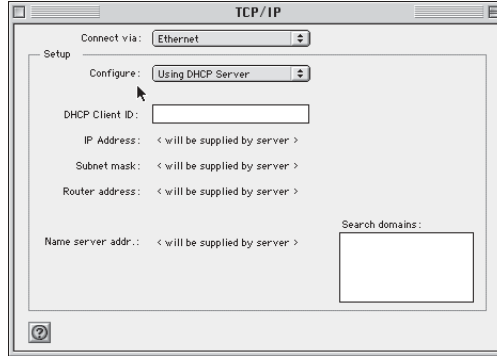
3. Per impostare un indirizzo IP dovete selezionare **Utilizza il seguente indirizzo IP**: ed inserire *Indirizzo IP*, la *Subnet mask* ed il *Gateway* predefinito come in figura. Confermate con **OK** le nuove impostazioni.
4. Riavviate Windows® per rendere attive le nuove impostazioni.

**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 **Configura**.



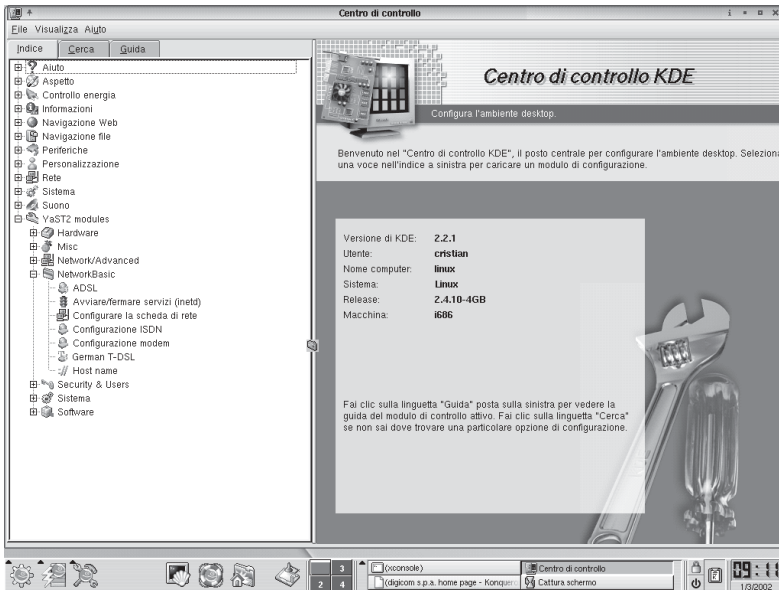
4. Inserite gli indirizzi come riportato in figura.
5. Chiudete la finestra TCP/IP e salvate.
6. Riavviate il Mac per rendere attive le impostazioni.



**Linux**

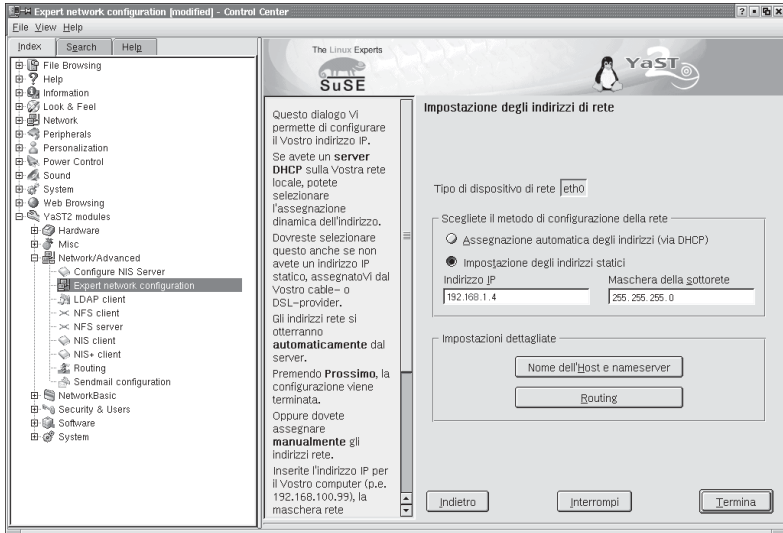
Di seguito verranno date alcune informazioni su come configurare le risorse di rete utilizzando il Centro di Controllo KDE, con la distribuzione Suse 6.2.

1. Attivate il Control Center.
2. Selezionate **Configurare la scheda di rete** nel menù **Network Basic**.



3. Selezionate **Impostazione degli indirizzi statici**, ed inserite gli indirizzi come riportato in figura.



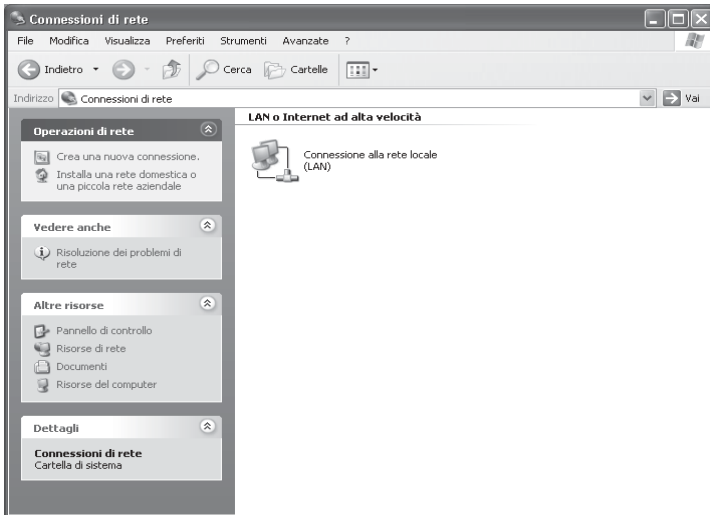


4. Per impostare il gateway, cliccate su Routing e inserite l'indirizzo 192.168.1.254 nel campo Gateway predefinito.

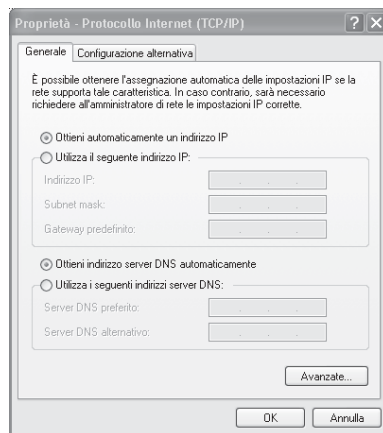
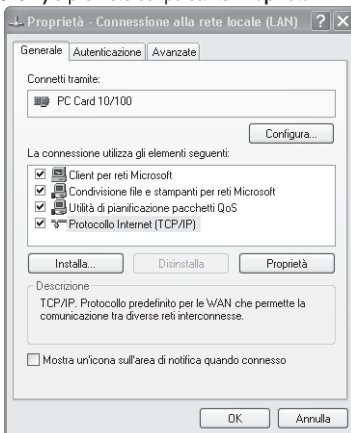
### 3.1.2. IMPOSTAZIONE COME CLIENT DHCP

#### Windows® XP

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



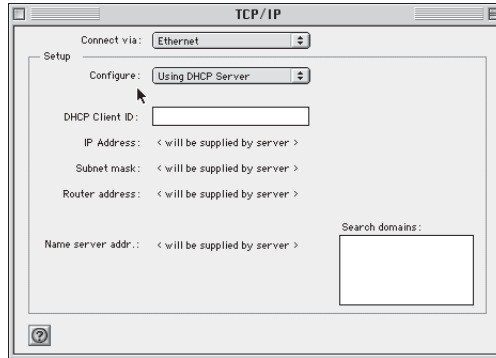
2. Selezionate **Connessione alla rete locale (LAN)** e visualizzate le **Proprietà**, selezionate **Protocollo Internet (TCP/IP)** e premete sul pulsante **Proprietà**.



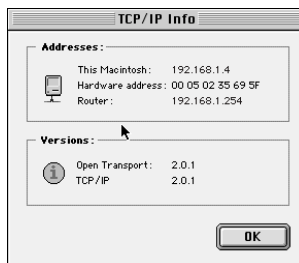
3. Per impostare il Computer come client DHCP dovete selezionare **Ottieni automaticamente un Indirizzo IP**, a questo punto potete chiudere le finestre confermando con **OK**.
4. Riavviate Windows® per rendere attive le nuove impostazioni.

## 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 DHCP 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**.

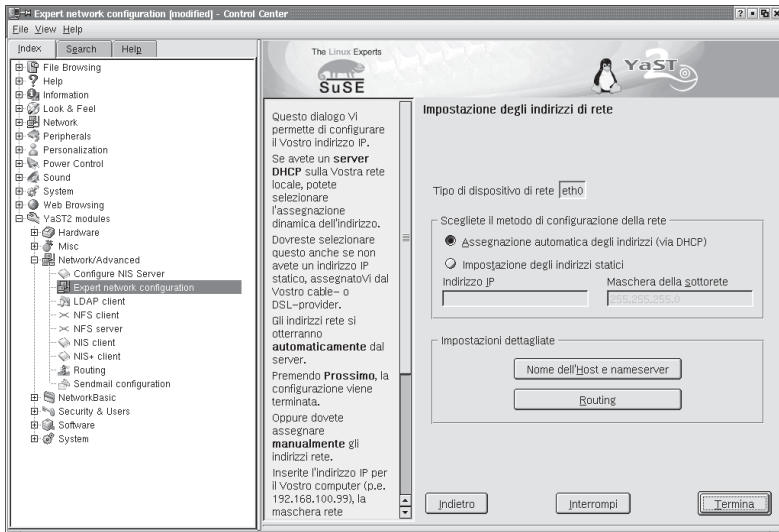
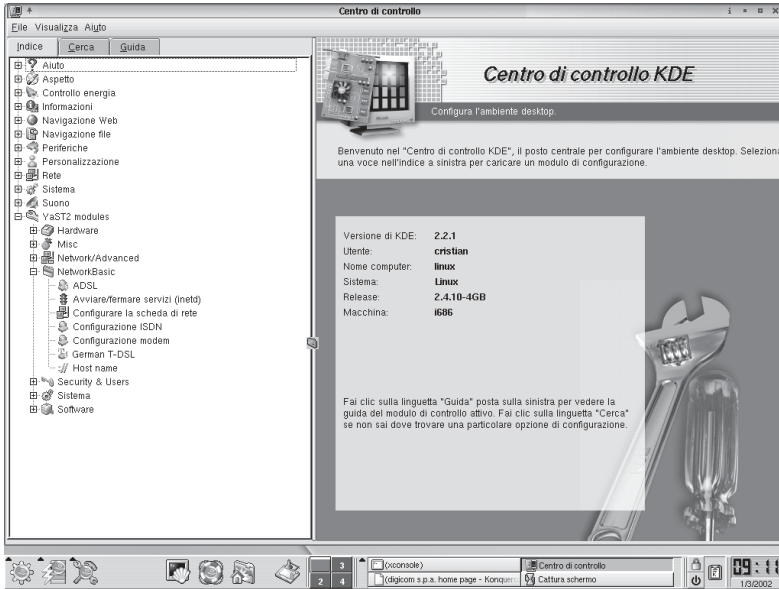


## Linux

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**.



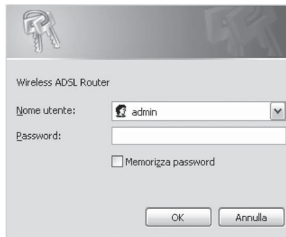
### 3.2. ACCESSO ALLA CONFIGURAZIONE

Per accedere alla configurazione è necessario configurare sul PC un indirizzo IP compatibile con quello impostato nel dispositivo.

Impostate il PC nel seguente modo\*:

<b>Indirizzo IP</b>	<b>192.168.1.2</b>
<b>Subnet mask</b>	<b>255.255.255.0</b>
<b>Gateway</b>	<b>192.168.1.254</b>
<b>DNS</b>	<b>Forniti dal vostro ISP</b>

Lanciate il vostro Browser Internet (IE, Netscape, Mozilla, ...) ed accedete alla pagina: <http://192.168.1.254>  
Verrà visualizzata una finestra simile alla seguente:



Wireless ADSL Router

Nome utente:

Password:

Memorizza password

OK Annulla

Inserite come nome utente **admin** e come password **admin**.

Cliccate sul tasto **OK** per accedere alla configurazione.

#### **Reset alla configurazione di default tramite il tasto di reset**

1. Attendere che il router sia completamente avviato (circa 90-120 sec) dall'accensione.
2. Premere il tasto di reset e mantenerlo premuto per 6 secondi.
3. Rilasciare il tasto.

Il router effettuerà un riavvio e sarà accessibile all'indirizzo 192.168.1.254. Tutte le impostazioni vengono riportate al default di fabbrica.

## Site Map – Menù di configurazione

Terminata la fase di autenticazione per l'accesso alla configurazione è possibile modificare tutte le funzionalità del dispositivo.

I Menù di configurazione sono i seguenti:

### Wizard Setup

**Wizard Setup**

[Wizard Setup](#)

Procedura guidata per la configurazione dell'accesso Internet

### Advanced Setup

**Advanced Setup**

[Password](#)

[LAN](#)

[Wireless](#)

[WAN](#)

[NAT](#)

[Security](#)

[Dynamic DNS](#)

[Time Zone](#)

[Remote Management](#)

Ogni sezione permette la modifica di tutte le funzionalità del dispositivo

### Maintenance

**Maintenance**

[System Status](#)

[DHCP Table](#)

[Wireless](#)

[Diagnostic](#)

[Firmware](#)

Insieme di pagine per monitorare lo stato del dispositivo

## 3.3. WIZARD SETUP

Prima di procedere con la configurazione dell'accesso Internet è necessario verificare di avere a disposizione tutti i dati necessari alla configurazione.

Per configurare un accesso Adsl sono necessari i seguenti dati legati alla linea Adsl da utilizzare:

<b>Protocollo</b>	<b>PPPoA, PPPoE, RFC1483, ENET*</b>
<b>Virtual Circuit</b>	<b>VPI, VCI (se non specificato sono rispettivamente 8 e 35)</b>
<b>Indirizzi IP</b>	<b>Dinamici oppure Specificati</b>
<b>Dati Utente</b>	<b>Username e Password di connessione (per PPPoA e PPPoE)</b>

\*Fare riferimento all'Appendice del manuale in formato PDF presente sul CDROM per maggiori dettagli in merito ai protocolli.

Cliccate sul link [Wizard Setup](#) per iniziare la procedura guidata di configurazione:

### 3.3.1. FASE 1

#### Wizard Setup- ISP Parameters for Internet Access

<b>Mode</b>	<input type="text" value="Routing"/>
<b>Encapsulation</b>	<input type="text" value="PPPoA"/>
<b>Multiplex</b>	<input type="text" value="VC"/>
<b>Virtual Circuit ID</b>	
VPI	<input type="text" value="8"/>
VCI	<input type="text" value="35"/>

#### Mode

Impostate la modalità di funzionamento corretta:

- Routing*                    il dispositivo opera normalmente effettuando routing tra la LAN ed Internet  
*Bridge*                     il dispositivo opera in modalità trasparente (da utilizzare solamente con abbonamenti specifici)

#### Encapsulation

Selezionate il protocollo corretto da utilizzare sulla linea.

- PPPoA, PPPoE*            per abbonamenti con autenticazione (username e password)  
*RFC 1483*                 per abbonamenti con indirizzi IP statici globali\*  
*ENET ENCAP*            per applicazioni di Bridging\*

\* fate riferimento al manuale completo disponibile in formato PDF sul CDROM allegato al prodotto.

#### Multiplex

Selezionate il parametro corretto:

- VC*                         utilizzato solitamente con PPPoA  
*LLC*                        utilizzato solitamente con PPPoE e RFC 1483

#### Virtual Circuit ID

Inserite le coordinate corrette:

- VPI*                        se non specificato diversamente è 8  
*VCI*                        se non specificato diversamente è 35

Cliccate su **Next** per passare alla finestra successiva.

### 3.3.2. FASE 2

#### Impostazioni per PPPoA oppure PPPoE:

*Wizard Setup- ISP Parameters for Internet Access*

---

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

Connection

Connect on Demand: Max Idle Timeout  sec

Nailed-Up Connection

Network Address Translation

▼

---

#### User Name

Inserite il nome utente per l'accesso ad Internet

#### Password

Inserite la password per l'accesso ad Internet

#### IP Address

Solitamente in questi abbonamenti l'indirizzo IP viene assegnato dal Provider dopo l'autenticazione. In questo caso selezionate l'opzione *Obtain an IP Address Automatically*

Se il vostro provider vi ha assegnato un indirizzo IP specifico selezionate *Static IP Address* ed inserite l'indirizzo IP nella casella di testo sottostante.

#### Connection

In questa sezione potete abilitare la connessione permanente ad Internet (*Nailed-Up Connection*) oppure la connessione ad Internet solo a fronte di una richiesta di accesso a risorse esterne *Connected on Demand*; in questo caso impostate il tempo di inattività dati prima della sconnessione Max Idle Timeout (default: 0 sec. = infinito, non sconnettere mai).

#### Network Address Translation

Impostate il tipo di NAT che volete abilitare

<i>None</i>	NAT disabilitato
<i>SUA Only</i>	NAT abilitato per <b>Single User Account</b> (vedi sezione NAT del manuale)
<i>Full Feature</i>	NAT abilitato con funzionalità avanzate (vedi sezione NAT del manuale).

## Impostazioni per RFC 1483:

### Wizard Setup- ISP Parameters for Internet Access

---

IP Address

Network Address Translation

---

### IP Address

Inserite l'indirizzo di WAN del dispositivo; questo indirizzo è specificato nei paramtri per la linea forniti dall'ISP.

### Network Address Translation

Impostate il tipo di NAT che volete abilitare

*None* NAT disabilitato

*SUA Only* NAT abilitato per **Single User Account** (vedi sezione NAT del manuale).

*Full Feature* NAT abilitato con funzionalità avanzate (vedi sezione NAT del manuale).

### 3.3.3. FASE 3

---

La terza finestra di configurazione del Wizard mostra un riepilogo della configurazione impostata.

Selezionate il tasto **Save Configuration** per abilitare le impostazioni selezionate.

Selezionate il tasto **Change LAN Configuration** se dovete modificare le impostazioni di LAN.

### 3.3.4. FASE 4 (CHANGE LAN CONFIGURATION)

#### Wizard Setup- ISP Parameters for Internet Access

LAN IP Address	<input type="text" value="192.168.1.254"/>
LAN Subnet Mask	<input type="text" value="255.255.255.0"/>
<b>DHCP</b>	
DHCP Server	<input type="text" value="ON"/>
Client IP Pool Starting Address	<input type="text" value="192.168.1.50"/>
Size of Client IP Pool	<input type="text" value="100"/>
Primary DNS Server	<input type="text" value="151.99.125.2"/>
Secondary DNS Server	<input type="text" value="212.216.112.112"/>

#### LAN IP Address

Inserite l'indirizzo IP che volete assegnare in LAN al router.

#### LAN Subnet Mask

Inserite la Subnet Mask di LAN del router

#### DHCP Server

*ON*

abilita il servizio DHCP Server. Il router assegna gli indirizzi IP ai client di LAN.

*OFF*

disabilita il servizio DHCP Server. Indirizzi IP di LAN statici o assegnati dal altro DHCP Server.

#### Client IP Pool Starting Address

Impostate l'indirizzo IP di partenza che il DHCP Server assegnerà ai client di LAN.

#### Size of Client IP Pool

Impostate il numero massimo di Indirizzi assegnabili dal DHCP Server

#### Primary DNS Server

Inserite l'indirizzo DNS primario che il DHCP Server assegnerà ai Client

#### Secondary DNS Server

Inserite l'indirizzo DNS secondario che il DHCP Server assegnerà ai Client

Clickate sul tasto **Finish** per terminare la configurazione con Wizard.



## 4. ADVANCED SETUP

# 4

### 4.1. PASSWORD

In questa sezione è possibile personalizzare i dati per l'accesso alla configurazione del dispositivo.

*Password*

---

Old Password

New Password

Retype to confirm

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

---

Inserite la password attuale nel campo *Old Password*, Inserite la nuova password nel campo *New Password* e confermatela riscrivendola nel campo *Retype to confirm*.

Cliccate sul tasto **Apply** per abilitare la nuova password.

### 4.2. LAN

*LAN - Setup*

---

**DHCP**

DHCP

Client IP Pool Starting Address

Size of Client IP Pool

Primary DNS Server

Secondary DNS Server

Remote DHCP Server

**TCP/IP**

IP Address

IP Subnet Mask

RIP Direction

RIP Version

Multicast

---

**DHCP**

*Server*

abilita il servizio DHCP Server

*None*

disabilita il servizio DHCP Server

*Relay*

inoltra le richieste DHCP ad un altro server presente in rete.

**Client IP Pool Starting Address**

Impostate l'indirizzo IP di partenza che il DHCP Server assegnerà ai clienti di LAN.



**Size of Client IP Pool**

Impostate il numero massimo di Indirizzi assegnabili dal DHCP Server

**Primary DNS Server**

Inserite l'indirizzo DNS primario che il DHCP Server assegnerà ai Client

**Secondary DNS Server**

Inserite l'indirizzo DNS secondario che il DHCP Server assegnerà ai Client

**Remote DHCP Server**

Se avete selezionato l'opzione "Relay" inserite qui l'indirizzo IP del DHCP Server raggiungibile in rete.

**IP Address**

Inserite l'indirizzo IP che volete assegnare in LAN al router.

**Subnet Mask**

Inserite la Subnet Mask di LAN del router

**RIP Direction**

Selezionate la modalità di gestione del protocollo RIP:

<i>None</i>	disabilitato
<i>Both</i>	abilitato in invio e ricezione
<i>In Only</i>	abilitata solo la ricezione di pacchetto RIP
<i>Out Only</i>	abilitato solo l'invio di pacchetti RIP

**RIP Version**

Selezionate la versione di RIP che volete utilizzare:

RIP-1  
RIP-2B  
RIP-2M

**Multicast**

<i>None</i>	disabilita le gestione di traffico Multicast
<i>IGMP-v1</i>	abilita la gestione di traffico IGMP versione 1
<i>IGMP-v2</i>	abilita la gestione di traffico IGMP versione 2

Cliccate su **Apply** per attivare le modifiche.

Se avete modificato l'indirizzo IP del dispositivo, chiudete il browser, modificate l'indirizzo IP del PC e rientrate in configurazione puntando al nuovo indirizzo del dispositivo.

### 4.3. WIRELESS

#### Wireless LAN

##### Wireless

Use this screen to configure the wireless LAN parameters.

##### MAC Filter

Use this screen to configure the MAC address filter for wireless LAN security.

Selezionate **Wireless** per configurare la sezione Wireless.

Selezionate **MAC Filter** per abilitare e configurare le restrizioni di accesso basate sul MAC Address dei client.

**Per maggiori dettagli sui livelli di sicurezza Wireless, fate riferimento all'appendice del manuale.**

#### Wireless

##### Wireless LAN- Wireless

ESSID	<input type="text" value="wlan-ap"/>
Hide ESSID	<input type="button" value="No"/>
Channel ID	<input type="button" value="Channel02 2417MHz"/>
<input checked="" type="checkbox"/> RTS/CTS Threshold	<input type="text" value="0"/> (0 ~ 2432)
<input type="checkbox"/> Fragmentation Threshold	<input type="text" value="2432"/> (256 ~ 2432)
WEP Encryption	<input type="button" value="Disable"/>
<small>64-bit WEP: Enter 5 characters or 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).                  128-bit WEP: Enter 13 characters or 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).</small>	
<input checked="" type="radio"/> Key1	<input type="text"/>
<input type="radio"/> Key2	<input type="text"/>
<input type="radio"/> Key3	<input type="text"/>
<input type="radio"/> Key4	<input type="text"/>

#### ESSID

Inserite il nome della rete Wireless.

#### Hide ESSID

Se impostate **Yes** la rete Wireless generata da questo Access Point non sarà visibile eseguendo una ricerca (Site survey) da un Client, solo gli utenti che conoscono a priori il nome della rete potranno collegarsi e farne parte.

#### Channel ID

Selezionate il canale Wireless da utilizzare.

#### RTS/CTS Threshold

Selezionate l'opzione per abilitare la funzione ed impostate il valore che volete sia usato come soglia di attivazione per l'handshake RTS/CTS. Se attivato e configurato saranno necessari n byte per attivare la trasmissione (0=disabilitato).



### Fragmentation Threshold

Selezionate l'opzione per abilitare la funzione ed impostate il valore che volete sia usato come soglia di attivazione per attivazione della frammentazione dei pacchetti. Se attivato, rappresenta la dimensione massima di frammentazione dei pacchetti trasmissibili.

### WEP Encryption

Per abilitare la crittografia, selezionate:

<i>64-bit WEP</i>	abilita la crittografia WEP a 64bit
<i>128-bit WEP</i>	abilita la crittografia WEP a 128bit
<i>None</i>	crittografia disabilitata (non consigliato, vedi nota)

### Key 1~4

Inserite qui la Key da utilizzare per la crittografia; la Key può essere inserita in formato Esadecimale oppure in formato ASCII.

Inserite:

5 caratteri ASCII oppure 10 numeri esadecimali per la crittografia a 64bit

13 caratteri ASCII oppure 26 numeri esadecimali per la crittografia a 128bit.

Se inserite la key in formato ASCII non utilizzate spazi o punteggiature, ad esempio **abcdef**

Se inserite la Key in formato esadecimale, inserite **0x** (Zero x) prima dei valori esadecimali, ad esempio **0xA1B2C3D4E5**

***NOTA: Se non si attiva alcun livello di sicurezza wireless nel router (WEP, MAC filtering o Hide ESSID), la rete sarà raggiungibile da qualsiasi dispositivo di rete wireless nel raggio di copertura radio. Ciò è altamente sconsigliato.***

Active

Action

MAC Address			
1	<input type="text" value="00:00:00:00:00:00"/>	2	<input type="text" value="00:00:00:00:00:00"/>
3	<input type="text" value="00:00:00:00:00:00"/>	4	<input type="text" value="00:00:00:00:00:00"/>
5	<input type="text" value="00:00:00:00:00:00"/>	6	<input type="text" value="00:00:00:00:00:00"/>
7	<input type="text" value="00:00:00:00:00:00"/>	8	<input type="text" value="00:00:00:00:00:00"/>
9	<input type="text" value="00:00:00:00:00:00"/>	10	<input type="text" value="00:00:00:00:00:00"/>
11	<input type="text" value="00:00:00:00:00:00"/>	12	<input type="text" value="00:00:00:00:00:00"/>
13	<input type="text" value="00:00:00:00:00:00"/>	14	<input type="text" value="00:00:00:00:00:00"/>
15	<input type="text" value="00:00:00:00:00:00"/>	16	<input type="text" value="00:00:00:00:00:00"/>
17	<input type="text" value="00:00:00:00:00:00"/>	18	<input type="text" value="00:00:00:00:00:00"/>
19	<input type="text" value="00:00:00:00:00:00"/>	20	<input type="text" value="00:00:00:00:00:00"/>
21	<input type="text" value="00:00:00:00:00:00"/>	22	<input type="text" value="00:00:00:00:00:00"/>
23	<input type="text" value="00:00:00:00:00:00"/>	24	<input type="text" value="00:00:00:00:00:00"/>
25	<input type="text" value="00:00:00:00:00:00"/>	26	<input type="text" value="00:00:00:00:00:00"/>
27	<input type="text" value="00:00:00:00:00:00"/>	28	<input type="text" value="00:00:00:00:00:00"/>
29	<input type="text" value="00:00:00:00:00:00"/>	30	<input type="text" value="00:00:00:00:00:00"/>
31	<input type="text" value="00:00:00:00:00:00"/>	32	<input type="text" value="00:00:00:00:00:00"/>

**Active**

Selezionate Yes per abilitare questa funzionalità.

**Action**

Impostare la regola del filtro:

*Allow Association* permette la connessione ai soli client inseriti nella lista

*Deny Association* blocca l'accesso da parte dei client inseriti nella lista

**MAC Address 1~32**

Inserite qui i valori dei MAC Address dei client.

Cliccate su **Apply** per attivare le impostazioni.



## 4.4. WAN

### WAN Functions

#### WAN Setup

Set up WAN.

Selezionate **WAN Setup** per accedere alla finestra di configurazione della WAN.

La configurazione della sezione di WAN permette la gestione del Multiple PVC, cioè l'utilizzo di più abbonamenti ADSL sul singolo doppino telefonico (linea ADSL).

#### Wan - Wan List

- Route
- Bridge
- Half Bridge

	Name	Active	Mode	VPI	VCI	Encap	IP Address
Profile 1	isp	Yes	Route	8	35	RFC 1483	Static
Profile 2	-	-	-	-	-	-	-
Profile 3	-	-	-	-	-	-	-
Profile 4	-	-	-	-	-	-	-
Profile 5	-	-	-	-	-	-	-
Profile 6	-	-	-	-	-	-	-
Profile 7	-	-	-	-	-	-	-
Profile 8	-	-	-	-	-	-	-

Selezionate l'opzione **Route** per abilitare l'utilizzo di profili Route (PPPoA, PPPoE, RFC1483);

Selezionate l'opzione **Bridge** per abilitare l'utilizzo di profili Bridge (ENET ENCAP);

Selezionate le opzioni **Route** e **Half Bridge** per abilitare l'utilizzo di profili PPPoA oppure PPPoE **Half Bridge**. Vedere l'Appendice per maggiori dettagli su Half Bridge.

Cliccate sul link [Profile 1](#) per configurare la WAN.

Le Opzioni configurabili sono descritte nel capitolo *Wizard Setup*.

**TCP MSS** (Solo per PPPoA e PPPoE, solo a connessione avvenuta)

#### TCP MSS Option

TCP MSS(0 means use default)

bytes

Permette di definire la dimensione massima dei pacchetti.

Secondo RFC879 il valore MSS deve corrispondere a MTU – 40, quindi limitando il valore MSS si limita anche il valore MTU.

Inserendo il valore 0 (zero) si imposta la dimensione di default per l'MSS definito a 1400 bytes.

## 4.5. NETWORK ADDRESS TRANSLATION (NAT)

---

### NAT - Descrizione

Il protocollo NAT (Network Address Translation, RFC 1631) svolge la funzione di modificare l'indirizzo IP di rete di un host, traducendolo (o traslandolo) in un indirizzo IP di rete diverso.

### NAT - Definizioni

Per la descrizione delle funzionalità e modalità del NAT verranno utilizzate alcune definizioni di seguito descritte:

Inside (all'interno)

Outside (all'esterno).

Per inside/outside si intende la posizione dell'host rispetto al router, ad esempio i computer di LAN sono considerati **inside hosts**, mentre i server WEB in Internet sono considerati outside hosts.

Global (globale)

Local (locale)

Per Global/local si intende un indirizzo IP di un host all'interno di un pacchetto, quando il pacchetto attraversa il router, ad esempio il **local address** di un host quando il pacchetto si trova sulla LAN del router ed il **global address** dell'host quando lo stesso pacchetto si trova sulla sezione WAN.

**Nota: inside/outside fa riferimento alla locazione di un host mentre global/local fa riferimento all'indirizzo IP di un host all'interno del pacchetto.**

Detto ciò si definisce che un **inside local address (ILA)** è l'indirizzo IP di un host interno quando il pacchetto è ancora sulla **LAN** interna, mentre un **inside global address (IGA)** è l'indirizzo IP dello stesso host interno quando però il pacchetto è sulla **WAN**.

Definizione	Descrizione
Inside	Si riferisce all'host sulla LAN
Outside	Si riferisce all'host sulla WAN
Local	Si riferisce all'indirizzo nel pacchetto (sorgente o destinazione) quando il pacchetto si trova sulla LAN.
Global	Si riferisce all'indirizzo nel pacchetto (sorgente o destinazione) quando il pacchetto si trova sulla WAN.

### 4.5.1. COSA FA IL NAT

---

Nella sua funzione più elementare, il NAT cambia l'indirizzo IP sorgente di un pacchetto quando questo viene ricevuto da un host interno (inside local address) in un indirizzo diverso (inside global address) prima che il pacchetto venga inviato sulla sezione WAN

Quando la 'risposta' al pacchetto torna al router, il NAT cambia l'indirizzo IP di destinazione (inside global address) reinserendo l'indirizzo IP sorgente originario prima di inviare il pacchetto all'host che aveva effettuato la 'richiesta'.

**Nota: L'indirizzo IP (sorgente o destinazione) di un host esterno non viene mai modificato.**

Gli indirizzi IP globali per gli host interni possono essere staticamente o dinamicamente assegnati dall' ISP.

Inoltre è possibile designare dei server (ad esempio Web o telnet server) per far sì che questi possano essere accessibili dal 'mondo esterno'.

Se non si definiscono server accessibili dall'esterno, il router filtrerà e bloccherà qualsiasi richiesta in ingresso, proteggendo il router da eventuali scan di intrusione.

ss Translator (NAT).

### 4.5.2. COME FUNZIONA IL NAT

Ogni pacchetto ha 2 indirizzi, uno sorgente ed uno di destinazione.

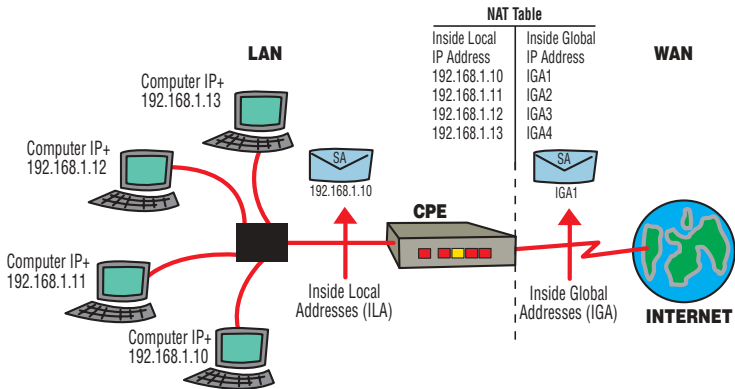
Per i pacchetti uscenti, l'indirizzo ILA (Inside Local Address) è l'indirizzo sorgente della LAN, mentre l'indirizzo IGA (Inside Global Address) è l'indirizzo sorgente sulla WAN.

Per i pacchetti entranti, l'indirizzo ILA è l'indirizzo di destinazione sulla LAN mentre l'indirizzo IGA è l'indirizzo di destinazione sulla WAN.

Il NAT effettua una mappatura di indirizzi IP privati (locali) su indirizzi IP globali necessari per la comunicazione con hosts di altre reti.

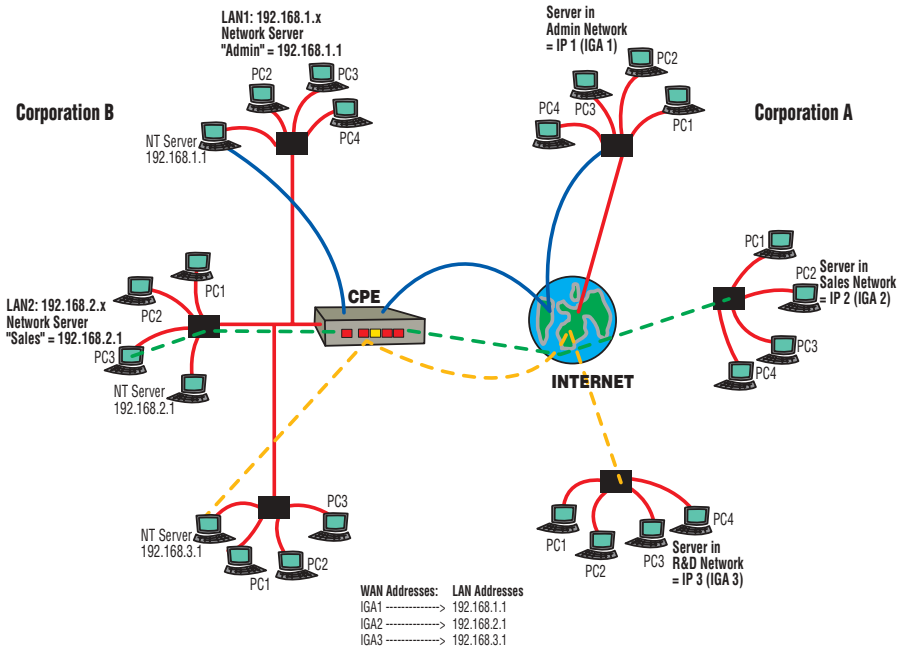
IL NAT rimpiazza l'indirizzo IP sorgente originale (ed il numero di porta TCP o UDP sorgente per i mapping Many-to-One e Many-to-Many Overload) in ogni pacchetto e quindi lo inoltra verso Internet.

Il router tiene traccia degli indirizzi IP originali e delle relative porte in modo da poterli ripristinare una volta che la risposta tornerà indietro, come illustrato nella figura seguente.



### Applicazione NAT

La figura seguente illustra una delle possibili applicazioni NAT, dove 3 diversi segmenti logici di rete locale (attraverso IP aliasing) serviti dal router, possono comunicare con l'esterno su 3 diversi indirizzi IP di WAN (uno per segmento) ed i server di questi possono essere raggiunti attraverso questi ultimi indirizzi globali.



#### 4.5.3. TIPOLOGIE DI NAT MAPPING

Il NAT supporta 5 diverse tipologie di IP/port mapping:

**1. One to One:**

In modalità One-to-One il router mappa un indirizzo IP locale su un indirizzo IP globale.

- IP\_locale1 -> IP\_Globale1
- IP\_locale2 -> IP\_Globale2
- IP\_locale3 -> IP\_Globale3

**2. Many to One:**

In modalità Many-to-One il router mappa molti indirizzi IP locali su un indirizzo IP globale. Questa modalità corrisponde alla modalità SUA (o anche PAT, Port Address Translation).

- IP\_locale1 -> IP\_Globale1
- IP\_locale2 -> IP\_Globale1
- IP\_locale3 -> IP\_Globale1



**3. Many to Many Overload:**

In modalità Many-to-Many Overload il router mappa molti indirizzi IP locali sugli indirizzi IP globali a disposizione in modo dinamico e ridondante.

IP\_locale1 -> IP\_Globale1  
 IP\_locale2 -> IP\_Globale2  
 IP\_locale3 -> IP\_Globale1  
 IP\_locale4 -> IP\_Globale2

**4. Many-to-Many No Overload:**

In modalità Many-to-Many No Overload il router mappa molti indirizzi IP locali sugli indirizzi IP globali a disposizione fino ad esaurimenti di questi ultimi. Una volta effettuato il mapping di tutti gli indirizzi IP globali, ulteriori richieste non vengono servite, a meno che un indirizzo IP globale non venga rilasciato.

IP\_locale1 -> IP\_Globale1  
 IP\_locale2 -> IP\_Globale2  
 IP\_locale3 -> IP\_Globale3  
 IP\_locale4 -> IP\_Globale4  
 IP\_locale5 -> IP\_Globale5  
 IP\_locale6 -> IP\_Globale6  
 IP\_locale7 -> nn  
 IP\_locale8 -> nn  
 ...  
 ...

Terminata la disponibilità di IP Globali, richiesta di accesso Internet della macchina con IP\_locale7 non viene accettata.

**5. Server:**

Questa modalità permette di definire quali server (quali servizi) locali saranno accessibili dal mondo esterno attraverso il NAT.

**4.5.4. SUA SERVER**

Un set di SUA server è una lista di server di LAN (WWW, TFTP, ecc. dietro al NAT) che l'utente può rendere "visibili" da Internet, anche se l'intera rete LAN appare all'esterno, per effetto del NAT stesso, come una singola stazione.

E' possibile definire una singola porta, oppure un range di porte, che devono essere inoltrate, oltre l'indirizzo IP di LAN del server al quale si vogliono recapitare pacchetti delle suddette porte.

Il numero di porta identifica di fatto un servizio, ad esempio la porta 80 per il servizio WEB, la porta 21 per il servizio FTP e così via. In alcuni casi una singola macchina può svolgere più servizi contemporaneamente (vedi il caso di un server che è contemporaneamente server web e server FTP), oppure un servizio può utilizzare più di una porta. Altre volte non è possibile conoscere il numero esatto di porte utilizzato da un'applicazione. In tal caso è preferibile definire un range di porte.

L'utente può mappare una singola porta (o un range) con un indirizzo IP di LAN, facendo sì che ogni pacchetto ricevuto sulla WAN che contenga l'informazione della porta in oggetto gli venga automaticamente inoltrato.

**Default Server IP Address**

Oltre alla lista di porte definibili, il NAT supporta anche una funzionalità aggiuntiva, chiamata Default server IP address oppure DMZ. Definendo un indirizzo IP in questa funzione, tutti i pacchetti destinati a porte non altrimenti definite (sconosciute), verranno inoltrati a questo server. Questa modalità è da utilizzarsi solamente quando non si hanno altre possibilità.

**Attenzione: L'uso di questa funzione espone il server in modo completo, generando un potenziale rischio di sicurezza.**

Se l'indirizzo per il Default Server non è definito, I pacchetti verranno semplicemente scartati.

Una lista dei servizi e relative porte più comuni è riportato nell'Appendice A di questo manuale. Per ulteriori informazioni fare riferimento all'RFC 1700.

**NAT - Mode**

---

Network Address Translation

None

SUA Only [Edit Details](#)

Full Feature [Edit Details](#)

---

**NAT - Mode**

**Network Address Translation**

Impostate il tipo di NAT che volete abilitare

- None* NAT disabilitato
- SUA Only* NAT abilitato per **Single User Account**
- Full Feature* NAT abilitato con funzionalità avanzate.

Cliccate su **Apply** per abilitare l'opzione selezionata.  
 Cliccate sul link **Edit Detail** per configurare le opzioni del tipo di NAT impostato.

**4.5.4.1. SUA Only**

*NAT - Edit SUA/NAT Server Set*

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	0	0	0.0.0.0
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

La funzione **Edit SUA/NAT Server Set** permette ad utenti connessi in Internet di avere accesso a Server presenti nella LAN locale (funzione Virtual Server).

Selezionate un range di porte indicando la porta di inizio (*Start Port No.*) e la porta finale del range (*Stop Port No.*); Indicate l'indirizzo IP del Server collegato in LAN nel campo *IP Address*.



La regola n°1 è riservata alla funzione solitamente chiamata **DMZ**.

Definendo un indirizzo IP in questa funzione, tutti i pacchetti destinati a porte non altrimenti definite (sconosciute) verranno inoltrati a questo server. Questa modalità è da utilizzarsi solamente quando non si hanno altre possibilità.

**Attenzione: L'uso di questa funzione espone il server in modo completo, generando un potenziale rischio di sicurezza.**

Se l'indirizzo non è definito, I pacchetti verranno semplicemente scartati.

**4.5.4.2. Full Features**

Questo tipo di NAT permette la gestione di diversi indirizzi IP statici sul lato WAN.

NAT - Address Mapping Rules

	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
Rule 1	...	...	...	...	-
Rule 2	...	...	...	...	-
Rule 3	...	...	...	...	-
Rule 4	...	...	...	...	-
Rule 5	...	...	...	...	-
Rule 6	...	...	...	...	-
Rule 7	...	...	...	...	-
Rule 8	...	...	...	...	-
Rule 9	...	...	...	...	-
Rule 10	...	...	...	...	-

E' possibile aggiungere fino a 10 regole differenti.

Selezionate la regola che volete aggiungere cliccando sul link nella colonna di sinistra ("Rule 1", "Rule2",...)

**4.5.4.3. Type One-to-One**

NAT - Edit Address Mapping Rule 1

Type	One-to-One <input type="button" value="v"/>
Local Start IP	<input type="text" value="0.0.0.0"/>
Local End IP	<input type="text" value="N/A"/>
Global Start IP	<input type="text" value="0.0.0.0"/>
Global End IP	<input type="text" value="N/A"/>
Server Mapping Set	<input type="text" value="N/A"/> <input type="button" value="Edit Details"/>

Questa regola effettua un associazione UNO ad UNO di un indirizzo IP Locale (Privato di LAN) con un indirizzo IP Globale (Pubblico di WAN).

Inserite l'indirizzo Privato in **Local Start IP** e l'indirizzo Pubblico in **Global Start IP**.

#### 4.5.4.4. Type Many-to-One

##### NAT - Edit Address Mapping Rule 1

Type	Many-to-Many Overload ▼
Local Start IP	0.0.0.0
Local End IP	0.0.0.0
Global Start IP	0.0.0.0
Global End IP	0.0.0.0
Server Mapping Set	N/A ▼ <a href="#">Edit Details</a>

Questa regola effettua un associazione di un gruppo di indirizzi IP Locali con un solo indirizzo IP Globale. Il funzionamento di questo tipo di NAT è equivalente al SUA; in questa modalità è però possibile creare più regole e ripartire l'accesso Internet su più indirizzi.

Indicate il gruppo di indirizzi IP Privati specificandone il range con **Local Start IP** e **Local End IP**, indicate l'indirizzo pubblico in **Global Start IP**.

#### 4.5.4.5. Type Many-to-Many Overload

##### NAT - Edit Address Mapping Rule 1

Type	Many-to-Many No Overload ▼
Local Start IP	0.0.0.0
Local End IP	0.0.0.0
Global Start IP	0.0.0.0
Global End IP	0.0.0.0
Server Mapping Set	N/A ▼ <a href="#">Edit Details</a>

Questa regola effettua un associazione di un gruppo di indirizzi IP Locali con un gruppo di indirizzi IP Globali, l'associazione viene effettuata dinamicamente in base alle richieste di accesso effettuate dai PC di LAN.

Indicate il range di IP Locali utilizzando **Local Start IP** e **Local End IP**; indicate il range di IP Globali utilizzando **Global Start IP** e **Global End IP**.

### 4.5.4.6. Type Many-to-Many no Overload

NAT - Edit Address Mapping Rule 1

Type	Many-to-Many No Overload
Local Start IP	0.0.0.0
Local End IP	0.0.0.0
Global Start IP	0.0.0.0
Global End IP	0.0.0.0
Server Mapping Set	N/A <a href="#">Edit Details</a>

Questa regola effettua un associazione di un gruppo di indirizzi IP Locali con un gruppo di indirizzi IP Globali, l'associazione viene effettuata dinamicamente in base alle richieste di accesso effettuate dai PC di LAN. A differenza della modalità *Overload* terminata l'assegnazione di tutti gli indirizzi, nessuna altra macchina potrà accedere ad Internet.

Indicate il range di IP Locali utilizzando **Local Start IP** e **Local End IP**; indicate il range di IP Globali utilizzando **Global Start IP** e **Global End IP**.

### 4.5.4.7. Type Server

NAT - Edit Address Mapping Rule 1

Type	Server
Local Start IP	N/A
Local End IP	N/A
Global Start IP	0.0.0.0
Global End IP	N/A
Server Mapping Set	2 <a href="#">Edit Details</a>

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.
1	All ports	All ports
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0

Questa regola permette di definire dei Virtual Server utilizzando diversi indirizzi IP Globali.

Indicate l'indirizzo IP Globale in **Global Start IP**  
 Selezionate da **Server Mapping Set** il numero della regola del Virtual Server da utilizzare.

Cliccate sul link [Edit Details](#) per configurare le regole del Virtual Server.

## 4.6. SECURITY

*Internet Security*

---

Your device provides the following filter rules

<input type="checkbox"/> Telnet	Telnet traffic is blocked from the WAN to the LAN
<input type="checkbox"/> FTP	FTP traffic is blocked from the WAN to the LAN
<input type="checkbox"/> TFTP	TFTP traffic is blocked from the WAN to the LAN
<input type="checkbox"/> Web	Web traffic is blocked from the WAN to the LAN
<input type="checkbox"/> SNMP	SNMP traffic is blocked from the WAN
<input type="checkbox"/> Ping	Ping traffic is blocked from the WAN

In questa sezione è possibile bloccare l'accesso dall'esterno di alcuni servizi base. Selezionate i servizi che volete bloccare.

## 4.7. DYNAMIC DNS

*Dynamic DNS*

---

Active

Service Provider

Host Name

E-mail Address

User

Password

Enable Wildcard

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 di **Dynamic DNS**, dopo aver effettuato una registrazione gratuita a questi servizi potete attivare un vostro dominio del tipo `vostronome.dyndns.org`

Abilitate il servizio selezionando **Active**.

Selezionate il vostro server del servizio da **Service Provider** ed inserite i dati del vostro account.

La funzionalità WildCard deve essere abilitata anche nell'abbonamento gratuito sottoscritto con il provider *dyndns*. Il vostro dominio diventa `xxxxxxx.vostronome.dyndns.org` xxxxxx rappresenta qualsiasi carattere; solitamente viene utilizzato per rendere disponibile il dominio nella forma `www.vostronome.dyndns.org`

Ogni volta che il router rileva un indirizzo IP differente sulla WAN effettua una nuova registrazione al server DDSN ([www.dyndns.org](http://www.dyndns.org)), pertanto qualsiasi sia l'indirizzo IP del router i PC collegati in Internet potranno raggiungere l'indirizzo IP del vostro Router utilizzando il dominio che avete registrato.

## 4.8. TIME ZONE

*Time Zone*

---

**Time Server**

Use Time Server when Bootup  NTP (RFC-1305)

Time Server IP Address

Time Zone

Daylight Saving

Start Date  month  day

End Date  month  day

Calibrate system clock with Time Server now.  
(Attention! This may take up to 60 seconds if Time Server is unreachable).

**Date**

Current Date

New Date (yyyy-mm-dd)

**Time**

Current Time

New Time

---

In questa finestra è possibile attivare la sincronizzazione della date e dell'ora con un Time Server.

### Use Time Server when Bootup

Selezionate il tipo di Time Server

### Time Server IP Address

Inserite l'indirizzo IP del Time Server (potete utilizzare quello dell'immagine)

### Time Zone

Selezionate il fuso orario

### Daylight Savings

Abilitate quest'opzione per aggiornare automaticamente il dispositivo all'ora legale.

Inserite in *Start Date* ed in *End Date* il periodo in cui è attiva l'ora legale.

### Calibrate system clock with Time Server Now

Selezionate quest'opzione per forzare una sincronizzazione con il Time Server impostato.

Se non utilizzate un Time Server, potete regolare Data ed Ora utilizzando i campi **Date** e **Time**.

## 4.9. REMOTE MANAGEMENT

### Remote Management Control

Server Type	Access Status	Port	Secured Client IP
Telnet	LAN Only	23	0.0.0.0
FTP	LAN Only	21	0.0.0.0
Web	LAN Only	80	0.0.0.0

In questa sezione è possibile abilitare l'accesso alla configurazione del dispositivo.

Per ogni servizio *Telnet*, *FTP*, *Web* è possibile indicare la porta ed eventualmente l'unico indirizzo IP che può accedere.

In **Access Status** potete definire dove il servizio viene reso accessibile:

<i>None</i>	servizio disabilitato
<i>LAN Only</i>	servizio abilitato solo dalla LAN
<i>WAN Only</i>	servizio abilitato solo dalla WAN (Internet)
<i>All</i>	servizio abilitato sia dalla LAN che dalla WAN.

### 4.9.1. LIMITAZIONI DEL REMOTE MANAGEMENT

Il Remote management via LAN o WAN non funzionerà se:

1. E' stata disattivata questa funzione in uno dei menu del Remote management
2. E' attivo un filtro che blocca Telnet, FTP o servizio Web.
3. L'indirizzo IP del Secured Client non corrisponde a quello inserito.
4. E' attiva una sessione di console locale.
5. E' già attiva una sessione di remote management dello stesso tipo (web, FTP o Telnet).
6. Ha luogo una sessione Web quando è attiva una sessione Telnet. La sessione Telnet viene terminata quando viene iniziata una sessione Web.
7. Si tenta di attivare una sessione Telnet quando è già attiva una sessione Web. La sessione Telnet non si attiverà finchè non viene terminata la sessione Web.

### 4.9.2. REMOTE MANAGEMENT E NAT

Se è attivo il NAT, utilizzare l'indirizzo IP di WAN del router per la configurazione dalla WAN, l'indirizzo IP di LAN del router per la configurazione da LAN.

### 4.9.3. TIMEOUT

Il router termina le sessioni di management dopo 5 minuti (300 secondi) di inattività delle connessioni via console, telnet, web o FTP. Il router effettuerà un log out automatico dell'utente se non rileva attività nel periodo definito.

## 4.10. UPnP

---

### UPnP

- Enable the Universal Plug and Play(UPnP) Service
- Allow users to make configuration changes through UPnP

Apply Reset

### 4.10.1. DESCRIZIONE

---

Il protocollo Universal Plug and Play (UPnP) è uno standard per l'open networking distribuito ed utilizza il protocollo TCP/IP per connessioni peer-to-peer tra dispositivi.

Un dispositivo UPnP può, in modo dinamico ed autonomo, partecipare a delle reti, ottenere un indirizzo IP, "mostrare" le proprie funzionalità ed apprendere le funzionalità degli altri dispositivi UPnP raggiungibili in rete. Inoltre può sconnettersi da una rete in modo automatico e controllato quando non utilizzato.

#### Come sapere se si sta utilizzando l'UPnP?

Un dispositivo UPnP viene identificato con una icona nel Pannello delle Risorse di rete di Windows XP o Me. Selezionando l'icona si accede alle informazioni e Proprietà del dispositivo.

### 4.10.2. NAT TRAVERSAL

---

La funzione di UPnP NAT traversal automatizza il processo che permette ad una applicazione di funzionare attraverso il NAT.

I dispositivi di rete UPnP network possono auto-configurarsi l'indirizzo di rete e rendere nota la loro presenza in rete condividendo informazioni relative ai servizi supportati con altri dispositivi UPnP.

NAT Traversal permette

- Il Port Mapping Dinamico
- L'apprendimento di indirizzi IP
- L'assegnazione di tempi e periodi di validità dei port mapping

Windows Messenger è un classico esempio di applicazione che supporta NAT traversal e UPnP.

#### Precauzioni nell'utilizzo di UPnP

La natura di automaticità delle applicazioni NAT Traversal e la capacità di attivare automaticamente dei servizi può comportare un rischio di sicurezza, in quanto le informazioni di rete e loro configurazioni possono essere accessibili.

Tutti i dispositivi UPnP possono comunicare tra di loro senza alcuna configurazione aggiuntiva.

**NOTA: Disabilitate questa funzione se non intendete utilizzarla**

Selezionate **Enable the Universal Plug and Play(UPnP) Service** per abilitare il servizio.

Selezionate **Allow user to make configuration changes through UPnP** per permettere la configurazione del dispositivo basandosi su questo servizio.

## 4.11. MAINTENANCE

---

### 4.11.1. SYSTEM STATUS

---

Questa finestra mostra una serie di informazioni sull'hardware e alla configurazione delle 3 interfacce del dispositivo. Cliccando sul tasto **Show Statistic** è possibile verificare le informazioni relative al traffico gestito dal dispositivo.

### 4.11.2. DHCP TABLE

---

In questo menù è disponibile l'elenco di macchine che hanno ricevuto un indirizzo IP dal DHCP Server integrato nel dispositivo.

### 4.11.3. WIRELESS

---

#### Association List

Mostra l'elenco di tutti i Client connessi all'Access Point integrato

#### Channel Usage Table

Il dispositivo esegue una scansione della rete Wireless ed indica quali canali sono liberi.

### 4.11.4. DIAGNOSTIC

---

#### General

Offre la possibilità di eseguire dei **Ping** direttamente dal router.

Cliccando il tasto **Reset System** viene riavviato il dispositivo (equivalente allo spegnimento e riaccensione del router).

#### DSL Line

Offre una serie di tools per i test sulla qualità della linea.

### 4.11.5. FIRMWARE

---

#### FIRMWARE

---

##### Firmware Upgrade

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click **UPLOAD**.

File Path:




#### CONFIGURATION FILE

---

Click Reset to clear all user-defined configurations and return to the factory defaults.

Cliccate sul tasto **Sfogle...** per selezionare il file di aggiornamento e cliccate sul tasto di **Upload** per aggiornare il Firmware del dispositivo.

**Attenzione, utilizzare un file errato durante l'aggiornamento può provocare un BLOCCO IRREVERSIBILE del dispositivo.**

**NON effettuate alcun aggiornamento se non necessario**

**NON effettuate alcun aggiornamento se il file non è stato rilasciato per questo prodotto da Digicom S.p.a.**

Cliccate sul tasto **Reset** per riportare il router alle impostazioni di fabbrica.

#### **4.12. IP ALIAS**

---

Il dispositivo supporta fino a 3 indirizzi IP differenti (ALIAS) per la sezione LAN.

*Fare riferimento al "Command Line Reference Manual" per la configurazione.*

#### **4.13. IP POLICY ROUTING (IPPR)**

---

Il dispositivo supporta la funzione di IP Policy Routing (fino a 12 regole).

Normalmente il routing avviene basandosi sull'indirizzo di destinazione di un pacchetto ed il router utilizza l'instradamento più breve per raggiungere la destinazione.

IPPR permette di "alterare" il contenuto del pacchetto per effettuare l'instradamento secondo delle regole definibili dall'utente.

*Fare riferimento al "Command Line Reference Manual" per la configurazione.*

## A. APPENDICE

### A.1. PROTOCOLLI ED ENCAPSULATION

#### Encapsulation

L'encapsulation è un parametro fondamentale. L'impostazione deve corrispondere a quella effettuata dall'ISP sul lato centro.

#### PPPE – PPP over Ethernet

L'encapsulation PPPoE permette di effettuare accessi ad Internet comparabili alle connessioni Dial-up che utilizzano PPP. E' possibile effettuare tariffazione e controllo di accesso. Tecnicamente il router provvede ad effettuare un bridging della sessione PPP over Ethernet (RFC 2516) dal vostro computer, su un PVC ATM (Permanent Virtual Circuit) che vi collega ad un ADSL Access Concentrator che "termina" la sessione PPP dall'altro lato. Un PVC può supportare tutte le sessioni PPP provenienti dalla vostra LAN.

#### PPPoA – PPP over ATM (Adaptation Layer 5 - AAL5)

L'encapsulation PPPoA. L'encapsulation PPPoE permette di effettuare accessi ad Internet comparabili alle connessioni Dial-up che utilizzano PPP. E' possibile effettuare tariffazione e controllo di accesso. Tecnicamente il router provvede ad incapsulare la sessione PPP basata su RFC1483 e ad inoltrarla al DSLAM dell'ISP (Digital Access Multiplexer).

#### RFC 1483

L'encapsulation RFC 1483 definisce due modalità di Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). Il primo metodo permette di multiplexare molteplici protocolli su un singolo circuito virtuale ATM; in questo caso si parla di LLC-based multiplexing.

Il secondo metodo assume che ogni protocollo è veicolato su un diverso circuito virtuale ATM; in questo caso si parla di VC-based multiplexing.

#### ENET ENCAP

L'encapsulation definita MAC Encapsulated Routing Link Protocol (o ENET ENCAP) viene implementata solamente con il protocollo di rete IP. I pacchetti IP sono ruotati tra le interfacce LAN e WAN del router e formattati in modo che possano essere intelleggibili in un ambiente basato su Bridge. Tecnicamente il router incapsula le frame Ethernet ruotate in celle ATM veicolate in bridge. L'encapsulation ENET ENCAP richiede che venga specificato l'indirizzo IP di un Ethernet Encapsulation Gateway.

#### Multiplexing

Esistono due convenzioni per identificare quale protocollo è veicolato da un circuito virtuale (VC). Questa impostazione deve corrispondere a quella utilizzata dall'ISP.

#### VC-based Multiplexing (VCMUX)

In questo caso, previo mutuo accordo, ogni protocollo è veicolato su uno specifico circuito virtuale, ad esempio protocollo IP su VC0, protocollo IPX su VC1 ecc.

#### LLC-based Multiplexing

In questo caso un singolo circuito virtuale (VC) veicola molteplici protocolli, che sono identificati negli header dei pacchetti che li contengono.

#### VPI e VCI

Virtual Path Identifier (VPI) e Virtual Channel Identifier (VCI) identificano il circuito sul quale il router comunica con la rete ATM e l'ISP. Il range valido per VPI va da 0 a 255, l'impostazione più comune è 8. Il range valido per VCI va da 32 a 65535 (0 - 31 riservati per gestione locale del traffico ATM).

## A.2. PPP HALF BRIDGE

---

Quando si attiva l'opzione PPP Half Bridge, il router si rende di fatto "invisibile" alla rete WAN.

Il DHCP server provvederà a duplicare (inoltrare) l'indirizzo IP di WAN assegnato dall'ISP al client di LAN ad esso collegato. La modalità Half bridge è possibile solamente con abbonamenti che prevedono un singolo indirizzo IP; non è possibile utilizzarlo su abbonamenti multi-indirizzo.

La modalità Half bridge viene utilizzata quando non si vuole utilizzare il NAT o NAPT ed una singola stazione è connessa al router.

### **Quando utilizzare la modalità Half Bridge**

Quando si utilizza un firewall a protezione della rete, la modalità half bridge farà sì che l'indirizzo IP assegnato dall'ISP venga di fatto utilizzato dal firewall, e di conseguenza il firewall apparirà su Internet con questo indirizzo. Questa configurazione permette di definire sul firewall il controllo totale delle sessioni in ingresso ed uscita, basandosi sull'indirizzo globale di WAN.

In alcuni casi, le applicazioni utilizzate sui computer non sono compatibili con il protocollo NAT, e richiedono di operare con un indirizzo IP globale per poter funzionare. Tuttavia questa evenualità è sempre meno frequente. Prima di decidere di utilizzare la modalità half bridgeverificate se l'applicazione può funzionare utilizzando una funzionalità virtual server offerta dal router. L'Uso del NAT/NAPT è preferibile perché fornisce una prima linea di difesa dagli attacchi degli hacker e permette la connesione di più computer.

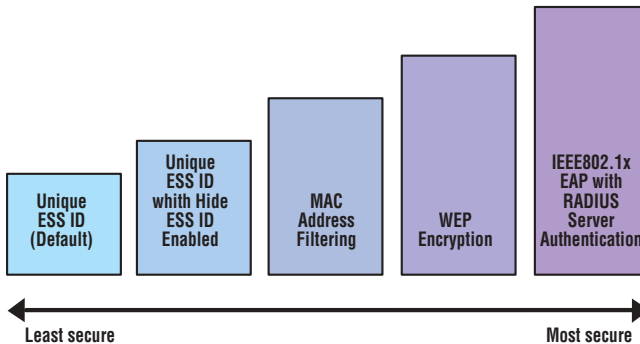
### A.3. LIVELLI DI SICUREZZA WIRELESS

La sicurezza Wireless è di fondamentale importanza per proteggere le comunicazioni ed i dati trasferiti tra i client wireless, gli Access Point e la rete cablata.

Il router implementa la crittografia dei dati WEP che è un primo e significativo livello di protezione delle comunicazioni wireless. E' possibile attivare anche la funzione di Hide ESSID.

E' a discrezione dell'utilizzatore l'implementazione di ulteriori livelli di sicurezza, se questi sono ritenuti necessari.

La figura seguente mostra i possibili livelli di sicurezza che possono essere messi in atto su una rete Wireless.



#### Unique ESSID

La rete ed i suoi componenti devono condividere un ESSID univoco.

#### Unique ESSID with Hide ESSID enabled

La rete ed i suoi componenti devono condividere un ESSID univoco. L'ESSID viene "nascosto" in quanto non trasmesso nei pacchetti Wireless e pertanto non rilevabile dai client tramite una ricerca degli Access Point disponibili nel raggio di copertura radio.

E' necessario conoscere a priori l'ESSID per poter accedere alla rete wireless.

#### MAC address filtering

L'utente può restringere l'accesso alla rete wireless solamente ai client wireless dei quali il MAC address è sia stato preventivamente e manualmente inserito in una lista.

#### WEP Encryption

I pacchetti wireless ed i dati in essi contenuti vengono criptati secondo delle chiavi a 64 o 128 bit preventivamente e manualmente configurate. I dati, anche se ricevuti sono non intelleggibili da parte di una stazione wireless che non ha le stesse impostazioni WEP.

#### IEEE802.1x EAP with Radius Server Authentication

L'accesso alla rete è gestito dai servizi EAP con chiavi crittografiche dinamiche e da un servizio di autenticazione client basato su server RADIUS.

**NOTA: Se non si attiva alcun livello di sicurezza wireless nel router (WEP, MAC filtering o Hide ESSID), la rete sarà raggiungibile da qualsiasi dispositivo di rete wireless nel raggio di copertura radio. Ciò è altamente sconsigliato.**



21010 Cardano al Campo VA  
via A. Volta 39

