# ADSL2/2+
## *11n Wireless ROUTER*

- Collega la tua rete ad Internet via ADSL fino a **24 Mbit/s**
- Realizza una rete **Wireless a 300M** con l'Access Point 11n integrato
- **WPS (Wi-Fi Protected Setup)**, configurazione crittografia wireless con la semplice pressione di un tasto
- **Switch 4 porte 10/100** Autosensing MDI/MDI-X integrato


Michelangelo Wave 300

**Manuale Operativo**
rev. 1.0 del 05/2008

**802.11n 300Mbps**

# INDICE

## PRECAUZIONI

Al fine di salvaguardare la sicurezza, l'incolumità dell'operatore e il funzionamento dell'apparato, devono essere rispettate le seguenti norme per l'installazione. Il sistema, compresi i cavi, deve venire installato in un luogo privo o distante da:

- 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.

**CONDIZIONI AMBIENTALI**
Temperatura ambiente da 0 a +45°C Umidità relativa da 20 a 80% n.c.
Si dovrà evitare ogni cambiamento rapido di temperatura e umidità.
**PULIZIA DELL'APPARATO**
Usate 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 (VA) Italy dichiariamo sotto la nostra esclusiva responsabilità, che il prodotto a nome **Michelangelo Wave 300** 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), Decreto Legislativo del 9 maggio 2001, n.269, (G.U. n. 156 del 7-7-2001).
  Come designato in conformità alle richieste dei seguenti Standard di Riferimento o ad altri documenti normativi:
  EN 300 328
  EN 301 489-01
  EN 301 489-017
  EN 55022
  EN 55024
  EN 61000-3-2
  EN 61000-3-3
  EN 60950-1

CE (!)

Questa apparecchiatura può essere utilizzata nei seguenti paesi: IT, DE, ES, PT, BE, NL, GB, IE, DK, GR, CH

## ASSISTENZA E CONTATTI

La maggior parte dei problemi può essere risolta consultando il capitolo F.A.Q. del manuale utente, oppure facendo riferimento alla sezione Supporto > F.A.Q. presente sul nostro sito www.digicom.it.
Se, dopo un'attenta lettura delle procedure ivi descritte, non riusciste comunque a risolvere il problema, vi invitiamo a contattare l'assistenza Digicom.

**E-mail: support@digicom.it**

**È possibile stampare il modulo di "RICHIESTA ASSISTENZA" scaricandolo dal nostro sito Internet www.digicom.it nella sezione Supporto > Riparazioni e Garanzia, o prelevando il file PDF dal CD-ROM incluso nella confezione (ove presente).**

# INFORMAZIONI RELATIVE ALL'UTILIZZO DI QUESTO APPARATO WIRELESS (RADIO LAN)

Questo apparato è conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Pertanto, in accordo con quanto previsto dall'art. 6.3 del D.Lgs. 9.5.01 n.269, si informa che l'uso di questo apparato è regolamentato da:

- D.Lgs 1.8.2003, n.259, art. 104 (attività soggette ad autorizzazione generale) e art. 105 (libero uso), per uso privato.
- D.M. 28/5/03, per la fornitura al pubblico dell'accesso R-LAN alle reti e servizi di telecomunicazione.

**Marcatura**

Il prodotto riporta sull'apparato, sulla confezione e sul libretto di istruzioni, il simbolo di allarme  in quanto esiste una restrizione all'uso dell'apparecchiatura.

**Restrizioni Nazionali**

Questo prodotto è soggetto a restrizioni nazionali per l'utilizzo all'interno della comunità europea ed altri paesi extracomunitari.
Nella maggior parte dei paesi appartenenti alla Comunità Europea la banda di frequenza 2400-2483,5 MHz è stata liberalizzata per l'utilizzo di Wireless LAN.
Tuttavia in alcuni paesi vigono delle restrizioni sull'uso di frequenze, canali, potenza emessa o utilizzo in aree pubbliche.
Di seguito una lista di restrizioni esistenti al momento della redazione di questo documento. La lista potrebbe modificarsi ed evolvere nel tempo, perciò consigliamo l'utilizzatore ad informarsi presso gli organi e le autorità competenti in ambito locale sullo stato ultimo della regolamentazione per l'utilizzo delle frequenze Wireless LAN 2.4GHz.

Note

- Pur non appartenendo alla Comunità Europea, i paesi: Norvegia, Svizzera e Liechtenstein applicano la direttiva europea 1999/5/EC.
- I limiti massimi per la potenza irradiata sono di 100mW specificati in EIRP (Effective Isotropic Radiated Power) ad eccezione dei paesi dove sono previste delle limitazioni sulla potenza irradiata. Il livello EIRP di un dispositivo può essere calcolato sommando il guadagno dell'antenna utilizzata (specificato in dBi) al valore della potenza emessa disponibile al connettore d'antenna (specificato in dBm).

**Italia**

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia.
Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale".
Consultare il sito http://www.comunicazioni.it/it per maggiori informazioni.

**Belgio**

Il Belgian Institute for Postal Services and Telecommunications (BIPT) deve essere informato di qualsiasi link Wireless in Outdoor che raggiunga un raggio superiore ai 300 metri.
Consultare il sito http://www.bipt.be per maggiori dettagli.

**Francia**

Nella banda di frequenza 2400-2483,5 MHz la potenza di emissione è limitata a 10 mW EIRP quando il prodotto è utilizzato in esterno (Outdoor). Non ci sono restrizioni per l'utilizzo nella restante parte della banda 2.4Ghz o nell'utilizzo in interni (Indoor).
Consultare il sito http://www.arcep.fr per maggiori informazioni.

**Uso di antenne esterne**

Il prodotto è conforme alle norme e limiti della normativa vigente quando utilizzato con l'antenna fornita a corredo. Nel caso di rimozione dell'antenna originale ed utilizzo di una antenna diversa, l'utilizzatore deve assicurarsi di non infrangere o superare i limiti o le restrizioni imposte in ambito interno ed esterno dalle normative vigenti nel paese.

**Impostazione del Regulatory Domain (canali utilizzabili)**

I prodotti vengono forniti con l'impostazione del Regulatory Domain per la Comunità Europea (ETSI). Il Regulatory Domain definisce quali canali sono ammessi all'uso in quel specifico contesto locale (Paese o lista di paesi).
Per gli apparati che permettono la modifica di tale impostazione, l'utilizzatore deve assicurarsi di non infrangere le limitazioni imposte sull'uso dei canali (e relative potenze) vigenti nel paese.

**INFORMAZIONE AGLI UTENTI**

ai sensi dell'art. 13 del Decreto Legislativo 25 Luglio 2005, n.151 "Attuazione delle Direttive 2002/95/CE, 2002/96/CE e 2003/108/CE, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonchè allo smaltimento dei rifiuti".

Il simbolo del cassonetto barrato riportato sull'apparecchiatura o sulla sua confezione indica che il prodotto alla fine della propria vita utile deve essere raccolto separatamente dagli altri rifiuti.

L'utente dovrà, pertanto, conferire l'apparecchiatura giunta a fine vita agli idonei centri di raccolta differenziata dei rifiuti elettronici ed elettrotecnici, oppure riconsegnarla al rivenditore al momento dell'acquisto di una nuova apparecchiatura di tipo equivalente, in ragione di uno a uno.

L'adeguata raccolta differenziata per l'avvio successivo dell'apparecchiatura dismessa al riciclaggio, al trattamento e allo smaltimento ambientalmente compatibile contribuisce ad evitare possibili effetti negativi sull'ambiente e sulla salute e favorisce il reimpegno e/o riciclo dei materiali di cui è composta l'apparecchiatura.

Lo smaltimento abusivo del prodotto da parte dell'utente comporta l'applicazione delle sanzioni amministrative previste dalla normativa vigente.

# 1. INTRODUZIONE



**Grazie per la fiducia accordataci nell'acquistare un prodotto Digicom!**

**Michelangelo Wave 300: la soluzione integrata e compatta per il networking wireless su ADSL2/2+.**
**Avete infatti a disposizione ben 3 dispositivi racchiusi in uno: un Router ADSL2/2+, un Access Point wireless a 300 Mbit/s e uno Switch a 4 porte 10/100.**


## FUNZIONI BASE

Michelangelo Wave 300 vi permette di collegare a Internet una rete (domestica o aziendale) di PC, via cavo o senza fili.

I PC presenti sulla vostra rete locale LAN wireless e cablata avranno la possibilità di accedere a Internet per la navigazione (WWW, HTTP), l'accesso alla posta elettronica (e-mail) o ad altri servizi Internet utilizzando la linea ADSL e 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 Wave 300, senza intervento alcuno da parte degli utilizzatori della rete.

Michelangelo Wave 300 dispone di un'interfaccia Wireless che segue il nuovo standard 802.11n (comunemente chiamato MIMO) che supporta la velocità di collegamento a 300Mbps. Per garantire l'interoperabilità , l'interfaccia Wireless è compatibile con gli standard 802.11b a 11Mbps e 802.11g a 54Mbps.

## FUNZIONI AVANZATE

Il dispositivo è dotato anche di funzionalità avanzate, utili per gestire in modo efficiente l'accesso a Internet dei vostri PC realizzando, se necessario, l'esportazioni di servizi interni.

La sua LAN sarà inoltre protetta dai più comuni attacchi di hacker che potenzialmente possono provenire da Internet (Denial Of Service) grazie al firewall integrato. Michelangelo Wave 300 supporta trasparentemente i protocolli L2TP, PPTP e IPSEC per il VPN Passthrough.

## 1.1. CONTENUTO DELLA CONFEZIONE (CHECK LIST)

Prima di installare il prodotto, assicuratevi che siano presenti i seguenti articoli:

- 1 Michelangelo Wave 300
- 1 Alimentatore 12VDC - 220VAC
- 1 Cavo di linea RJ11 – RJ11
- 1 Cavo di rete RJ45 - RJ45
- 1 CD-ROM contenente il Manuale Operativo
- 1 Guida Rapida

Spuntate man mano le voci della lista (check list) per completare il controllo.

Se qualcosa all'interno della confezione risultasse danneggiato o mancante, vi invitiamo a contattare immediatamente il vostro rivenditore locale. Vi consigliamo anche di conservare la confezione e lo scontrino nel caso in cui doveste rispedire il materiale in futuro.

## 1.2. REQUISITI

- PC con scheda di rete Ethernet o compatibile 802.11b/g/n
- Protocollo TCP/IP installato su ogni PC
- Cavi di rete UTP Cat. 5 con connettore RJ45
- Linea ADSL su linea analogica con connettore RJ11
- Abbonamento ADSL singolo o multi-utente
- Dati dell'abbonamento ADSL
- Browser web (Internet Explorer, Firefox, Mozilla, ecc.)

## 1.3. CARATTERISTICHE E SPECIFICHE TECNICHE

**ADSL**
- Supporto ADSL2+, ADSL2, DELT, READSL2, 24 Mbps download, 1 Mbps upload
- Supporto ADSL 8 Mbps download, 1 Mbps upload, Full-rate ANSI T1.413 Issue 2, G.dmt, G.lite, G.hs
- Supporto protocolli PPPoA, PPPoE, RFC1483 Routed e Bridged, Classical IPoA, AAL5, VC/LLC multiplexing, OAM F4/F5
- Connettore RJ11

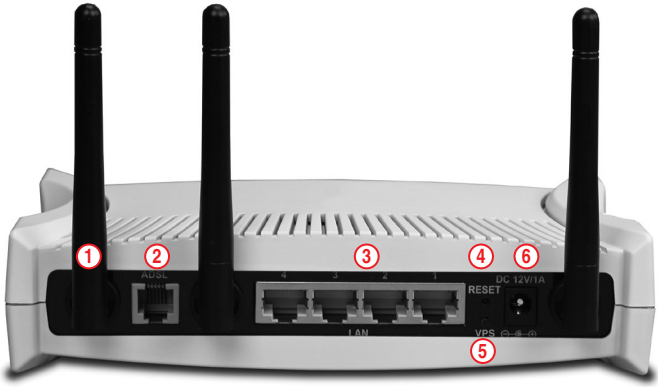
**LAN**
- Switch a 4 porte 10/100 Mbit/s Autosensing
- Riconoscimento automatico cavo di LAN dritto o incrociato (funzione MDI / MDI-X su tutte le porte)

**WIRELESS**
- Tecnologia wireless IEEE802.11n, IEEE 802.11b, IEEE 802.11g 2.4GHz
- 13 canali
- Velocità wireless da 300 fino a 1Mbit/s
- Supporto crittografia dati WEP (64/128 bit), WPA e WPA2
- Interoperabile Wi-Fi

## 1.4. DESCRIZIONE PANNELLO FRONTALE


| | LED | DESCRIZIONE |
|---|---|---|
| 1 | **POWER** | **Acceso**: dispositivo alimentato<br>**Spento**: dispositivo non alimentato |
| 2 | **ETHERNET 1-4** | **Acceso**: quando la corrispondente porta Ethernet è connessa a un dispositivo di rete LAN<br>**Verde**: 100 Mbps, Arancio: 10 Mbps<br>**Lampeggiante**: quando dei dati vengono trasmessi o ricevuti sulla corrispondente porta Ethernet |
| 3 | **WIRELESS** | **Acceso**: Interfaccia Wireless attivata<br>**Lampeggiante**: quando dei dati vengono trasmessi o ricevuti sull'interfaccia Wireless<br>**Spento**: Interfaccia Wireless disabilitata |
| 4 | **WPS** | **Lampeggiante**: procedura WPS in corso<br>**Spento**: WPS non avviato |
| 5 | **DSL** | **Spento**: Linea ADSL non rilevata o collegata<br>**Lampeggiante**: durante la fase di training della linea ADSL<br>**Acceso**: sincronizzazione ADSL avvenuta con successo |
| 6 | **INTERNET** | **Acceso**: Stato della connessione ad Internet<br>**Verde**: Connessione Internet disponibile Rosso: Connessione Internet non attiva |

## 1.5. DESCRIZIONE PANNELLO POSTERIORE




| | | DESCRIZIONE |
|---|---|---|
| 1 | **Antenna** | Antenna della sezione wireless LAN. Posizionate il router possibilmente in una area centrale rispetto alla copertura che volete realizzare |
| 2 | **LINE** | Connettore RJ11 per la linea ADSL |
| 3 | **ETHERNET 1-4** | Porte UTP RJ45 per la connessione di computer o altri dispositivi di rete LAN; sono tutte Autosensing 10/100Mbps e Auto MDI/MDI-X |
| 4 | **RESET** | Pulsante di reset. Una volta acceso il dispositivo, tenerlo premuto:<br>- da 0 a 3 secondi: per effettuare un reset del dispositivo;<br>- più di 6 secondi: per ripristinare le impostazioni di fabbrica del dispositivo (inclusa la password di accesso alla configurazione) |
| 5 | **WPS** | Pulsante WPS |
| 6 | **PWR** | Connettore per l'alimentatore 12VDC |

*** Utilizzare solamente l'alimentatore fornito nella confezione, pena il possibile danneggiamento del dispositivo e conseguente invalidazione delle condizioni di garanzia.**

# 2. INSTALLAZIONE HARDWARE



## 2.1. FILTRI ADSL

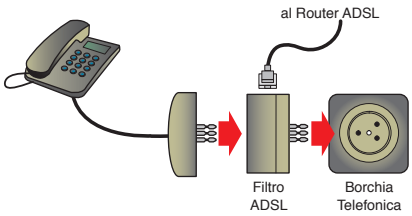
### Linea telefonica tradizionale

L'installazione di un filtro si rende necessaria per isolare il modem ADSL dai disturbi che il canale telefonico potrebbe causare quando l'accesso ADSL utilizza la linea telefonica già esistente.

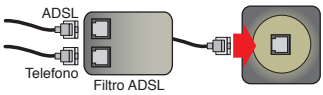
**In questo caso è possibile installare due tipi di filtro:**

- **Filtro distribuito**: se l'impianto telefonico non prevede la presenza di apparecchi diversi dai tradizionali telefoni e fax (centralini, smart box, sistemi di telesoccorso, antifurto, ecc.). Basta collegare il cavo telefonico (RJ11-RJ11) direttamente alla presa telefonica, oppure all'apposita uscita del filtro distribuito indicato dalla scritta ADSL.

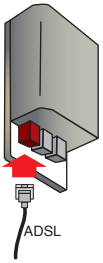
**Filtro distribuito Tripolare**




**Filtro Distribuito RJ11**

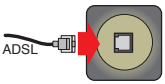



- **Filtro centralizzato**: se l'impianto telefonico prevede invece la presenza di apparecchi diversi dai tradizionali telefoni e fax (centralini, smart box, sistemi di telesoccorso, antifurto, ecc.). Basta collegare il cavo telefonico (RJ11-RJ11) direttamente all'apposita uscita del filtro distribuito indicato dalla scritta ADSL.




### Linea ISDN

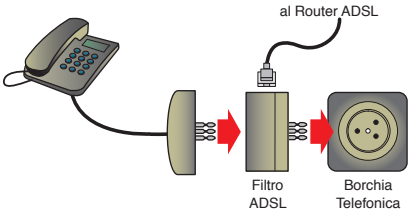
In questo caso esiste una linea totalmente dedicata alla connessione dati ADSL.
Basta collegare il cavo telefonico (RJ11-RJ11) direttamente alla presa RJ di questa linea dedicata.



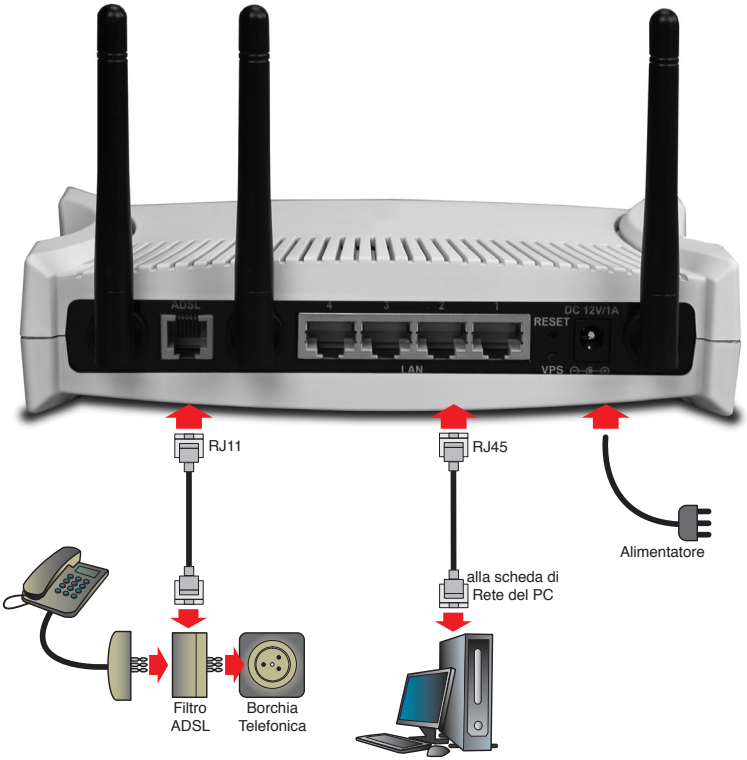
## 2.2. INSTALLAZIONE DI MICHELANGELO WAVE 300

**Seguite questa procedura per installare in modo semplice e rapido il vostro dispositivo.**

1. Collegate un'estremità del cavo di rete RJ45 (incluso nella confezione) a una delle 4 porte LAN (poste sul retro del dispositivo) e l'altra alla scheda di rete del PC.
2. Collegate il dispositivo alla linea ADSL tramite il cavo di linea RJ11 incluso nella confezione. Se sulla stessa linea telefonica sono già presenti apparati analogici come ad esempio normali telefoni, Fax oppure modem analogici, è necessario collegare dei filtri ADSL ad ogni borchia telefonica in cui sono stati collegati questi apparati (vedi paragrafo precedente).




3. Collegate il dispositivo alla rete elettrica tramite l'alimentatore 12VDC incluso nella confezione.
4. **Accendete Michelangelo Wave 300.**



# 3. CONFIGURAZIONE



## 3.1. PREMESSA

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

**Prima di configurare il dispositivo è necessario disporre delle seguenti informazioni:**

- **Dati linea ADSL**
  Dati autenticazione o indirizzi IP
  VPI
  VCI
  Protocollo
- **Dati rete locale**
  Indirizzi IP dei PC già presenti in rete (solo in caso di integrazioni in una rete già esistente)
- **Dati rete wireless**
  Nome rete e crittografia (solo in caso di integrazioni in una rete già esistente)
- **Impostazioni di fabbrica del dispositivo**

| | |
|---|---|
| IP: | 192.168.1.254 |
| SM: | 255.255.255.0 |
| User Name: | admin |
| Password: | admin |

## 3.2. CONFIGURAZIONE BASE

1. Accendete il PC.
2. Configurate la scheda di rete Ethernet o wireless del PC in modo che possa comunicare con il dispositivo. Una soluzione rapida di configurazione è quella automatica (impostazione del PC come DHCP Client)*.

*** Fate riferimento all'APPENDICE A per i sistemi operativi diversi da Windows.**

### Esempio (Microsoft Vista)

- Premete il pulsante sinistro del mouse sull'icona relativa al pulsante **Start**, posizionata in basso a sinistra dello schermo del computer ed in seguito selezionate a voce **Pannello di Controllo**.

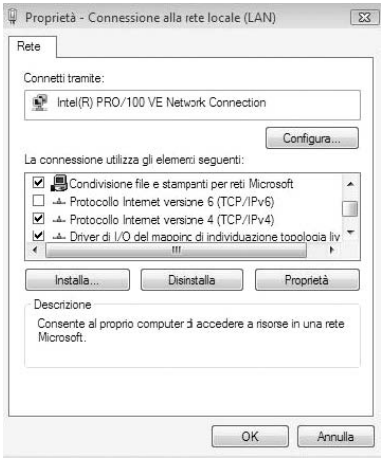

- Comparirà la finestra relativa al **Pannello di Controllo**.


- In modalità di **Visualizzazione Classica**, effettuate un doppio click sull'icona **Centro connessioni di rete e condivisione**.


- Nella finestra **Centro connessioni di rete e condivisione** selezionate **Visualizza stato**.


- Nella finestra **Stato di connessione alla rete locale (LAN)** cliccate sul pulsante **Proprietà**.


- Vi verrà mostrata la configurazione della scheda di rete e dei protocolli.
  Disabilitate il protocollo internet versione 6 (TCP/IPv6) eliminando il flag dalla voce corrispondente.
  Controllate che il protocollo Internet TCP/IP versione 4 (TCP/IPv4) sia abilitato, selezionatelo e cliccate sul tasto **Proprietà**.



- Verificate che le configurazioni siano impostate in modo automatico come mostrato in figura.


## Esempio (Windows XP)

- Selezionate **Start > Pannello di Controllo > Connessioni di rete**.
- Selezionate **Connessione alla Rete Locale (LAN)** e cliccate col destro su **Proprietà**. Selezionate alla scheda "Generale" la voce **Protocollo Internet (TCP/IP)** e premete il pulsante **Proprietà**.
- Selezionate le voci **Ottieni automaticamente un indirizzo IP** e **Ottieni indirizzo server DNS automaticamente**.
- Per rendere attive le nuove impostazioni basta staccare il cavo di rete dalla relativa scheda (per 3/4 secondi) e poi ricollegarlo, oppure riavviare il PC.

3. Aprite il vostro browser web per accedere alla configurazione del router. Digitate **http://192.168.1.254** (l'indirizzo IP di default del router) nella relativa barra e premete **Invio**. Si aprirà una finestra di questo tipo:


- Inserite come nome utente **admin** e come password **admin**(*).
- Selezionate OK per accedere alla configurazione.

*** Fate riferimento al capitolo 4 relativo alle "impostazioni di sicurezza"**

4. Cliccate sul link **Quick Start** per accedere alla procedura di configurazione rapida e seguite questa procedura:


- Cliccate il pulsante **Run Wizard**.
- Nella sezione **Password** modificate la password di default per motivi di sicurezza e cliccate il pulsante **Next**.
- Nella sezione **Time Zone** selezionate il fuso orario per l'Italia (GMT+01:00) e cliccate il pulsante **Next**.
- Nella sezione **ISP Connection Type** dovrete inserire le informazioni principali della linea ADSL forniti dal vostro provider, ossia:
  - Dati autenticazione (Username/Password) o indirizzi IP
  - VPI
  - VCI
  - Protocollo (Connection Type)

**Di seguito forniamo gli esempi relativi a 4 dei principali provider italiani:**

| PROVIDER | Username | Password | VPI | VCI | Connection Type |
|---|---|---|---|---|---|
| ALICE | Fornito dal provider | Fornita dal provider | 8 | 35 | PPPoE LLC |
| LIBERO | Fornito dal provider | Fornita dal provider | 8 | 35 | PPPoA VC-Mux (USB)<br>PPPoE LLC (Ethernet) |
| TELE2 | Fornito dal provider | Fornita dal provider | 8 | 35 | PPPoA VC-Mux |
| TISCALI | Fornito dal provider | Fornita dal provider | 8 | 35 | PPPoA VC-Mux |

- Al termine premete il pulsante **Next**.
- Premete il pulsante **Next** per salvare la configurazione guidata e poi **Close** per chiuderla.

## 3.3. CONFIGURAZIONE COMPLETA

1. Accendete il PC.
2. Configurate la scheda di rete Ethernet o wireless del PC in modo che possa comunicare con il dispositivo. Per fornire al PC degli indirizzi statici compatibili con quelli del dispositivo procedete nel modo seguente*:

*** Fate riferimento all'APPENDICE A per i sistemi operativi diversi da Windows.**

### Esempio (Microsoft Vista)

- Premete il pulsante sinistro del mouse sull'icona relativa al pulsante **Start**, posizionata in basso a sinistra dello schermo del computer ed in seguito selezionate a voce **Pannello di Controllo**.


- Comparirà la finestra relativa al **Pannello di Controllo**.

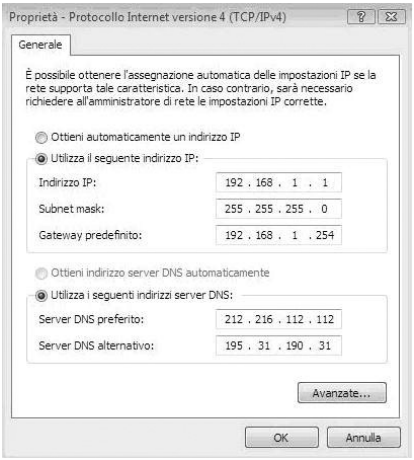

- In modalità di **Visualizzazione Classica**, effettuate un doppio click sull'icona **Centro connessioni di rete e condivisione**.


- Nella finestra **Centro connessioni di rete e condivisione** selezionate **Visualizza stato**.


- Nella finestra **Stato di connessione alla rete locale (LAN)** cliccate sul pulsante **Proprietà**.


- Vi verrà mostrata la configurazione della scheda di rete e dei protocolli.
  Disabilitate il protocollo internet versione 6 (TCP/IPv6) eliminando il flag dalla voce corrispondente.
  Controllate che il protocollo Internet TCP/IP versione 4 (TCP/IPv4) sia abilitato, selezionatelo e cliccate sul tasto **Proprietà**.


- Impostate un indirizzo IP al computer compatibile con l'indirizzo IP assegnato al Michelanhelo Wave 300 come mostrato in figura.




### Esempio (Windows XP)

- Selezionate **Start > Pannello di Controllo > Connessioni di rete.**
- Selezionate **Connessione alla Rete Locale (LAN)** e cliccate col destro su **Proprietà**. Selezionate alla scheda "Generale" la voce **Protocollo Internet (TCP/IP)** e premete il pulsante **Proprietà**.
- Selezionate le voci **Utilizza il seguente indirizzo IP** e **Utilizza i seguenti indirizzi server**, immettendo questi dati:
  **Indirizzo IP:** **192.168.1.1**
  **Subnet Mask:** **255.255.255.0**
  **Gateway predefinito:** **192.168.1.254**
  **Server DNS preferito:** **dato fornito dal vostro provider**

**Di seguito forniamo gli esempi relativi ai DNS di alcuni provider italiani:**

**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 |

**Libero**

| | |
|---|---|
| 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 |

**Tiscali**

| | |
|---|---|
| ns.tiscali.it | 195.130.224.18 |
| sns.tiscali.it | 195.130.225.129 |

**Tele2**

| | |
|---|---|
| | 130.244.127.161 |
| | 130.244.127.169 |

- Confermate le impostazioni col pulsante **OK**.

3. Aprite il vostro browser (ad esempio Internet Explorer). Digitate **http://192.168.1.254** (l'indirizzo IP di default del router) nella relativa barra e premete **Invio**.
   Si aprirà la seguente finestra:


- Inserite come nome utente **admin** e come password **admin**. Cliccate sul tasto **OK** per accedere alla configurazione.

*** Fate riferimento al capitolo 4 relativo alle "impostazioni di sicurezza"**

L'utility web è suddivisa in varie pagine di configurazione, accessibili tramite il menù in alto. Ogni voce del menù permette di accedere a più pagine.

4. Per accedere alla procedura di configurazione rapida (Quick Setup) andate al punto 4 della configurazione base. Se invece desiderate procedere a una configurazione completa del dispositivo andate alla voce di menù **Interface Setup**.

**Qui di seguito viene mostrato l'albero del menù di configurazione con una spiegazione schematica di tutte le voci presenti nel menù e con una legenda relativa ai principali pulsanti di configurazione.**


### Quick Start
- Guida interattiva di configurazione rapida

### Interface Setup
- **Internet**: Configurazione parte ADSL
- **LAN**: Configurazione LAN e DHCP Server
- **Wireless**: Configurazione Access Point integrato

### Advanced Setup
- **Firewall**: Attivazione / disattivazione protezioni standard
- **Routing**: Tabella di routing e impostazioni Route
- **NAT**: Impostazioni avanzate di NAT, Multi-Nat e Virtual Server
- **QoS**: impostazioni avanzate per priorità dei dati trasmessi e ricevuti
- **ADSL**: Impostazioni link fisico ADSL

### Access Management
- **ACL**: Controllo accessi
- **Filter**: Blocco sessioni IP, from-to protocol
- **SNMP**: Impostazioni community SNMP
- **UPnP**: Abilitazione e configurazione Universal Plug'n Play
- **DDNS**: Abilitazione e configurazione Dynamic DNS

### Maintenance
- **Administration**: Impostazione Password di accesso alla configurazione
- **Time Zone**: Impostazione Time Server e fuso orario
- **Firmware**: Aggiornamento del Firmware
- **SysRestart**: Riavvio e Reset dispositivo
- **Diagnostics**: Test automatico di configurazione

### Status
- **Device Info**: Informazioni generali di sistema
- **System Log**: Log di sistema
- **Statistics**: Statistiche invio / ricezione pacchetti sulle interfacce

### Help
- Supporto in linea (inglese)

**LEGENDA**

| | |
|---|---|
| SAVE | pulsante da utilizzare per SALVARE e ATTIVARE LE MODIFICHE apportate in una pagina di configurazione. |
| CANCEL | pulsante da utilizzare per CANCELLARE e ANNULLARE LE MODIFICHE apportate in una pagina di configurazione. |
| DELETE | pulsante da utilizzare per ELIMINARE in modo permanente LE MODIFICHE apportate in una pagina di configurazione. |
| RESTART | pulsante da utilizzare per RIAVVIARE il dispositivo. Per RESETTARLO ripristinando le impostazioni di fabbrica (default) selezionare dal menù la funzione Maintenance > SysRestart > Factory Default Settings, oppure mantenete premuto il pulsante di Reset posto sul retro del router per circa 6 secondi. |
| ⚠ | simbolo usato nel manuale per segnalare all'utente la necessità di prestare la massima ATTENZIONE nello svolgimento o meno di una certa procedura. |

**NOTA: Modificando l'indirizzo IP del dispositivo è necessario modificare anche l'indirizzo IP del PC per poter accedere nuovamente alla configurazione.**

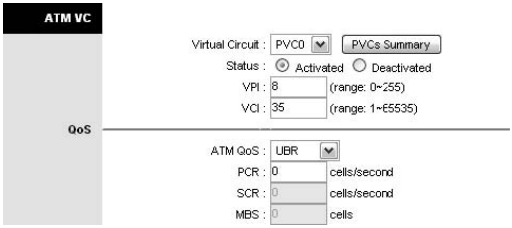
**Al fine di evitare problemi in configurazione della sezione wireless del dispositivo, è consigliabile utilizzare un PC connesso via Ethernet per modificare le impostazione di crittografia. In alternativa disattivate e riattivate la scheda wireless del vostro PC dopo aver effettuato le modifiche in configurazione.**

## 3.3.1. INTERFACE SETUP (CONFIGURAZIONE INTERFACCIA)


### Interface Setup > Internet

In questa pagina di configurazione è possibile impostare l'interfaccia ADSL per l'accesso a Internet.

**ATM VC**

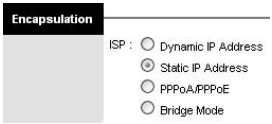



| | |
|---|---|
| **Virtual Circuit:** | lasciate impostato PVC0, questo parametro è da utilizzare solo in caso di abbonamenti multipli (più abbonamenti sulla stessa linea ADSL oppure canali dati separati). |
| **Status:** | Activated attiva il PVC selezionato. |
| **VPI, VCI:** | inserite i valori specificati sul vostro contratto ADSL, solitamente sono 8 e 35. |
| **ATM QoS:** | impostate i parametri specificati sul vostro contratto, se non indicati lasciate impostato UBR. |

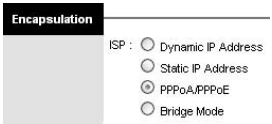
**ENCAPSULATION**

Le opzioni relative a questo parametro di configurazione, fornitovi dal provider (ISP), dipendono dal tipo di abbonamento ADSL di cui disponete:

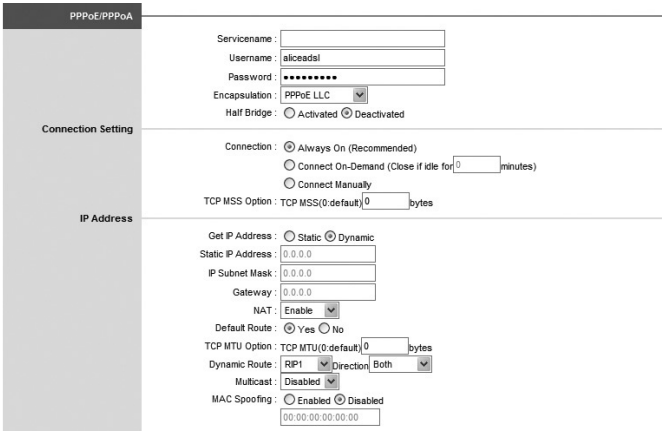
**A.** se il provider vi ha fornito uno **Username** e una **Password** (Abbonamento ADSL singolo utente), ossia un abbonamento tramite autenticazione e con indirizzo IP dinamico, allora dovrete selezionare l'opzione **PPPoA/PPPoE**;




**B.** se invece il provider NON vi ha fornito uno **Username** e una **Password** (Abbonamento ADSL Professionale), ossia disponete di un abbonamento senza autenticazione e con uno o più indirizzi IP globali statici, allora dovrete selezionare l'opzione **Static IP Address**.



**Opzione A: PPPoE/PPPoA**




**Servicename:** inserite un nome (non obbligatorio) da associare alla connessione.

**Username:** inserite il vostro nome utente per la connessione alla linea ADSL.

**Password:** inserite la vostra password per la connessione alla linea ADSL.

**Encapsulation:** selezionate PPPoA VC-Mux oppure PPPoE LLC in accordo con le specifiche del vostro contratto. Per le linee ADSL attualmente disponibili in Italia sono solo queste due le configurazioni utilizzate.

**Connection:** Always On = la connessione è sempre attiva.
**Connect On-Demand** = la connessione viene disattivata dopo x minuti di inattività, questa impostazione viene utilizzata per abbonamenti con tariffa a tempo. In caso di prolungata inattività è sempre consigliata la disconnessione della linea ADSL dal router (cavo linea RJ11).
**Connect Manually** = la connessione viene gestita in modo manuale dall'utente. Per attivare o disattivare la connessione è necessario accedere al menù Status. In questo menù sarà disponibile il pulsante Connect/Disconnect per gestire la connessione PPP.

**TCP MSS Option:** Inserite il valore massimo di byte di dati che saranno inviati in un singolo pacchetto. Per una configurazione corretta e performante, questo campo deve essere settato in modo da evitare la deframmentazione del pacchetto da parte del router. Il valore 0 indica che verrà utilizzata la configurazione di default (consigliata).

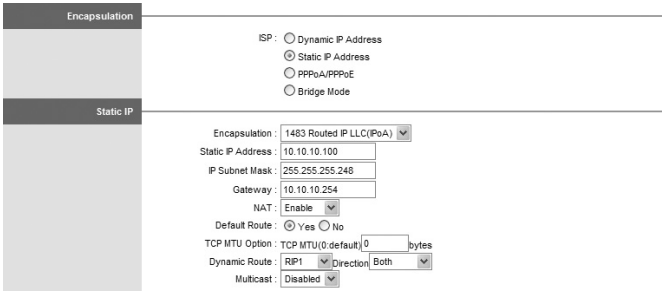
**Get IP Address:** gli abbonamenti di questo tipo utilizzano solitamente un indirizzo IP dinamico, pertanto selezionate Dynamic.

**NAT:** impostate Enable.

**Default Route:** selezionate Yes.

**TCP MTU Option:** inserite il valore relativo al parametro MTU (Maximum Transmission Unit). Questo corrisponde alla dimensione massima di pacchetto che il router può inviare. I valori consentiti vanno da un minimo di 128 a un massimo di 1500 byte. Il valore 0 indica che verrà utilizzata la configurazione di default (ossia il valore massimo di MTU, pari a 1500 byte).

**Opzione B: Static IP Address**




**Encapsulation:** selezionate 1483 Routed IP LLC.
**Static IP Address:** inserite l'indirizzo IP che vi è stato assegnato dal provider.
**IP Subnet Mask:** inserite la Subnet Mask che vi è stata assegnata dal provider.
**Gateway:** inserite il gateway predefinito (Default Gateway) che vi è stato assegnato dal provider.
**NAT:** impostate Enable.
**Default Route:** selezionate Yes.
**TCP MTU Option:** inserite il valore relativo al parametro MTU (Maximum Transmission Unit). Questo corrisponde alla dimensione massima di pacchetto che il router può inviare. I valori consentiti vanno da un minimo di 128 a un massimo di 1500 byte. Il valore 0 indica che verrà utilizzata la configurazione di default (ossia il valore massimo di MTU, pari a 1500 byte).

## Interface Setup > LAN

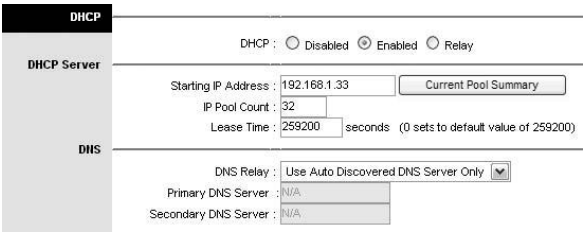
In questa sezione è possibile configurare i parametri relativi alla rete locale LAN e al server DHCP.

**ROUTER LOCAL IP**


**IP Address:** indirizzo IP del router.
**IP Subnet Mask:** Subnet Mask del router.
**Dynamic Route:** gestione del protocollo di RIP.
**Multicast:** selezionate IGMP v1 o v2 per abilitare la gestione dei pacchetti di Multicast sulla rete LAN.
**IGMP Snooping:** tecnica che permette di ottimizzare i flussi di Multicast all'interno della LAN, inoltrando il traffico Multicast solo sulle porte LAN che effettivamente ne fanno uso. Selezionate Enabled per abilitare questa tecnica.

**DHCP (*)**

*** Fate riferimento al capitolo 4 relativo alle "Impostazioni di sicurezza"**




**DHCP:** Disabled disattiva il Server DHCP.
Enabled abilita il Server DHCP.
Relay abilita il server DHCP in modalità Relay.

**Quando il DHCP Server è abilitato è possibile impostare i seguenti parametri:**

**Starting IP Address:** inserite l'indirizzo IP di partenza del pool di indirizzi assegnabili tramite DHCP.

**IP Pool Count:** inserite il numero di indirizzi IP assegnabili.

**Lease Time:** inserite il tempo di validità, in secondi, degli indirizzi assegnati.

**DNS Relay:** Use Auto Discovered DNS Server Only assegna ai client DHCP gli indirizzi DNS ricevuti dal provider ADSL; questa funzione può essere utilizzata solo in caso di assegnazione dinamica degli indirizzi. Se la linea ADSL utilizza indirizzi IP statici è necessario selezionare l'opzione Use User Discovered DNS Server Only e specificare nei campi Primary/Secondary DNS Server gli indirizzi IP dei server DNS che volete utilizzare.

Tramite il pulsante **Currente Pool Summary** è possibile visualizzare un elenco aggiornato dei Client DHCP connessi al router.

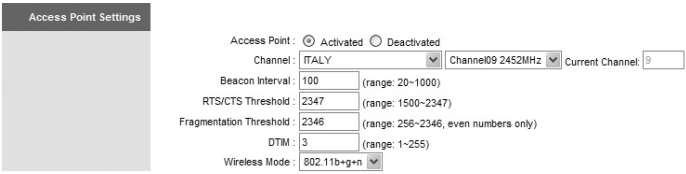
**Quando il DHCP Server è abilitato in modalità Relay è possibile impostare:**

**DHCP Server IP for Relay Agent:** inserite l'indirizzo IP del server DHCP già presente in rete.

## Interface Setup > Wireless

In questa sezione è possibile impostare i parametri relativi alla rete wireless IEEE802.11b&g&n generata dall'Access Point integrato.

**ACCESS POINT SETTINGS**




**Access Point:** Activated attiva la rete wireless.

**Channel:** sezione in cui impostare il canale wireless da utilizzare (cercate di mantenere almeno 5 canali di differenza tra altri Access Point nella zona). Nel primo menù a tendina scegliete la vostra nazione, nel secondo il canale prescelto. Se desiderate che sia il dispositivo a fare una ricerca automatica del canale migliore, selezionate in questo menù a tendina la funzione Auto. L'impostazione attualmente attiva relativa al numero di canale utilizzato viene indicata nel campo Current Channel

**Beacon Interval:** definisce il tempo di invio dei pacchetti di Beacon (ms). Si consiglia vivamente di lasciare il valore di default.

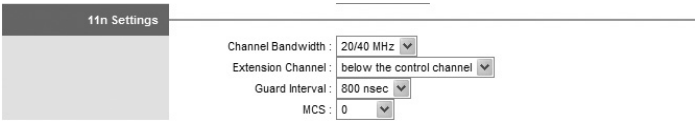
**RTS/CTS Threshold:** definisce la soglia per la gestione del controllo di flusso in trasmissione. Si consiglia vivamente di lasciare il valore di default.

**Fragmentation Threshold:** definisce la dimensione massima dei pacchetti. Si consiglia vivamente di lasciare il valore di default.

**DTIM:** definisce ogni quanti pacchetti di Beacon l'Access Point può inoltrare sulla rete wireless pacchetti Multicast e Broadcast. Si consiglia vivamente di lasciare il valore di default.

**Wireless Mode:** impostate il tipo di rete wireless che volete utilizzare.
802.11b: rete wireless 11 Mbit/s.
802.11g: rete wireless 54 Mbit/s.
802.11b+g: rete wireless 11 e 54 Mbit/s.
802.11n: rete wireless 300 Mbit/s
802.11g+n: rete wireless 54 e 300 Mbit/s
802.11b+g+n: rete wireless 11, 54 e 300 Mbit/s

**11N SETTINGS**



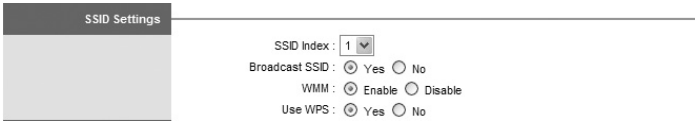

**Channel Bandwidth:** Questa impostazione influisce su come il dispositivo utilizzerà la banda di frequenza ed i canali Wireless. Selezionate:
**20MHz** se la vostra rete non utilizza Client 802.11n
**20/40MHz** se la vostra rete utilizza sia Client 802.11n che 802.11g o b

**Extension Channel:** Lo standard 802.11n utilizza una banda maggiore rispetto ai precedenti 802.11b/g e pertanto va a coprire un numero maggiore di canali per l'instaurazione e il mantenimento della connessione Wireless a 300Mbps. Se nella zona in cui state posizionando il Michelangelo Wave 300 sono già presenti delle reti Wireless su canali fissi, al fine di evitare la sovrapposizione con altri canali è possibile definire se utilizzare i 4 canali che precedono **(below the control channel)** il canale impostato in **Channel** oppure utilizzare i 4 canali successivi **(above the control channel)** al canale impostato in **Channel**.
Allo stesso modo, se fosse già presente un Access Point 802.11n è consigliato configurare il canale 'centrale' e l'extension channel in modo tale che nessuno di questi canali venga utilizzato da entrambi gli Access Point.

**Guard Interval:** selezionate il tempo di guardia utilizzato dal Michelangelo Wave 300. Il tempo di guardia è stato introdotto per evitare che la trasmissione dei dati tramite l'interfaccia Wireless interferisca con altre applicazione Wireless attive.

**MCS:** Modulation and Coding Scheme. Raccomandiamo di mantenere il valore Auto.

**SSID SETTINGS**



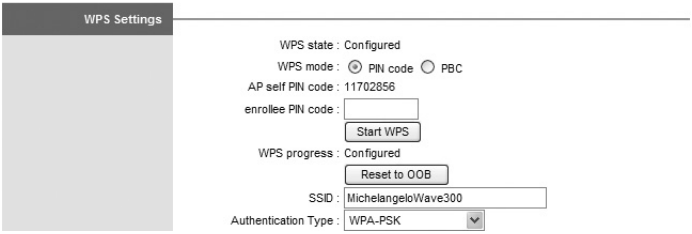

**SSID Index:** selezionate l'indice della rete wireless che intendete configurare.

**Broadcast SSID:** impostando Yes il nome della rete wireless sarà visibile a tutti i client tramite la funzione di ricerca rete (Site Survey, Reti Wireless Disponibili). Selezionando No solo i client che conoscono a priori il nome della rete wireless potranno collegarsi.

**WMM:** Wireless MultiMedia support fornisce funzioni QoS di base per assegnare maggiore priorità ai pacchetti di applicazioni wireless multimediali come Voce e Video.

**Use WPS:** La funzionalità WPS permette la configurazione automatica della crittografia su ogni Client Wireless che supporta questa modalità. È possibile utilizzare la funzionalità WPS in tre modalità: tramite la pressione del tasto WPS presente sul Michelangelo Wave 300, tramite uno scambio PIN inizializzato dal Michelangelo Wave 300 e tramite uno scambio PIN inizializzato dal Client Wireless. In tutti e tre i casi, per poter utilizzare la funzionalità WPS è necessario che una chiave di crittografia sia già stata configurata con protocollo WPA (oppure WEP). Se selezionato, abilitata la possibilità di utilizzare il WPS per la configurazione della crittografia nelle stazioni di rete Wireless.

**WPS SETTINGS**




La funzionalità WPS permette la configurazione automatica della crittografia su ogni Client Wireless che supporta questa modalità. È possibile utilizzare la funzionalità WPS in tre modalità: tramite la pressione del tasto **WPS** presente sul Michelangelo Wave 300, tramite uno scambio **PIN** inizializzato dal Michelangelo Wave 300 e tramite uno scambio PIN inizializzato dal Client Wireless. In tutti e tre i casi, per poter utilizzare la funzionalità WPS è necessario che una chiave di crittografia sia già stata configurata con protocollo WPA (oppure WEP).

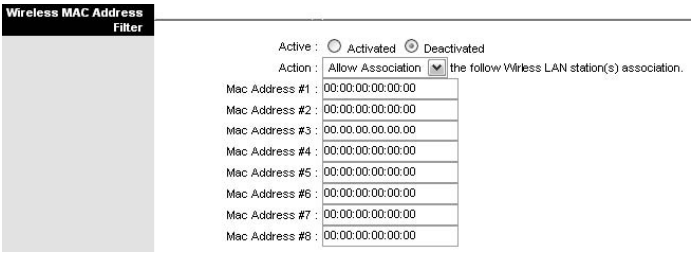
**WPS State:** indica se la funzionalità WPS è abilitata
**WPS Mode:** Selezionate la voce PIN Code se volete configurare il WPS tramite lo scambio di un PIN numerica, altrimenti selezionate PBC se volete configurare i client Wireless tramite la pressione del pulsante.
**AP Self PIN code:** in questo campo, visibile solo con WPS Mode impostato su PIN Code, viene visualizzato il codice PIN che verrà generato dal Michelangelo Wave 300 per sincronizzare e quindi configurare le stazioni Wireless.
**Enrollee PIN code:** inserite il PIN che viene generato dalle stazioni Wireless durante una procedura WPS generata da queste stazioni.

Tramite il pulsante **Start WPS** è possibile attivare una delle due possibili procedure WPS basate su scambio PIN (ricordiamo che la terza possibilità viene avviata direttamente tramite il pulsante presente sul dispositivo stesso).
**WPS Progress:** Visualizza lo stato della procedura WPS

Tramite il pulsante **Reset to OOB** è possibile resettare alle impostazioni di fabbrica, tutti i parametri della sezione Wireless.
**SSID:** Inserite il nome che volete assegnare alla rete Wireless. Le stazioni di rete con supporto Wireless, rileveranno la vostra rete con il nome che avrete inserito.
**Authentication Type:** sezione in cui è possibile impostare la crittografia* per la protezione dei dati sulla rete wireless, a scelta tra Disabled (disattivato), WEP-64bit, WEP-128bit, WPA-PSK, WPA2-PSK oppure WPA-PSK/WPA2-PSK. **Per ulteriori dettagli sulla critografia si rimanda al capitolo 5 "FAQ".**

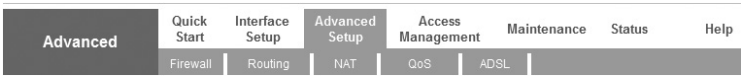
*** fate riferimento al capitolo 4 relativo alle "Impostazioni di sicurezza"**

**WIRELESS MAC ADDRESS FILTER**



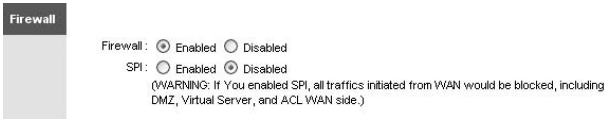

**Active:** Activated abilita la funzione di Mac Filter.
**Action:** selezionando la voce Allow Association solo i client con Mac Address inserito nella lista seguente (Mac Address #1-8) potranno collegarsi all'Access Point. Selezionando la voce Deny Association tutti i client potranno collegarsi, ad esclusione di quelli inseriti in lista.

## 3.3.2. ADVANCED SETUP (CONFIGURAZIONE AVANZATA)




### Advanced Setup > Firewall

In questa finestra è possibile abilitare o disabilitare il firewall, ossia la protezione di default da attacchi DOS e hacker dall'esterno e dall'interno.




**Firewall:** Enabled per abilitare il firewall oppure Disabled per disabilitarlo (sconsigliato).
**SPI:** la funzione Stateful Packet Inspection analizza i pacchetti in transito (da/verso Internet) nel dettaglio, entrando nel merito delle sessioni. Se lo stato delle sessioni non è valido, il pacchetto viene scartato. L'opzione Enabled abilita tale funzione, mentre l'opzione di default Disabled la disattiva.

**ATTENZIONE! Abilitando l'SPI tutto il traffico proveniente dalla linea ADSL verrà bloccato, inclusi DMZ, Virtual Server e accesso da remoto alla configurazione. Per i pacchetti in uscita (dalla LAN verso Internet) è possibile creare delle REGOLE DI FILTRO.**

### Advanced Setup > Routing

In questa finestra viene mostrata la tabella di routing ed è possibile aggiungere nuove route statiche. Funzione utile solo in presenza di più router (nel caso di 1 solo router non è necessario agire su questa configurazione).

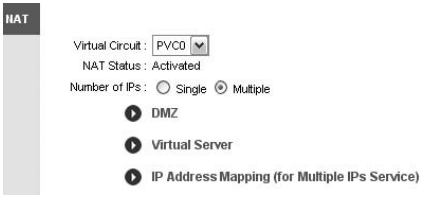
Routing Table List

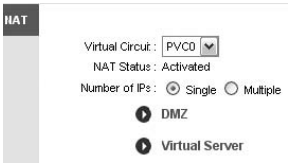
| # | Dest IP | Mask | Gateway IP | Metric | Device | Use | Edit | Drop |
|---|---|---|---|---|---|---|---|---|
| 1 | 192.168.1.0 | 24 | 192.168.1.1 | 1 | enet0 | 678 | | |
| 2 | 80.105.107.0 | 24 | 80.105.107.12 | 2 | Idle | 0 | | |
| 3 | default | 0 | 80.105.107.12 | 2 | Idle | 0 | | |

Per aggiungere nuove route statiche cliccate il pulsante "**Add Route**" e inserite nella finestra successiva i parametri della route che volete creare.

### Advanced Setup > NAT

In questa finestra è possibile configurare le opzioni del NAT, per esportare servizi o per creare associazioni con un pool aggiuntivo di indirizzi IP.

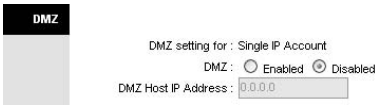



**Number of IPs:** selezionate Single per abbonamenti con un singolo indirizzo IP, oppure Multiple per abbonamenti con un pool di indirizzi IP aggiuntivi. Scegliendo l'opzione Multiple, oltre a i pulsanti DMZ e Virtual Server si attiverà anche il pulsante IP Address Mapping (for Multiple IPs Service).

**DMZ**

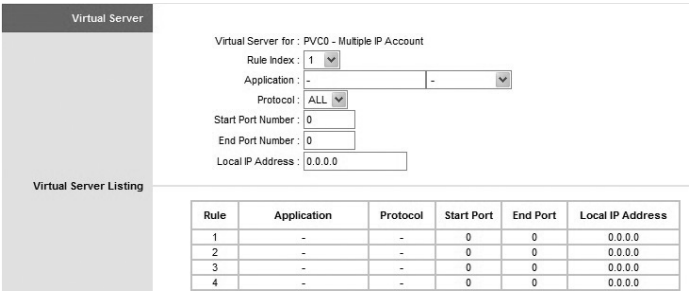
**De-Militarized Zone**, area neutra a cui tutte le richieste destinate all'indirizzo IP pubblico del router vengono ruotate automaticamente (tramite indirizzo IP di DMZ), ad esclusione delle porte specificate nella sezione Virtual Server.




**DMZ:** Enabled abilita la funzione DMZ.
**DMZ Host IP Address:** inserite l'indirizzo IP della macchina da posizionare in DMZ.

**VIRTUAL SERVER**

Letteralmente significa "Server virtuale". Funzione indispensabile per la pubblicazione di alcuni servizi (http, ftp, servizi P2P quali – ad esempio - emule, ecc.).




**Rule Index:** inserite l'indice della regola che state creando, da 1 a 16.
**Application:** dal menù a tendina selezionate, ove presente, il servizio che si desidera reindirizzare verso un PC in LAN (e il dispositivo imposterà automaticamente le relative porte). Se il servizio non è presente, inserite nel campo Application un nome a scelta e utilizzate il campo seguente per indicare il relativo range di porte.
**Protocol:** Selezionate il protocollo TCP, UDP o ALL (entrambi) usato dall'applicazione
**Start / End Port Number:** range di porte da reindirizzare. Campo da utilizzare solo nel caso di servizi non presenti nell'elenco del campo precedente.
**Local IP Address:** inserite l'indirizzo IP della macchina che ospita il servizio.

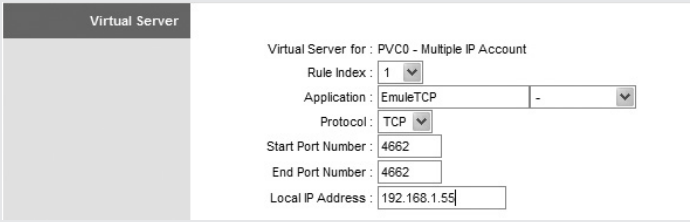
**Di seguito forniamo alcuni esempi di configurazione di tali servizi.**

Alcuni servizi, per essere completamente funzionali, richiedono l'apertura di alcune porte sull'indirizzo IP privato assegnato al PC che deve effettuare queste servizio.
Ad esempio, se è necessario pubblicare un server web presente su un PC collegato in LAN a Michelangelo Wave 300, è necessario mappare la porta 80 con il protocollo TCP verso l'indirizzo IP privato del PC che ospita il server web.
Per effettuare questa procedura è quindi necessario che tutti i PC in rete (o almeno i PC che devono effettuare questi particolari servizi) siano stati configurati con un indirizzo IP privato statico e non in DHCP Client (nei sistemi operativi Windows la funzione DHCP Client viene indicata come "Ottieni automaticamente un indirizzo IP").

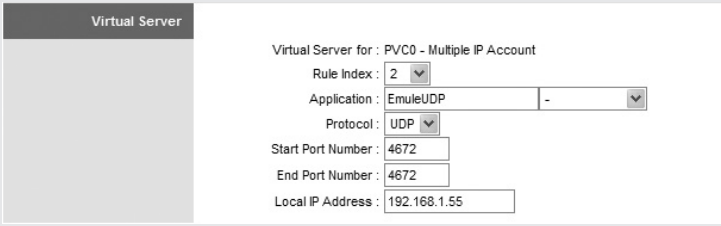
- **Emule**

Per configurare in moto ottimale un PC collegato al Michelangelo Wave 300 per ottenere un ID alto su Emule è necessario aprire le porte che di default vengono utilizzate dal programma. Per modificare o visualizzare queste porte dovete accedere alle opzioni di connessione del software Emule.
**Generalmente le porte reimpostate sono:**
4662 in TCP
4672 in UDP

In questo esempio mostreremo la configurazione del menù Virtual Server per un PC collegato in LAN con indirizzo IP 192.168.1.55
Dato che il software utilizza due porte diverse, è necessario creare due regole separate. Configurate quindi la sezione Virtual Server come mostrato nell'immagine e premete il pulsante "**SAVE**".




Una volta salvata, la prima regola create una seconda come mostrato in figura:




Se la configurazione è stata eseguita in modo corretto, vi verrà mostrata la seguente tabella riassuntiva:

Virtual Server Listing

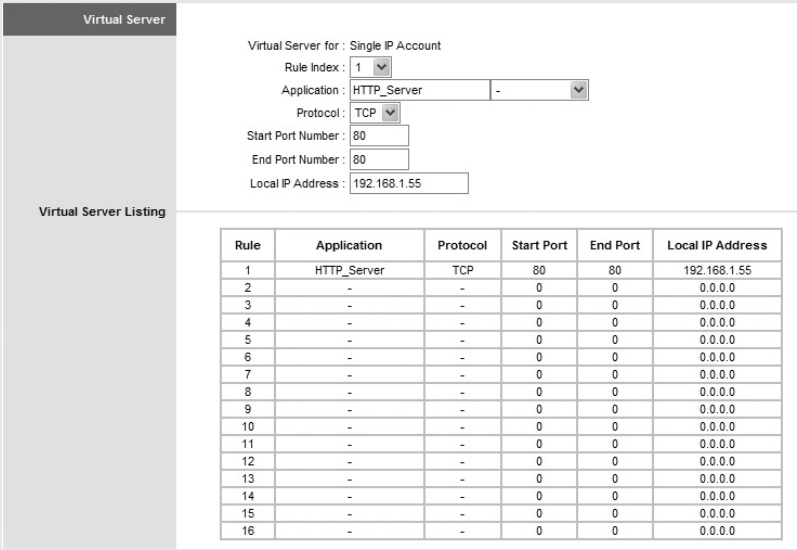
| Rule | Application | Protocol | Start Port | End Port | Local IP Address |
|---|---|---|---|---|---|
| 1 | EmuleTCP | TCP | 4662 | 4662 | 192.168.1.55 |
| 2 | EmuleUDP | UDP | 4672 | 4672 | 192.168.1.55 |
| 3 | - | - | 0 | 0 | 0.0.0.0 |
| 4 | - | - | 0 | 0 | 0.0.0.0 |
| 5 | - | - | 0 | 0 | 0.0.0.0 |
| 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 |
| 13 | - | - | 0 | 0 | 0.0.0.0 |
| 14 | - | - | 0 | 0 | 0.0.0.0 |
| 15 | - | - | 0 | 0 | 0.0.0.0 |
| 16 | - | - | 0 | 0 | 0.0.0.0 |

Avviate Emule e verificate la corretta e completa funzionalità.

- **Server web (http)**

In questo secondo esempio faremo riferimento alla configurazione del Virtual Server per permettere la visualizzazione dall'esterno di un server web residente su un PC collegato al Michelangelo Wave 300. Il Server web si appoggia sulla porta 80 in TCP ed è residente su un PC configurato con l'indirizzo IP 192.168.1.55

In base a queste indicazioni, la regola da configurare è quella riportata in figura:




| Rule | Application | Protocol | Start Port | End Port | Local IP Address |
|---|---|---|---|---|---|
| 1 | HTTP_Server | TCP | 80 | 80 | 192.168.1.55 |
| 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 |
| 13 | - | - | 0 | 0 | 0.0.0.0 |
| 14 | - | - | 0 | 0 | 0.0.0.0 |
| 15 | - | - | 0 | 0 | 0.0.0.0 |
| 16 | - | - | 0 | 0 | 0.0.0.0 |

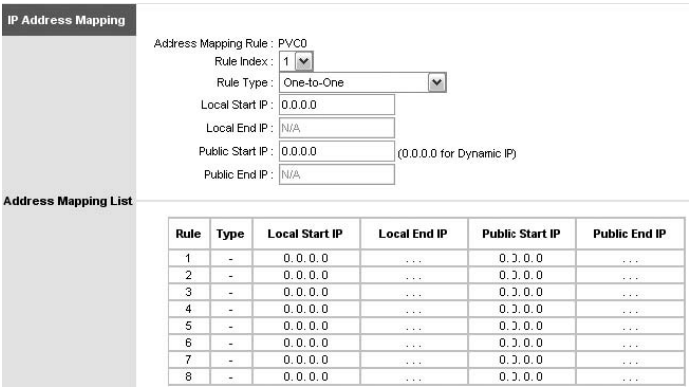
Come indicato, inserite nel campo **Rule Index** il numero progressivo della regola di Virtual Server in esecuzione. In questo caso, essendo la prima regola, è stato impostato l'Index 1.
In **Start Port Number** e in **End Port Number** è necessario inserire il range di porte che devono essere aperte. Se, come nel nostro esempio, si deve aprire una singola porta, in entrambi i campi occorre inserire la porta in questione.
In **Local IP Address** è necessario inserire l'indirizzo IP privato del PC su cui bisogna mappare la porta. Facendo riferimento al nostro esempio è stato inserito l'indirizzo IP 192.168.1.55.

Per rendere effettive le impostazioni premete il pulsante "**Save**".

In seguito a questa configurazione, se un PC presente in Internet effettua una richiesta con un browser Internet verso l'indirizzo IP pubblico fornito dal provider, il router, riconoscendo una richiesta sull'interfaccia WAN sulla porta 80 e verificando che in queste situazione non deve bloccare la richiesta di connessioni dati, provvederà a inoltrarla verso l'indirizzo 192.168.1.55, permettendo così al PC sorgente di visualizzare il server web caricato sul PC locale collegato a Michelangelo Wave 300.
Ricordiamo che per verificare la corretta funzionalità della procedura non è possibile effettuare una richiesta da un altro PC collegato a Michelangelo Wave 300 sull'indirizzo IP pubblico assegnato dal provider al router ADSL, in quanto il router ADSL non sarebbe in grado di effettuare in modo corretto il routing dei pacchetti.

Per questo motivo, per verificare la funzionalità dell'applicazione **consigliamo di utilizzare un PC momentaneamente collegato a Internet tramite un diverso tipo di connessione**, come ad esempio una tradizionale connessione remota con modem analogico/ISDN.

**IP ADDRESS MAPPING (for multiple IPs service)**
In questa sezione è possibile gestire l'abbinamento tra un pool di indirizzi IP pubblici e degli indirizzi privati in LAN.




| Rule | Type | Local Start IP | Local End IP | Public Start IP | Public End IP |
|---|---|---|---|---|---|
| 1 | - | 0.0.0.0 | ... | 0.0.0.0 | ... |
| 2 | - | 0.0.0.0 | ... | 0.0.0.0 | ... |
| 3 | - | 0.0.0.0 | ... | 0.0.0.0 | ... |
| 4 | - | 0.0.0.0 | ... | 0.0.0.0 | ... |
| 5 | - | 0.0.0.0 | ... | 0.0.0.0 | ... |
| 6 | - | 0.0.0.0 | ... | 0.0.0.0 | ... |
| 7 | - | 0.0.0.0 | ... | 0.0.0.0 | ... |
| 8 | - | 0.0.0.0 | ... | 0.0.0.0 | ... |

È possibile definire fino a 8 differenti regole di abbinamento in 4 modalità operative differenti.
**Rule Index:** selezionate il numero della regola che volete creare o modificare.

**Rule Type:**
- **One-to-One**
  Abbinamento "uno a uno", a un indirizzo IP pubblico viene associato un indirizzo IP privato. Inserite l'indirizzo IP privato in Local Start IP e quello pubblico in Public Start IP.
- **Many-to-One**
  Abbinamento "molti a uno", il comportamento è uguale a quello del classico NAPT (Network Address and Port Translation) o SUA (Single User Account), offre però il vantaggio di associare diversi gruppi di indirizzi IP privati con differenti IP pubblici, per integrare ad esempio una migliore gestione del traffico di diverse sezioni dell'azienda. Inserite in Local Start IP e Local End IP il range di indirizzi IP privati ed in Public Start IP l'indirizzo IP pubblico a loro associato.
- **Many-to-Many Overload**
  Abbinamento "molti a molti con opzione overload", indica che gli indirizzi pubblici verranno utilizzati anche da più indirizzi IP privati contemporaneamente. Inserite in Local Start IP e Local End IP il range di indirizzi IP privati ed in Public Start IP e Public End IP il range di indirizzi IP pubblici a loro associati.

**Esempio di 8 indirizzi IP locali su 2 IP pubblici**
IP_locale1 -> IP_Pubblico1
IP_locale2 -> IP_Pubblico2
IP_locale3 -> IP_Pubblico1
IP_locale4 -> IP_Pubblico2
IP_locale5 -> IP_Pubblico1
IP_locale6 -> IP_Pubblico2
IP_locale7 -> IP_Pubblico1
IP_locale8 -> IP_Pubblico2

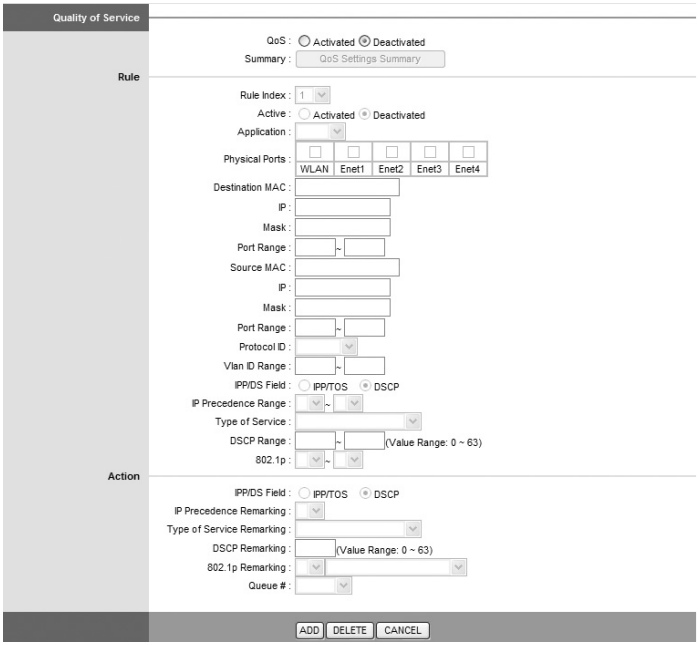
- **Many-to-Many No Overload**
  Abbinamento “molti a molti con opzione no overload”, indica che gli indirizzi pubblici verranno assegnati solo ad un indirizzo IP privato alla volta. Inserite in Local Start IP e Local End IP il range di indirizzi IP privati ed in Public Start IP e Public End IP il range di indirizzi IP pubblici a loro associati.

**Esempio di 8 Indirizzi IP locali su 6 IP pubblici**

| | |
|---|---|
| IP_locale1 -> IP_Pubblico1 | |
| IP_locale2 -> IP_Pubblico2 | |
| IP_locale3 -> IP_Pubblico3 | |
| IP_locale4 -> IP_Pubblico4 | |
| IP_locale5 -> IP_Pubblico5 | |
| IP_locale6 -> IP_Pubblico6 | |
| IP_locale7 -> nn | |
| IP_locale8 -> nn | |
| … | È terminata la disponibilità di IP pubblici, pertanto la richiesta di accesso Internet della |
| …. | macchina con IP_locale7 non può essere accettata. |
| IP_locale1 -X> IP_Pubblico1 | |
| IP_locale7 -> IP_Pubblico1 | Quando IP_Locale1 rilascia l’indirizzo, IP_Locale7 può accedere a Internet. |

## Advanced Setup > QoS

Tramite il menù QoS è possibile impostare la priorità dei pacchetti per privilegiare un flusso dati rispetto ad un altro. Alcune applicazioni basate su una connessione ad Internet richiedono, per un servizio migliore, un limite di banda. In situazioni di particolare traffico dati da o verso Internet, questa banda potrebbe non essere disponibile e il servizio potrebbe peggiorare o addirittura interrompersi. Se configurato opportunamente, il QoS consente di mantenere il servizio correttamente attivo e completamente funzionale.




**QoS:** Attiva o disattiva la funzionalità QoS

**Summary:** Cliccando sul pulsante QoS Settings Summary vengono visualizzate le regole di QoS precedentemente create.

Il menù del QoS si divide in due parti. La sezione Rule serve per "istruire" il Michelangelo Wave 300 a riconoscere, all'interno di tutto il traffico dati che gestisce, il servizio su cui deve assegnare maggiore o minore priorità. Per questo motivo, non tutti i campi presenti sono obbligatori. é comunque importante compilare i campi minimi e necessari per il corretto riconoscimento del servizio. La sezione Action identifica le azioni (livello di priorità) che il Michelangelo Wave 300 deve utilizzare una volta riconosciuta il servizio definito nella sezione precedente.

**RULE**

| | |
|---|---|
| **Rule Index:** | Selezionate il numero di regola che intendete creare o modificare |
| **Active:** | Permette di attivare o disattivare una regola di QoS |
| **Application:** | Permette di selezionare dei servizi preconfigurati. Selezionando una di queste applicazioni, verranno Configurati automaticamente alcuni campi sottostanti. |
| **Physical Ports:** | Permette di selezionare la porta fisica del Michelangelo Wave 300 su cui verrà applicata la regola che state creando. È possibile selezionare l'interfaccia Wireless (WLAN) e le quattro porta LAN (Enet1-4) |
| **Destination MAC:** | Permette di definire l'indirizzo MAC del dispositivo di destinazione |
| **IP:** | Permette di inserire l'indirizzo IP del dispositivo di destinazione |
| **Mask:** | Permette di inserite la maschera di rete del dispositivo di destinazione |
| **Port Range:** | Permette di inserire il range delle porte utilizzate dal dispositivo di destinazione per effettuare il servizio |
| **Sourse MAC:** | Permette di definire l'indirizzo MAC del dispositivo sorgente del servizio |
| **IP:** | Permette di inserire l'indirizzo IP del dispositivo sorgente del servizio |
| **Mask:** | Permette di inserite la maschera di rete del dispositivo sorgente del servizio |
| **Port Range:** | Permette di inserire il range delle porte utilizzate dal dispositivo sorgente del servizio |
| **Protocol ID:** | Permette di definire il protocollo utilizzato dall'applicazione |

I campi appena descritti vengono utilizzati per riconoscere l'applicazione da priorizzare. È possibile, che il dispositivo stesso che genera l'applicazione (un PC, una borchia VoIP, ect) generi dei pacchetti dati con QoS/ToS configurato. In questo caso è possibile configurare il Michelangelo Wave 300 per riconoscere l'applicazione in base alle informazioni già contenute nel pacchetto generato dal dispositivo. I campi possibili sono **Vlan ID range, IPP/DS Field, IP precedense Range, Type of Service, DSCP Range e 802.1p**. Fate riferimento alla documentazione tecnica del dispositivo o dell'applicazione per la configurazione di questi campi.

**ACTION**

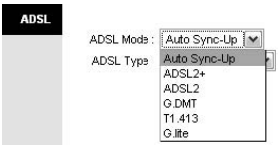
Nel caso appena descritto, dove cioè i pacchetti dati generati dal dispositivo sorgente dispongono già dei dati per la priorità dei pacchetti, è possibile modificare i parametri di QoS. I campi **IPP/DS Field, IP precedense Remarking, Type of Service Remarking, DSCPRemarking e 802.1p** remarking devono essere configurati nel caso in cui siano stati precedentemente definiti nella sezione Rule.

**Queue #:** Definisce il livello di priorità da assegnare ad un flusso dati che rispecchia i parametri di riconoscimento definiti nella sezione Rule. È possibile definire i seguenti livelli di priorità:
- Low
- Medium
- High
- Highest

- Cliccate sul pulsante **ADD** per aggiungere una regola oppure il pulsante **Delete** per eliminare una regola precedentemente creata.

### Advanced Setup > ADSL

In questa sezione è possibile configurare le impostazioni della linea ADSL.



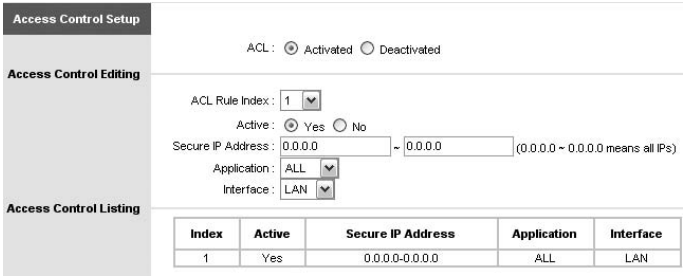

**ADSL Mode:** modalità ADSL.

**Lasciate impostato Auto Sync-Up per selezionare automaticamente il tipo di linea ADSL. In caso di problemi di connessione alla linea (mancata connessione, lunghi tempi di sincronizzazione) provate a selezionare la modulazione. Le linee ADSL sotto gli 8 Mbit sono solitamente G.DMT, le linee con velocità superiore sono sicuramente ADSL2 o ADSL2+.**

## 3.3.3. ACCESS MANAGEMENT (CONTROLLO ACCESSI)


### Access Management > ACL

In questa finestra è possibile gestire l'accesso alla configurazione del router secondo diverse modalità a scelta.




**ACL:** selezionate Activated per abilitare il controllo degli accessi al router.
**ACL Rule Index:** selezionate l'indice della regola che volete creare o modificare.
**Active:** selezionate Yes per abilitare la regola selezionata.
**Secure IP Address:** inserite l'indirizzo IP oppure il range di indirizzi IP della macchina o delle macchine a cui volete permettere l'accesso. Inserendo 0.0.0.0 indicherete tutte gli indirizzi IP.
**Application:** selezionate il tipo di servizio che volete rendere disponibile, a scelta tra Web, FTP, Telnet, SNMP, Ping, All (Tutte).
**Interface:** selezionate l'interfaccia di connessione dell'IP: WAN (Internet), LAN (Rete Locale), Both (Entrambe).

## Access Management > Filter

Questa sezione permette di bloccare alcuni servizi, in ingresso o uscita, basandosi sugli indirizzi IP o sulle porte utilizzate. Quando un pacchetto corrisponde alla regole definita, questo verrà filtrato.

**FILTER TYPE**


**Filter Type Selection:** a scelta tra 3 opzioni:

**1. IP / MAC Filter se volete creare una regola di firewall relativa a indirizzi IP oppure a Mac Address.**

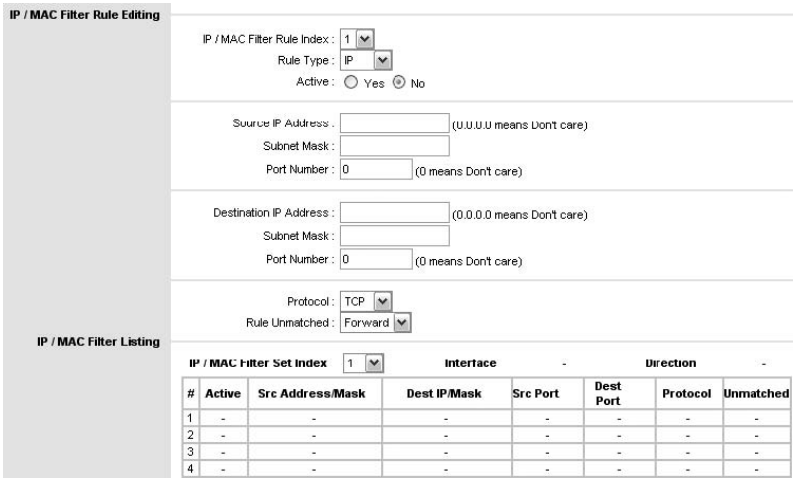
**IP / MAC FILTER SET EDITING**


**IP/MAC Filter Set Index**: selezionate in questo campo quale regola volete aggiungere o modificare. È possibile creare fino a 12 gruppi di regole per il filtering (ogni gruppo è formato da 6 regole).
**Interface:** selezionate l'interfaccia PVCX che state configurando.
**Direction:** selezionate la direzione dei pacchetti che volete controllare con questo gruppo di regole. Both (ingresso e uscita), Incoming (pacchetti in ingresso WAN LAN), Outgoing (pacchetti in uscita LAN WAN).

**IP / MAC FILTER RULE EDITING**


**IP / MAC Filter Rule Index:** selezionate in questo campo il numero della regola che volete aggiungere o modificare. Per ogni gruppo di regole è possibile creare fino a 6 regole diverse.
**Rule Type:** a scelta tra IP e MAC (vedi paragrafo sotto).
**Active:** selezionate Yes per attivare la regola selezionata. È possibile gestire le 6 regole a seconda della necessità (attivandole o disattivandole tutte o in parte).

- **RULE TYPE > IP**




Se volete configurare una regola basata sugli indirizzi IP vi saranno proposte le seguenti opzioni:

**Source IP Address:** inserite l'indirizzo IP sorgente della regola che volete creare (inserite 0.0.0.0 per escludere questo parametro).

**Subnet Mask:** inserite la Subnet Mask che identifica il gruppo di indirizzi IP sorgente, per indicare un singolo indirizzo IP inserite 255.255.255.255 .

**Port Number:** inserite il numero della porta sorgente (inserite 0 per escludere questo parametro).

**Destination IP Address:** inserite l'indirizzo IP di destinazione della regola che volete creare (inserite 0.0.0.0 per escludere questo parametro).

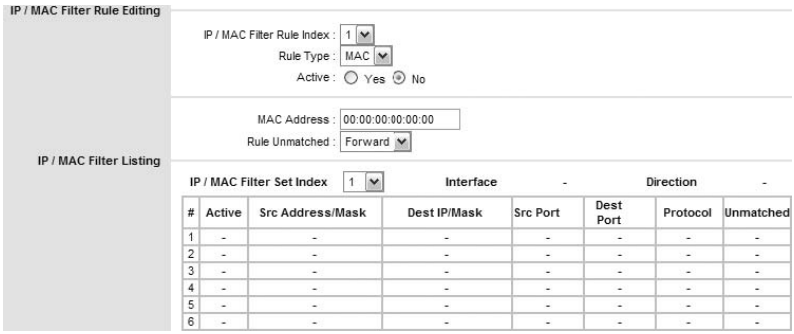
**Subnet Mask:** inserite la Subnet Mask che identifica il gruppo di indirizzi IP di destinazione, per indicare un singolo indirizzo IP inserite 255.255.255.255 .

**Port Number:** inserite il numero della porta di destinazione (inserite 0 per escludere questo parametro).

**Protocol:** selezionate il tipo di protocollo.

**Rule Unmatched:** selezionate il tipo di azione da intraprendere nel caso in cui il pacchetto analizzato NON corrisponda alla regola creata. Quando create un gruppo di regole (in ingresso per esempio) tutti i pacchetti in ingresso vengono analizzati sulla base delle regole inserite in tabella, da quella con indice #1 a quella con indice #6; se il pacchetto in ingresso corrisponde a una regola viene bloccato, in caso contrario l'analisi del pacchetto può essere sospesa se selezionate Forward (inoltra, permetti passaggio), oppure può essere analizzato dalla regola seguente se selezionate Next.
Quando in un gruppo inserite più regole sarà quindi selezionata per tutte l'opzione Next, tranne per l'ultima regola, che avrà l'opzione Forward.

- **RULE TYPE > MAC**

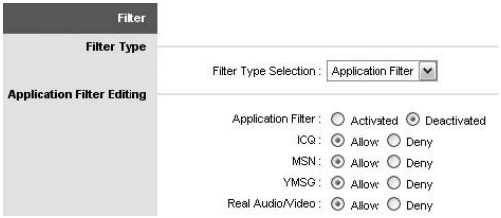



Per configurare una regola basata sul Mac Address avrete a disposizione queste opzioni:

**MAC Address:** inserite l'indirizzo MAC della macchina su cui far valere la regola che volete creare.

**Rule Unmatched:** selezionate il tipo di azione da intraprendere nel caso in cui il pacchetto analizzato NON corrisponda alla regola creata. Quando create un gruppo di regole (in ingresso per esempio) tutti i pacchetti in ingresso vengono analizzati sulla base delle regole inserite in tabella, da quella con indice #1 a quella con indice #6; se il pacchetto in ingresso corrisponde a una regola viene bloccato, in caso contrario l'analisi del pacchetto può essere sospesa se selezionate Forward (inoltra, permetti passaggio), oppure può essere analizzato dalla regola seguente se selezionate Next.
Quando in un gruppo inserite più regole sarà quindi selezionata per tutte l'opzione Next, tranne per l'ultima regola, che avrà l'opzione Forward.

**2. Application Filter per consentire o bloccare l'utilizzo di alcuni servizi predefiniti**




**Application Filter:** selezionate Activated per consentire (Allow) oppure bloccare (Deny) i seguenti applicativi:
- ICQ
- MSN
- YMSG
- Real Audio/Video

**3. URL Filter per abilitare il filtro delle pagine web visualizzabili**


**Active:** spuntate la casella Yes per attivare il filtro degli indirizzi Internet (URL). Di default quest'opzione non è attiva (casella No).

**URL Index:** numero progressivo di inserimento stringhe.

**URL:** l'indirizzo Internet che si desidera bloccare. La stringa d'indirizzo da inserire deve essere completa (ad esempio www.sex.com); se così non fosse (inserendo, ad esempio, solo www.sex) l'indirizzo incompleto non verrà bloccato. Il numero massimo di indirizzi bloccabili è pari a 16.

## Access Management > SNMP

In questa sezione è possibile modificare i parametri di accesso in SNMP.

## Access Management > UPnP

In questa sezione è possibile modificare le impostazioni dell'Universal Plug'n Play.

## Access Management > DDNS

In questa sezione è possibile abilitare la sincronizzazione con un dominio Dynamic DNS. La funzione di Dynamic DNS vi permette di associare a un dominio (ad es. vostronome.dyndns.org ) il vostro indirizzo IP di WAN, anche se dinamico; grazie a questa funzione è quindi possibile utilizzare servizi che richiedono solitamente un indirizzo IP statico, come la possibilità di hostare un server web, ftp o di accedere da remoto alla propria rete (FAQ in Capitolo 5).

## 3.3.4. MAINTENANCE (MANUTENZIONE)


### Maintenance > Administration

In questa sezione è possibile modificare la password di accesso alla configurazione del router.

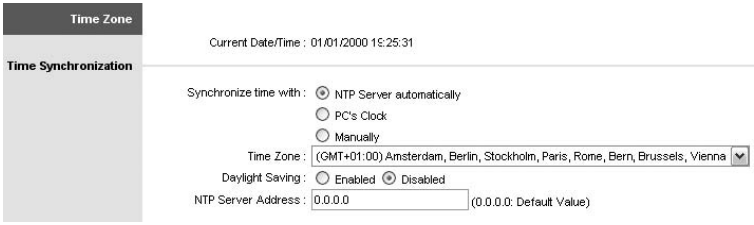

La password di default è di pubblico dominio (è scritta sui manuali), pertanto è sempre buona norma **modificare la password** con una personalizzata.
Inserite la nuova password da voi prescelta nel primo campo vuoto e poi riconfermatela nel secondo.

**Si consiglia di scrivere la password per ricordarsela. In caso di perdita della stessa è necessario resettare il router tramite il relativo pulsante (vedere capitolo 1).**

### Maintenance > Time Zone

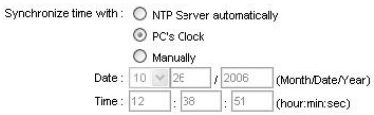
In questa sezione è possibile configurare la sincronizzazione dell'orologio interno del router, utilizzando appositi server presenti in Internet (chiamati appunto NTP Server). A scelta tra due opzioni:

- **NTP Server automatically**



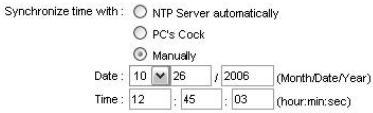

Selezionando quest'opzione l'orario verrà sincronizzato con un server apposito tramite Internet. Selezionate la **Time Zone** (fuso orario), abilitate o disabilitate il passaggio automatico all'ora legale (Daylight Saving) e inserite l'indirizzo IP del Server NTP nel campo **NTP Server Address**.

- **PC's Clock**




Sincronizzazione dell'orario con quello del PC.

- **Manually**




Inserimento manualmente di data e ora.

### Maintenance > Firmware

In questa sezione è possibile aggiornare il software interno del router.

**Utilizzate SOLO firmware rilasciati da Digicom S.p.A. - disponibili nell'apposita sezione (Supporto > Upgrade) sul nostro sito web http://www.digicom.it.**

**Le istruzioni per l'aggiornamento e le modifiche che questo apporterà al dispositivo sono solitamente descritte in un file di testo fornito insieme all'aggiornamento.**

**New Romfile Location:** tramite questa funzione è possibile caricare un file di configurazione precedentemente salvato. Con il pulsante Sfoglia… indicate il percorso per raggiungere il file di configurazione che si desidera ripristinare.

**Romfile Backup:** tramite questa funzione è possibile salvare su file l'attuale configurazione effettuata su Michelangelo Wave. Tramite il pulsante ROMFILE SAVE indicate la destinazione dove salvare il file.

### Maintenance > SysRestart

In questa sezione è possibile forzare un riavvio del dispositivo oppure un reset di tutte le impostazioni. A scelta tra:
- **Current Settings**, riavvia il dispositivo con la configurazione attuale.
- **Factory Default Settings**, riavvia il dispositivo e ripristina la configurazione di fabbrica (di default).


### Maintenance > Diagnostics

In questa sezione è possibile ottenere un rapporto di verifica sul funzionamento delle sezioni principali del router.

**Una volta selezionata la relativa pagina dal menù principale, si prega di attendere almeno 10 SECONDI prima di visualizzarne il contenuto, corrispondente al tempo minimo di caricamento delle informazioni da parte del sistema.**

### 3.3.5. STATUS (STATO)


#### Status > Device Info

In questa finestra è possibile verificare lo stato di tutte le interfacce del router.

#### Status > System Log

In questa finestra è possibile leggere un rapporto dettagliato delle attività di sistema del dispositivo, per poterne verificare l'attività in caso di problemi.

#### Status > Statistics

In questa finestra è possibile ottenere un rapporto dei pacchetti inviati e ricevuti sull'interfaccia Ethernet, ADSL e WLAN.

# 4. IMPOSTAZIONI DI SICUREZZA



Questo capitolo vuole essere una base di partenza per portare all'attenzione dell'utente gli strumenti di sicurezza di primo livello già presenti nei prodotti Digicom, spiegare come utilizzarli e proteggere così la propria rete privata o aziendale in modo semplice ma efficace.
Il secondo livello di sicurezza è dato da ulteriori contromisure aggiuntive, a scelta dell'utente, come software anti-virus, anti-spam, anti-malware e firewall.

**Bastano poche e semplici operazioni o accorgimenti di buon senso per risolvere gran parte dei problemi più comuni legati alla sicurezza della propria rete.**

## 4.1. COS'È UNA RETE?

Una rete è composta da almeno due computer o dispositivi in grado di comunicare tra loro, all'interno della rete locale (LAN, Local Area Network) e/o con il mondo esterno (WAN, Wide Area Network, comunemente la rete Internet).

Più nel dettaglio:

- **una rete "LAN" locale**

Quando si collegano due o più computer attraverso una connessione Ethernet, diretta o tramite switch, la rete è sostanzialmente costituita da queste macchine e si dice essere una rete locale.

In questo caso il concetto di sicurezza può essere delimitato alla possibilità che le informazioni di una macchina debbano o meno essere accessibili dall'altra. Attivando opportunamente la gestione degli utenti, le password e le condivisioni di file e cartelle si può realizzare una 'policy di sicurezza' consentendo solo a chi è autorizzato l'accesso a determinate risorse.
I pericoli ai quali si è esposti provengono prevalentemente dall'interno della rete stessa, inseriti su uno dei computer tramite floppy, CD-ROM, Memory Stick USB o altri media. Questi potrebbero contenere file infettati da virus, trojan o altro codice malware che successivamente si propagherebbe alle altre macchine in rete. Contro questo tipo di attacchi è opportuno che venga installato un software Anti-virus e Anti-Malware.
Non esistendo interconnessioni dirette con altre reti o con il mondo esterno costituito da Internet, si può stare ragionevolmente tranquilli.

- **una rete "LAN to Internet"**

Se il vostro computer è invece in qualche modo connesso a Internet, ecco che lo scenario si amplia notevolmente e le possibilità di essere esposti a pericoli ed attacchi cresce in modo esponenziale. Possiamo chiamare questa rete di tipo 'LAN to Internet' oppure 'LAN to WAN'.
Il punto debole di una rete connessa ad Internet, ma anche del singolo computer connesso a un modem, è - da un lato - il fatto stesso di poter accedere a una quantità svariata e praticamente illimitata di siti, database e informazioni, e - dall'altro - il fatto di poter essere raggiunti dall'esterno se non si è 'schermati' in qualche modo.

I pericoli si possono annidare:

- nei file che si scaricano, quindi in un qualcosa che l'utente deliberatamente porta all'interno della propria rete. In questo caso un buon software anti-virus/malware è già una ottima protezione, tanto più efficace quanto più aggiornati sono i database di riconoscimento dei codici infetti.
- nelle e-mail con allegati infetti. Anche in questo caso un buon software anti-virus/malware è la soluzione più adeguata.
- nei siti web visitati che possono contenere codici nascosti, come script Java, ActiveX, ecc. che possono installare o eseguire programmi nascosti e invisibili. Per queste situazioni è necessario agire in primo luogo sul browser, che è la porta d'ingresso per questo tipo di attacchi, attivando un livello di sicurezza medio-alto, agendo sulle impostazioni e disabilitando pop-up ed esecuzione automatica di script di vario tipo. L'installazione di un software 'Personal Firewall' può innalzare ulteriormente il livello di sicurezza.
- in intrusioni dall'esterno dovute a errata o insufficiente configurazione dei dispositivi che interconnettono la rete a Internet. In questo caso è bene accertarsi che non si siano inavvertitamente lasciate aperte delle falle che potrebbero essere sfruttate dagli hacker.

- **una rete "wireless"**

Per rete wireless si intende una rete LAN, oppure LAN to Internet, che abbia al suo interno uno o più 'punti di accesso' basati su tecnologie radio senza fili. Il concetto stesso del 'senza fili' presuppone che ci si possa (e debba) collegare a questa rete senza dover fisicamente collegare un cavo (e quindi in modo 'invisibile'), e che lo si possa fare virtualmente da ovunque ci si trovi purché nel raggio di copertura del segnale radio.
Questo tipo di rete è quella in assoluto più attaccabile e vulnerabile per sua stessa natura, e che necessita di maggiori accorgimenti per essere resa sicura o sufficientemente protetta da intrusioni indiscriminate.
Il fatto che la copertura radio 'esca' dai confini fisici dell'abitazione o dell'ufficio nella quale è installata la rende disponibile ad altri, che ne captano il segnale, e (se questa rete è 'aperta') di fatto la estende a qualsiasi utente esterno che voglia entrare a farne parte. Ecco che in questo caso è fondamentale mettere in atto le misure di sicurezza che delimitino l'accesso ai soli utenti legittimi ed autorizzati rendendo nulle le possibilità di intrusione da parte di chi pur ricevendone il segnale radio tenti di accedervi.

## 4.2. PERCHÉ ATTIVARE QUESTE MISURE DI SICUREZZA?

Per evitare che qualcuno possa entrare nella nostra proprietà, rubarci qualcosa, spiarci o semplicemente venire a conoscenza di cose e fatti personali e privati.

C'è un altro aspetto importantissimo da considerare e che è diventato di sempre più scottante attualità: il furto d'identità. Dobbiamo cioè preoccuparci del fatto che qualcuno possa utilizzare qualcosa che ci appartiene (o che sia riconducibile alla nostra identità) per compiere azioni, frodi o fatti criminali come ad esempio (nella realtà) la nostra automobile per compiere una rapina oppure (online) il nostro numero di carta di credito per fare acquisti o operazioni bancarie.
Ricorrendo a una metafora semplice ma efficace, è possibile paragonare il nostro computer o la nostra rete di computer e i dispositivi che ne fanno parte alla nostra casa, e in particolare:

- la serratura di casa equivale alla password di amministrazione;
- le chiavi di casa equivalgono alle chiavi di crittografia dei dispositivi di accesso wireless;
- il sistema di allarme antifurto equivale al firewall ed ai sistemi di filtering.

Lasciare la 'porta aperta' non significa necessariamente che qualcuno si introdurrà, ma di certo garantisce che se qualcuno tenterà di entrare (e quindi ha già una qualche volontà o intenzione precisa) non desista dal farlo.
Ecco lo scopo di questa breve guida: mettervi a conoscenza dei potenziali rischi e suggerirvi di attuare poche e semplici contromisure, gratuite e prontamente disponibili nel vostro router, access point o firewall Digicom. La decisione finale di attuarle o meno è ovviamente lasciata al singolo utente. Non necessariamente l'attuazione significa una garanzia di protezione totale, ma sicuramente vi mette al riparo da una discreta quantità di pericoli nascosti.

## 4.3. QUALI FUNZIONI DI SICUREZZA, QUALI RISULTATI?

A seconda del dispositivo avrete a disposizione diverse opzioni e funzionalità di sicurezza.
Vediamo di seguito le opzioni più comuni e le loro particolarità, rimandando alla manualistica e documentazione dei singoli prodotti per un eventuale approfondimento tecnico.

- **User Id e password di amministrazione**

E' sicuramente il primo sbarramento di accesso a un dispositivo. Tutti i dispositivi di rete (wireless e non) ne hanno almeno una che consente all'amministratore (o proprietario) di accedere alla configurazione dell'apparato. Solitamente hanno dei valori di fabbrica identici a molti altri apparati, spesso il default è admin - admin, e sono uno dei più comuni problemi di sicurezza, perchè pochissimi utenti le cambiano dopo aver installato un router, access point o firewall.

**ATTENZIONE!**
**Lasciare le password di accesso al default è come lasciare le chiavi nella toppa della porta blindata!**

Lasciare aperta la possibilità di modificare la configurazione può essere fonte di grossi problemi. Oltre ad abbassare o disattivare le difese, un intruso (umano o programma automatizzato) potrebbe ad esempio modificare le impostazioni DNS per ridirigere l'accesso a un sito bancario verso uno fittizio e identico a quello reale, carpendo così le informazioni di accesso dell'utente (phishing), oppure ridirigere le richieste di Windows Update verso un sito che in realtà non effettua mai gli aggiornamenti o le patch di sicurezza (pharming) lasciando eventuali malware o trojan in rete liberi di funzionare indisturbati.
È quindi buona regola modificare le password, inserendo una parola o sequenza di caratteri il più possibile difficile da indovinare. Sono assolutamente da evitare le classiche combinazioni (es. pippo-pluto) e sconsigliabili le date di nascita (ricavabili dal codice fiscale), i nomi di figli, mogli o mariti (non necessariamente difficili da conoscere).

Più è complessa la password, maggiore è la sua sicurezza intrinseca. Se possibile, cambiatela spesso.
Non utilizzate la stessa password per più dispositivi o servizi perchè una volta scoperta sono potenzialmente a rischio tutti.

| | |
|---|---|
| Risultato: | impedire l'accesso non autorizzato alla configurazione del dispositivo. |
| Importanza: | ALTA |

- **SSID di una rete wireless**

Una rete wireless si basa sull'esistenza di un SSID (Service Set Identifier), o più semplicemente il 'nome della rete wireless', configurato nell'Access Point (punto di accesso) al quale tutti gli altri dispositivi faranno riferimento per entrare a far parte di questa rete. Anche in questo caso i valori di fabbrica possono essere comuni a molti apparati, anche di costruttori diversi (spesso default, ap-wlan, wireless).
Modificate l'SSID dopo la configurazione dell'apparto inserendo un valore o parola univoca che possibilmente non riconduca alla marca o modello del vostro dispositivo o alla funzione della rete. Se possibile 'nascondete' l'SSID della rete (vedi più sotto).

| | |
|---|---|
| Risultato: | Evitare che si possa riconoscere il tipo o modello di dispositivo per tentare di accedervi basandosi su impostazioni di fabbrica conosciute. |
| Importanza: | MEDIA |

- **Nascondere l'SSID di una rete wireless**

Come descritto sopra, per entrare a far parte di una rete wireless è indispensabile conoscerne il 'nome' SSID. Normalmente i client effettuano una scansione radio dei SSID creando poi una lista delle reti wireless disponibili per permettere all'utilizzatore di scegliere a quale collegarsi.
Molti Access Point wireless possono nascondere l'SSID (non renderlo pubblico) evitando di trasmettere questa informazione via radio.
Attivando l'opzione 'Hide SSID' oppure 'Disable SSID broadcasting' la vostra rete non comparirà più in alcuna lista, escludendo automaticamente i vostri vicini, eventuali hacker e sniffer, permettendo l'accesso solamente ai vostri computer nei quali avrete configurato manualmente l'SSID.

| | |
|---|---|
| Risultato: | Rendere invisibile la rete wireless alle scansioni automatiche ed evitare tentativi di intrusione. |
| Importanza: | ALTA |

- **Attivare la crittografia in una rete wireless**

Tra le opzioni di sicurezza delle reti wireless è quella più importante. Una rete wireless non crittografata è assolutamente non sicura.
Se l'SSID è trasmesso 'in chiaro' (non nascosto) e non avete attivato la crittografia dei dati, chiunque riceva il segnale del vostro access point wireless può indisturbatamente entrare a far parte della rete, accedere ai vostri computer, ai vostri dati, utilizzare la vostra connessione Internet. In quest'ultimo caso le eventuali operazioni commesse in rete saranno ricondotte al vostro account (!) perchè originate dall'indirizzo IP del vostro router di accesso a Internet.

Tutti i dispositivi wireless implementano almeno un algoritmo di crittografia dei dati come il protocollo WEP o i più moderni WPA e WPA2. Si tratta sostanzialmente di password che verranno utilizzate per creare delle chiavi di crittografia applicate ai dati trasmessi tra il client e l'access point. Maggiore è il numero di bit che compongono la chiave, maggiore è la sicurezza applicata.

Attivate sempre la crittografia dei dati, possibilmente utilizzate gli algoritmi basati si WPA o WPA2 ed inserite dei valori composti da un numero più alto possibile di caratteri o numeri. Se il dispositivo supporta solamente la crittografia WEP utilizzatela comunque, perchè pur essendo meno elaborata della WPA offre comunque un buon livello di sicurezza.
Molti utenti non attivano la crittografia perchè ritengono che diminuisca le prestazioni. Questo non è sempre vero perchè dipende dal tipo di processore adottato dal dispositivo, e comunque, il beneficio apportato dalla sicurezza è di gran lunga superiore a qualche KB di velocità in più.

| | |
|---|---|
| Risultato: | Rendere impossibile la lettura e decodifica dei dati trasmessi. Se venissero intercettati (sniffing) i pacchetti della rete, la crittografia dei dati li rende non intelleggibili e molto difficili da crackare. |
| Importanza: | ALTA |

- **Attivazione di filtri a livello indirizzo MAC e regole di Firewall**

Molti dispositivi supportano funzionalità di filtering a vari livelli. Quello più efficace è rappresentato dal MAC filtering, una sorta di lista autorizzata per i client che si basa sul MAC Address (o indirizzo fisico) dell'interfaccia di rete cablata o wireless. Questo parametro è un dato univoco, una sorta di impronta digitale, che identifica ogni dispositivo in modo inequivocabile perchè virtualmente non esistono due indirizzi MAC uguali.
Attivando il MAC filtering si può stabilire che un determinato utente possa accedere in rete solamente se lo fa dal computer in cui l'indirizzo MAC della scheda di rete è esattamente quello configurato nel filtro. Un eventuale intruso non potrà accedere in rete perchè, pur simulando User Id, Password e indirizzi IP, dovrà simulare anche il MAC Address, cosa non impossibile ma tutt'altro che semplice.
Attivando anche il firewall si possono aggiungere ulteriori regole per impedire a un utente non autorizzato di accedere a determinate risorse, basandosi sul suo indirizzo IP sorgente, oppure al servizio o protocollo utilizzato.

| | |
|---|---|
| Risultato: | Restringere l'accesso alla rete ai soli computer dotati dell'hardware (schede di rete) dei quali si è inserito l'indirizzo fisico, oppure nel caso delle regole firewall, solamente a specifici utenti dotati del giusto indirizzo IP. |
| Importanza: | MEDIA |

- **Definire una porta diversa per il Management**

Alcuni dispositivi permettono di cambiare la porta HTTP per l'accesso alla configurazione. Di default la porta è impostata a 80, valore standard per le pagine web. Se modificate questo valore impostandolo ad esempio a 88, per accedere alla configurazione del dispositivo dovrà essere inserito l'URL http://indirizzo-IP-del-dispositivo:88

| | |
|---|---|
| Risultato: | Impedire tentativi di accesso alla configurazione da parte di utenti o programmi standard. |
| Importanza: | MEDIA |

- **Definire un indirizzo IP specifico per il Management**

Alcuni dispositivi permettono di definire un indirizzo IP ben preciso dal quale permettere l'accesso alla configurazione. Di default questo indirizzo è impostato a 0.0.0.0 (per definizione corrisponde a 'qualsiasi'). Inserendo un indirizzo IP specifico, le modifiche alla configurazione potranno essere effettuate solamente da quel computer, ad esempio dell'amministratore di rete, e non dagli altri utenti.

| | |
|---|---|
| Risultato: | Impedire tentativi di accesso alla configurazione da qualsiasi computer della rete. |
| Importanza: | MEDIA |

- **Disabilitare il Management remoto o attraverso altri metodi**

Alcuni dispositivi permettono la configurazione attraverso protocolli e metodi diversi dall'HTTP (browser web) come ad esempio Telnet, SNMP, RMON, FTP, TFTP.
Se alcune di queste opzioni fossero abilitate di default e non intendete utilizzarle (oppure semplicemente non le conoscete), disabilitatele senza indugio. Così facendo ridurrete il rischio che applicazioni, applet, script o altro malware possano modificare a vostra insaputa la configurazione, magari disattivando altre opzioni di sicurezza. Se non necessaria, non permettete la configurazione remota (dalla WAN o da Internet) disabilitando anche questa opzione.

| | |
|---|---|
| Risultato: | Impedire tentativi di accesso alla configurazione da Internet o da applicazioni indesiderate o difficilmente controllabili in quanto eseguite da programmi malware invisibili. |
| Importanza: | ALTA |

- **Disabilitare il servizio DHCP**

Il servizio DHCP permette di semplificare notevolmente le operazioni di configurazione di una rete basata su protocollo TCP/IP, in quanto si occupa di assegnare automaticamente ad ogni client che ne faccia richiesta tutti gli indirizzi IP necessari al funzionamento in rete e alla navigazione in internet. Questa comodità è a vantaggio anche di chi dovesse riuscire a penetrare le difese. Senza questo servizio l'intruso dovrebbe riuscire a identificare anche un indirizzo IP sicuramente valido per il client nonché quello del gateway ed eventuali altri.
Tra le precauzioni è probabilmente quella meno efficace ma rimane pur sempre valida.

| | |
|---|---|
| Risultato: | Non offrire parametri di configurazione di rete in modo automatico che facilitano il compito a un eventuale intruso. |
| Importanza: | BASSA |

# 5. F.A.Q.



Il seguente capitolo offre una panoramica delle principali F.A.Q. (presenti anche sul nostro sito) per la risoluzione dei quesiti più frequenti.

## 5.1. ENCRYPTION (CRITTOGRAFIA)

**Domanda**: Come posso abilitare la crittografia dei dati sul collegamento wireless?

**Risposta**: La crittografia è uno strumento per la sicurezza della rete wireless che permette solo agli apparati configurati in modo corretto la possibilità di accedere alla rete wireless. Questo presuppone il fatto che tutti i dispositivi presenti sulla rete wireless debbano essere configurati nella stessa modalità, quindi sia Michelangelo Wave 300 sia le diverse schede di rete wireless.

Ad oggi, la crittografia dei dati sul collegamento wireless utilizza diversi protocolli. Su Michelangelo Wave 300 sono stati implementati il protocollo WEP e WPA.

Il protocollo WEP si appoggia a un algoritmo di crittografia basato su una chiave numerica (tipicamente in formato esadecimale con caratteri da "0" a "9" e da "a" a "f"). Questa chiave può essere di varia lunghezza, in termini di numero di caratteri che compongono la chiave. Su Michelangelo Wave 300 è possibile impostare il protocollo WEP a 64 bit (che equivale a una chiave di 10 caratteri esadecimali) oppure a 128 bit (che equivale a una chiave di 26 caratteri esadecimali).

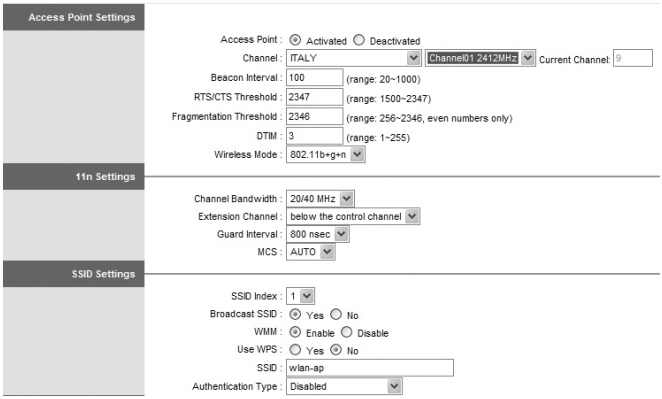
Il protocollo WPA è invece successivo a quello WEP e offre una maggiore sicurezza, in quanto la chiave di crittografia non è fissa, ma viene modificata periodicamente durante la connessione wireless in base a una stringa alfanumerica preimpostata.

In questo caso la stringa non richiede caratteri esadecimali, ed è quindi possibile inserire tutti i caratteri dell'alfabeto e tutti i numeri. Non è possibile invece inserire caratteri particolari, come ad esempio le lettere accentuate, la punteggiatura e i simboli matematici.

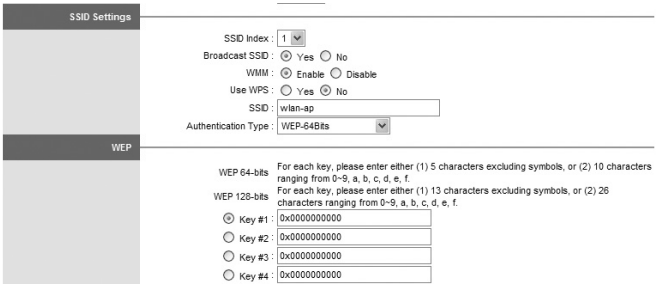
In questa procedura verranno illustrate entrambe le possibili configurazioni.

### 5.1.1. WEP (WEP-64bits/WEP-128bits)

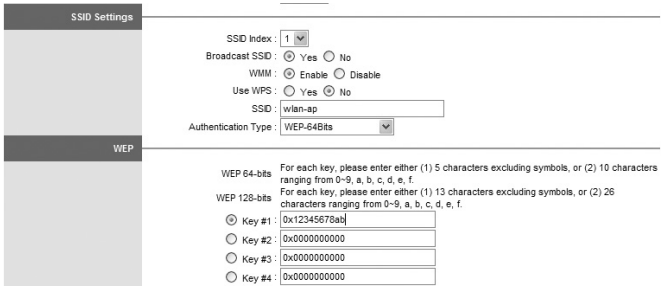
- Accedete al menù di configurazione di Michelangelo Wave 300, nella sezione Interface **Setup > Wireless**.




- Alla voce **Authentication Type** selezionate WEP-64bit oppure WEP-128bit a seconda delle proprie esigenze. In una prima fase consigliamo l'abilitazione della crittografia a 64 bit.
- Dopo alcuni istanti la pagina di configurazione verrà aggiornata inserendo un campo aggiuntivo:




- Nel campo Key #1 inserite la chiave esadecimale prescelta preceduta dalla stringa 0x (zero-ics). Potete inserire, ad esempio, la stringa:
  0x12345678ab




- e poi premere il pulsante “Save” in fondo alla pagina.

**La configurazione di Michelangelo Wave 300 per l’abilitazione della crittografia è completata. È ora necessario configurare ogni singolo PC dotato di connessione wireless, per permettere l’instaurazione del collegamento.**

## Configurazione crittografia WEP 64 bit con utility Zero Configuration (Windows Vista)

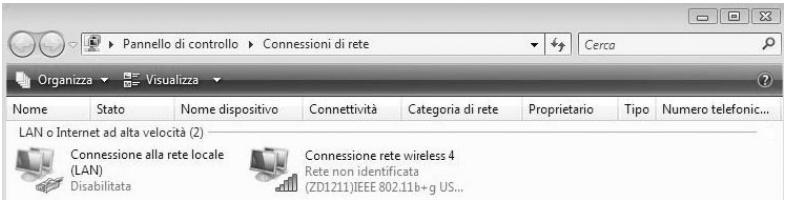
- Cliccate sull'icona **Start** , posizionata in basso a sinistra dello schermo del computer, e poi selezionate la voce **Pannello di Controllo**.


- Comparirà la finestra relativa al **Pannello di Controllo**.

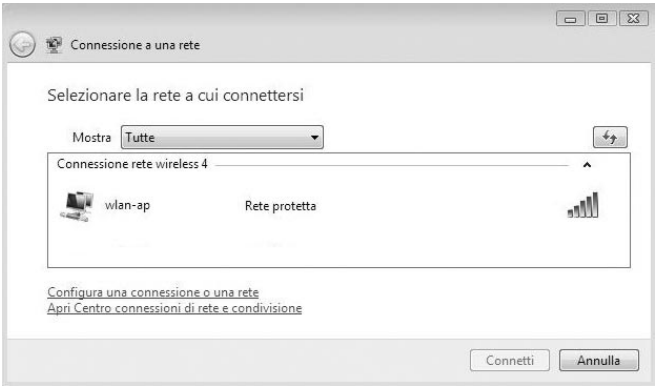

- In modalità di **Visualizzazione Classica** effettuate un doppio click sull'icona **Centro connessioni di rete e condivisione**.


- Nella finestra **Centro connessioni di rete e condivisione** selezionate **Gestisci connessioni di rete**.

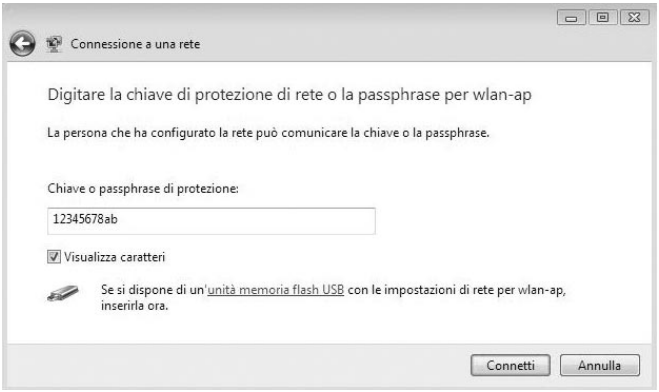

- Selezionate la **Connessione rete Wireless** e con il tasto destro del mouse selezionate l'opzione **Connetti / Disconnetti.**




- Selezionate la rete **Wlan-ap** che l'utility Zero Configuration indica come **Rete protetta** e premete il pulsante **Connetti**.



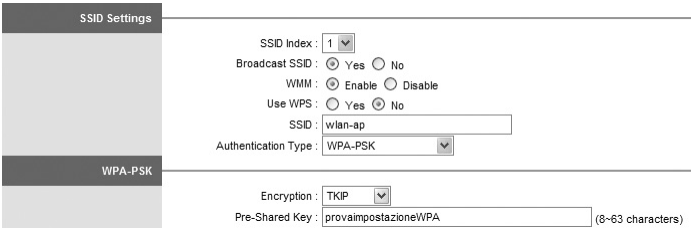

- Nella finestra successiva inserite la chiave di crittografia WEP che avete precedentemente inserito nella configurazione del Michelangelo Wave 300 e premete **Connetti**.




- Dopo alcuni istanti, l'utility Zero Configuration indicherà l'avvenuta connessione alla rete Wireless. Spuntate le voci **Salva questa rete** e **Avvia questa connessione automaticamente** in modo tale che all'avvio del PC la connessione wireless venga instaurata automaticamente.


### 5.1.2. WPA (WPA-PSK/WPA2-PSK)

- Accedete al menù di configurazione di Michelangelo Wave 300, nella sezione **Interface Setup > Wireless**.




- Selezionate nel campo **Authentication** Type la voce **WPA-PSK**.
- Dopo alcuni istanti verrà aggiunta in automatico una sezione di configurazione relativa alla crittografia WPA-PSK. Nel campo **Pre-Shared Key** inserite una stringa alfanumerica, senza spazi, caratteri accentuati e punteggiatura e premete il pulsante **SAVE** a fine pagina per abilitare la crittografia.
  Nell'esempio è stato impostata la stringa: **provaimpostazioneWPA**.

## Configurazione crittografia WPA con utility Zero Configuration (Windows Vista)

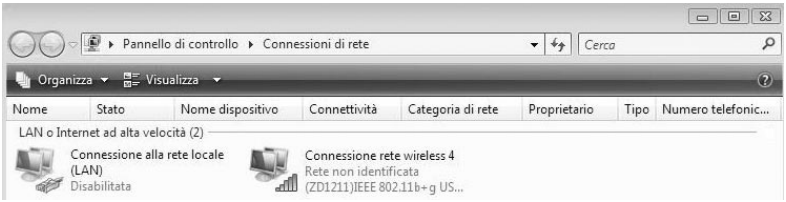
- Cliccate sull'icona **Start** , posizionata in basso a sinistra dello schermo del computer, e poi selezionate la voce **Pannello di Controllo**.


- Comparirà la finestra relativa al **Pannello di Controllo**.

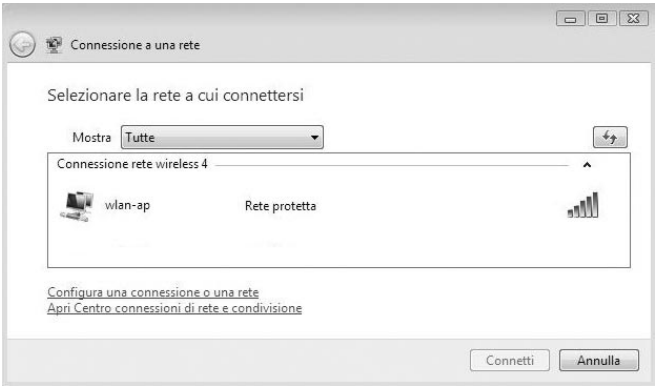

- In modalità di **Visualizzazione Classica** effettuate un doppio click sull'icona **Centro connessioni di rete e condivisione**.


- Nella finestra **Centro connessioni di rete e condivisione** selezionate **Gestisci connessioni di rete**.

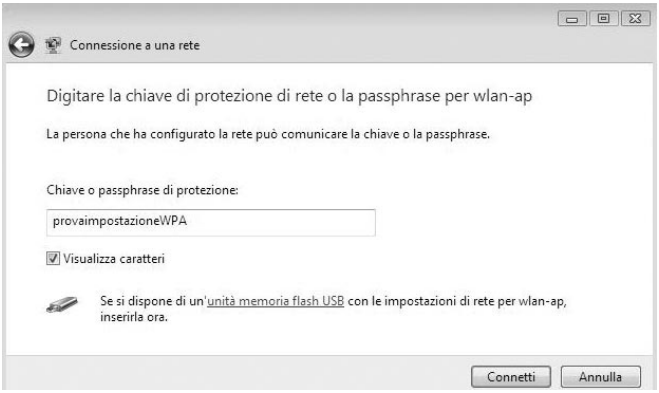

- Selezionate la **Connessione rete Wireless** e con il tasto destro del mouse selezionate l'opzione **Connetti / Disconnetti.**




- Selezionate la rete **Wlan-ap** che l'utility Zero Configuration indica come **Rete protetta** e premete il pulsante **Connetti**.




- Nella finestra successiva inserite la chiave di crittografia WAP inserita nella configurazione del Michelangelo Wave 300 e premete **Connetti**.




- Dopo alcuni istanti, l'utility Zero Configuration indicherà l'avvenuta connessione alla rete Wireless. Spuntate le voci **Salva questa rete** e **Avvia questa connessione automaticamente** in modo tale che all'avvio del PC la connessione wireless venga instaurata automaticamente.

## 5.2. CONFIGURAZIONE DEI CLIENT WIRELESS TRAMITE WPS

E' possibile configurare le stazioni di rete Wireless, in modo semplice ed automatizzato, tramite la funzione WPS. Questa funzionalità permette di configurare automaticamente la crittografia della rete Wireless sui PC che dispongono una scheda di rete Wireless compatibile con questo protocollo. Prima di effettuare questa procedura, verificate che la scheda di rete supporti il WPS.

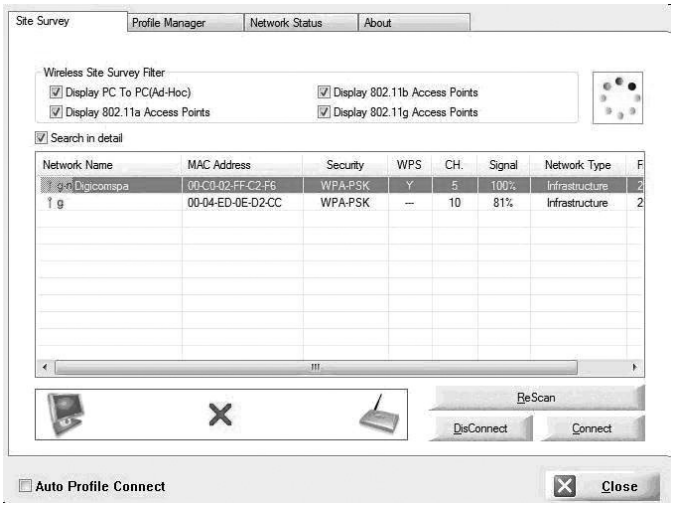
**Sono possibili tre modalità diverse di WPS:**

- **WPS tramite pressione del pulsante sul Michelangelo Wave 300**
- **WPS tramite scambio PIN inizializzato dal Michelangelo Wave 300**
- **WPS tramite scambio PIN inizializzato dal Client Wireless**

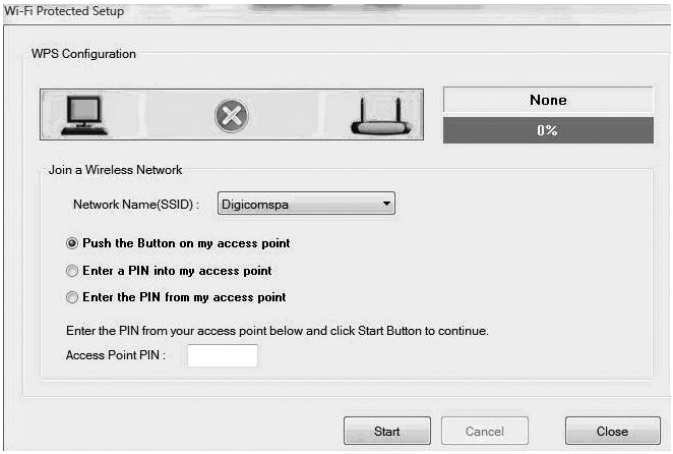
In questa procedura faremo riferimento all'utilizzo del Client Wireless USB Wave 300 in tutte e tre le situazioni. Per poter utilizzare il WPS, è necessario che sul Michelangelo Wave 300 sia già stata abilitata la crittografia WPA-PSK oppure la WPA2-PSK (vedi paragrafo 5.1).

### WPS tramite pressione del pulsante sul Michelangelo Wave 300

- Sul PC con USB Wave 300 installata, avviate l'utility di gestione dell'adattatore IEEE802.11n .
- Selezionate il menù a tendina **Site Survey** e premete il pulsante **Refresh**. Terminata la scansione delle reti Wireless, verificate che venga rilevata la rete gestita dal Michelangelo Wave 300 (**nell'esempio Digicomspa**)




- Selezionate la rete **Digicomspa** e premete il pulsante **Connect**. Dato che la crittografia su questa rete è abilitata, verrà mostrato direttamente il menù relativo alla gestione del **WPS**.

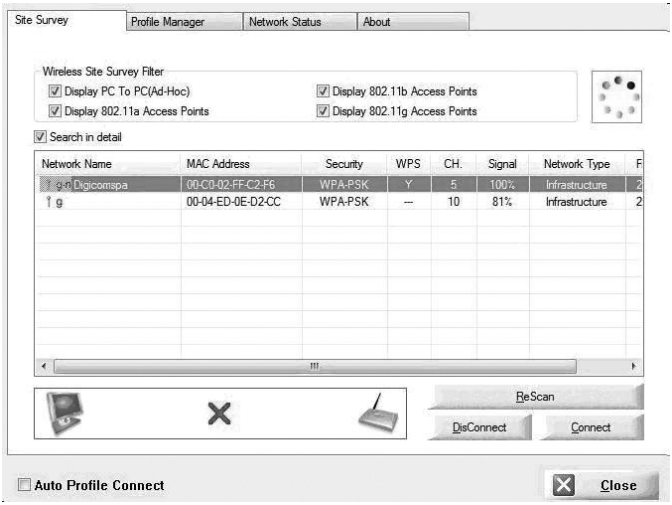



- Cliccate il pulsante **WPS** presente nella parte posteriore del Michelangelo Wave 300 e verificate che il led **WPS** inizi a lampeggiare.
- Ritornate ora sul Client Wireless e premete il pulsante **Start** e attendete che l'utility termini con successo la procedura di configurazione.

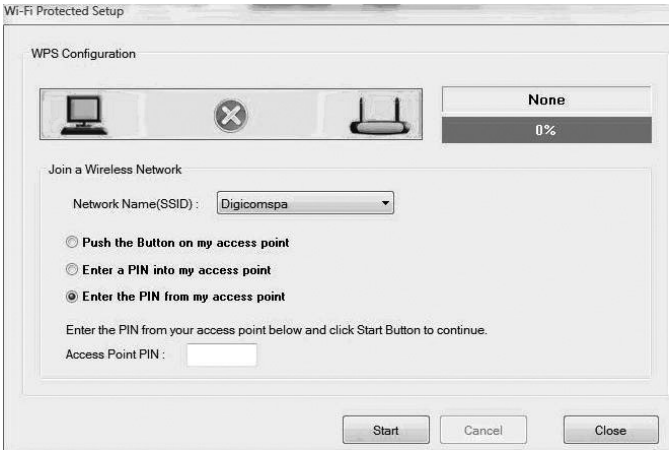

- Premete il pulsante **Close** a tutte le finestre proposte e verificate che il computer riesca ad accedere su Internet.
- Se necessario effettuare questa procedura su tutte le stazioni Wireless in rete che dispongano di una scheda di rete Wireless con supporto WPS.

## WPS tramite scambio PIN inizializzato dal Michelangelo Wave 300

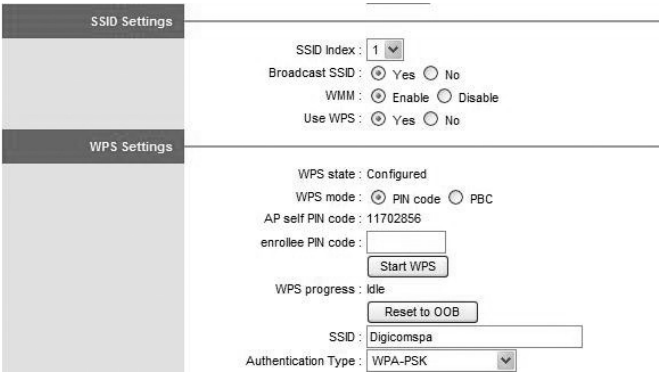
- Sul PC con USB Wave 300 installata, avviate l'utility di gestione.
- Selezionate il menù a tendina **Site Survey** e premete il pulsante **Refresh**. Terminata la scansione delle reti Wireless, verificate che venga rilevata la rete gestita dal Michelangelo Wave 300 (**nell'esempio Digicomspa**).




- Selezionate la rete **Digicomspa** e premete il pulsante **Connect**. Dato che la crittografia su questa rete è abilitata, verrà mostrato direttamente il menù relativo alla gestione del **WPS**.
- Selezionate la voce **Enter the PIN from my Access Point;** nel campo **Access Point PIN** dovrete inserire il codice **PIN** inserito nel menù di configurazione WPS del Michelangelo Wave 300.




- Prima di procedere con l'utility, da un PC collegato al Michelangelo Wave 300, entrate nel menù di configurazione nella sezione Wireless. Verificate che sia impostata su **Yes** il campo **Use WPS**. Nel campo **WPS Mode** mettere la spunta sulla voce **PIN Code** e prendete nota del PIN indicato nel campo **AP Self PIN Code**.

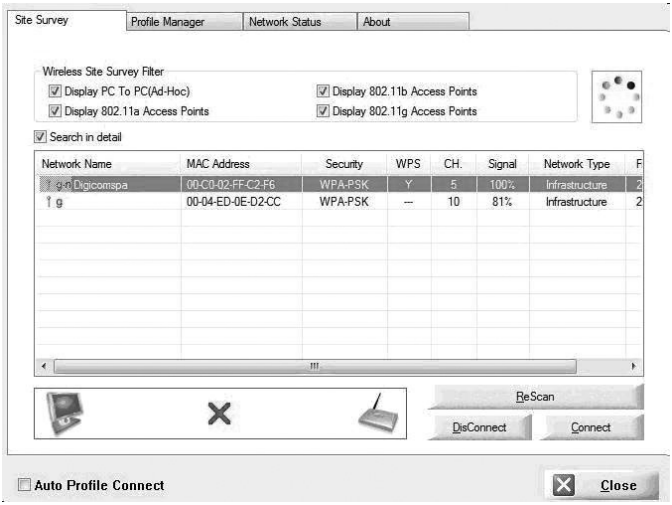



- Premete il pulsante **Start WPS** per avviare la procedura di configurazione automatica.
- Spostatevi nuovamente sul PC Client Wireless e inserite il PIN indicato nella configurazione del Michelangelo Wave 300 e premete il pulsante **Start**.

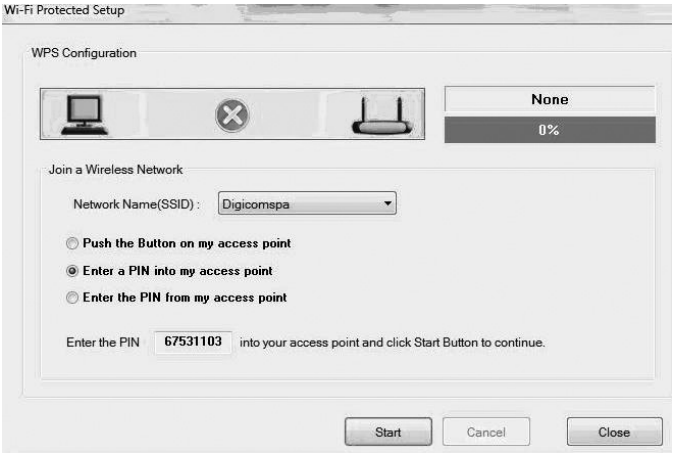

- Verificate che venga mostrata l'avvenuta connessione.

## WPS tramite scambio PIN inizializzato dal Client Wireless 802.11n

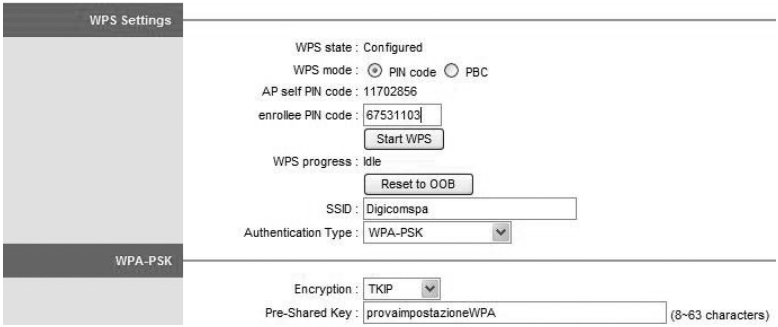
- Sul PC con USB Wave 300 installata, avviate l'utility di gestione dell'**adattatore IEEE802.11n**.
- Selezionate il menù a tendina **Site Survey** e premete il pulsante **Refresh**. Terminata la scansione delle reti Wireless, verificate che venga rilevata la rete gestita dal Michelangelo Wave 300 **(nell'esempio Digicomspa**).



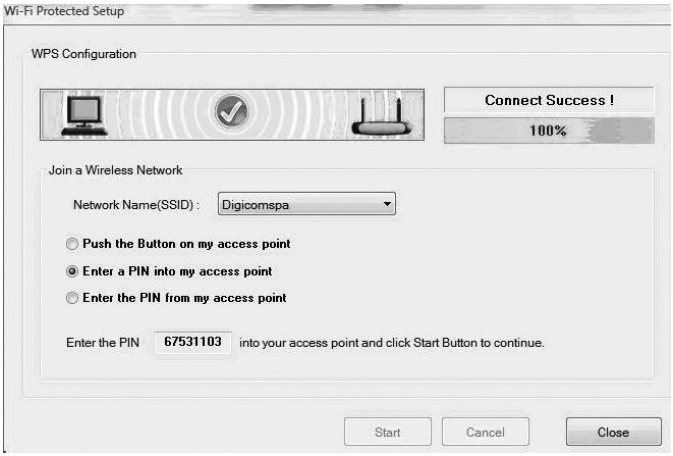

- Selezionate la rete **Digicomspa** gestita dal Michelangelo Wave 300 e premete il pulsante **Connect**. Dato che la crittografia su questa rete è abilitata, verrà mostrato direttamente il menù relativo alla gestione del **WPS**. Selezionate la voce **Enter a PIN into my Access Point**; nel campo **Enter the PIN** viene mostrato il codice **PIN** da inserite all'interno della configurazione **WPS** del Michelangelo Wave 300. Prendete nota del PIN.




- Entrate nel menù di configurazione del Michelangelo Wave 300 da un PC attualmente collegato e accedete alla sezione **WPS** presente nel menù **Interfaces Setup -> Wireless**. Inserite il codice indicato nell'utility di gestione dell'USB Wave 300 nel campo **enrollee PIN Code**.




- Premete il pulsante **Start WPS** per avviare la procedura.
- Dopo circa 3/4 secondi dalla pressione del pulsante, ritornate sul Client Wireless e premete il pulsante **Start** relativo alla gestione del WPS dell'utility.




- Verificate che, dopo alcuni istanti, la connessione avvenga con successo.

## 5.3. ADSL A TEMPO/CONSUMO

**Domanda**: Ho un abbonamento a tempo/consumo, come devo configurare il router ADSL in modo tale che non rimanga sempre connesso a Internet?

**Risposta**: Michelangelo Wave, come tutti i router ADSL ad oggi in commercio, è stato sviluppato per permettere l'accesso Internet a un'intera LAN di PC. Per permettere questa funzionalità, il router ADSL si sostituisce al PC, ed è questo apparato stesso a negoziare direttamente con la centrale la connessione. È quindi il router ad essere connesso a Internet, a differenza dell'utilizzo di un modem ADSL, in cui è comunque il PC a connettersi a Internet (tramite la connessione remota di Windows).

Con abbonamenti a tempo/consumo, il router ADSL manterrà sempre attiva la connessione.
Su questo tipo di linee ADSL non è consigliato l'utilizzo di un router, in quanto non è possibile gestire direttamente la connessione a Internet dal PC. In questa situazione si consiglia vivamente di spegnere il router ADSL oppure scollegare il cavo di linea ADSL dell'apparato quando non si necessita della connessione a Internet.
Michelangelo Wave 300 può comunque essere configurato in modo tale che, se l'apparato non rilevasse traffico dati verso Internet per un determinato periodo di tempo, il dispositivo abbatta automaticamente la connessione logica con la centrale (si spegne il Led PPP, a indicare che il router non è connesso alla centrale).

Pur essendo, a prima vista, una buona soluzione, bisogna tenere in considerazione alcuni aspetti:
1- Per riattivare la connessione è sufficiente che un PC effettui una richiesta dati verso Internet. Una volta rilevata questa richiesta, il router ADSL effettua in automatico una nuova connessione a Internet.
2- Alcuni programmi recenti, sviluppati in seguito all'avvento delle connessioni a banda larga, effettuano degli aggiornamenti periodici automatici su Internet. È questo il caso, ad esempio, degli antivirus, dei server DNS, di MSN Messenger e altri ancora.

A fronte di queste considerazioni è possibile che il router ADSL, se questi programmi non vengono configurati per ricercare gli aggiornamenti solo su richiesta dell'utente e non in automatico, possa collegarsi a Internet diverse volte per un periodo di tempo molto lungo, a insaputa dell'utente.

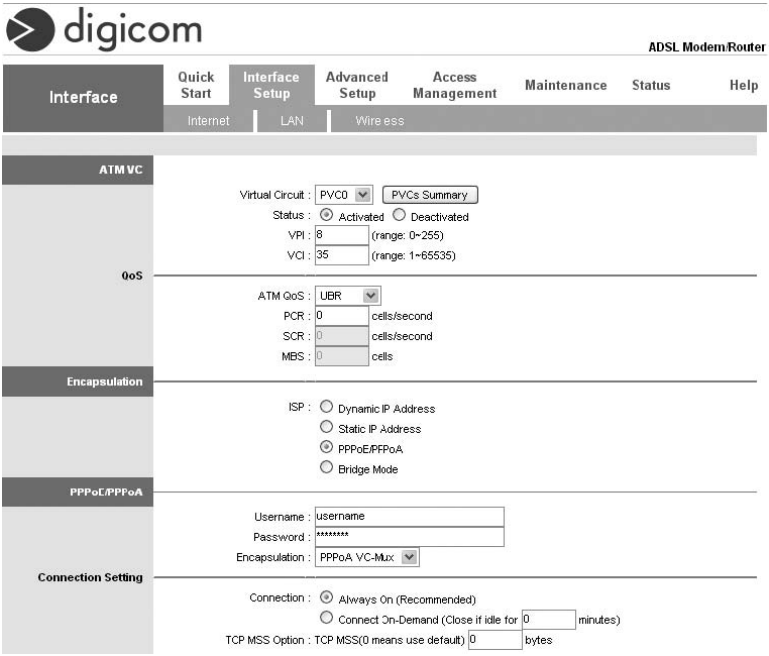
**È per questi motivi che tutte le case produttrici di router ADSL consigliano di spegnere il router ADSL quando non è necessario l'utilizzo di Internet.**

## 5.4. CONFIGURAZIONE CON ABBONAMENTI SMART (UN SOLO INDIRIZZO IP PUBBLICO)

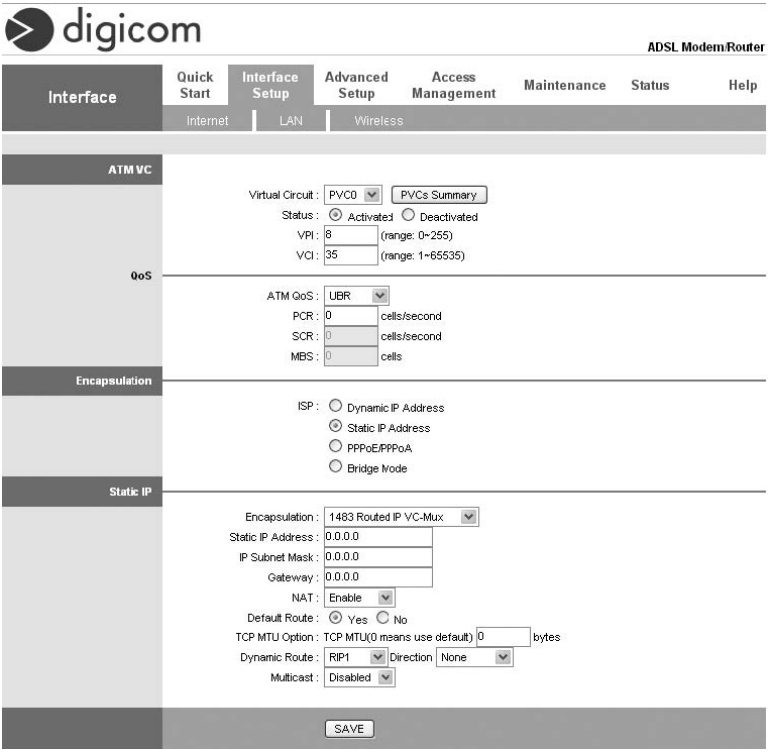
Questa tipologia di abbonamento ADSL prevede l'assegnazione di un indirizzo IP pubblico da parte del provider. I parametri ADSL necessari per la configurazione sono:

- Protocollo di linea (generalmente RFC 1483 Routed IP LLC)
- VPI
- VCI
- Indirizzo IP pubblico assegnato (ad esempio 80.105.91.253)
- Subnet Mask (ad esempio 255.255.255.0)
- Gateway predefinito (ad esempio 80.105.91.254)

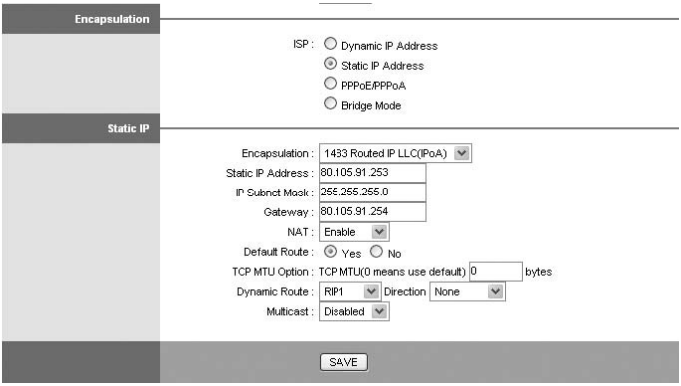
- Accedete, tramite un browser Internet (tipo Internet Explorer), al menù di configurazione di Michelangelo Wave 300 puntando sull'indirizzo IP di LAN attualmente impostato (nelle impostazioni di fabbrica Michelangelo Wave 300 è raggiungibile all'indirizzo 192.168.1.254).
- Selezionate il menù Interface **Setup > Internet**.




- Nelle impostazioni di fabbrica Michelangelo Wave 300 è preconfigurato per abbonamenti con protocollo PPPoA/PPPoE. Nel campo **ISP** della sezione **Encapsulation** selezionate la voce **Static IP Address**. Il menù di configurazione verrà modificato in automatico mostrando la seguente finestra:




- Inserite i parametri del vostro abbonamento ADSL, come nell'esempio:




- Premete il pulsante "**SAVE**" per rendere effettive le nuove impostazioni.
  **La configurazione di Michelangelo Wave 300 con i parametri della vostra linea ADSL è terminata.**

## 5.5. CONFIGURAZIONE CON ABBONAMENTI MULTI-UTENTE (INDIRIZZI IP PUBBLICI AGGIUNTIVI)

In questo esempio Michelangelo Wave 300 verrà configurato facendo riferimento ai parametri del contratto sotto riportato:

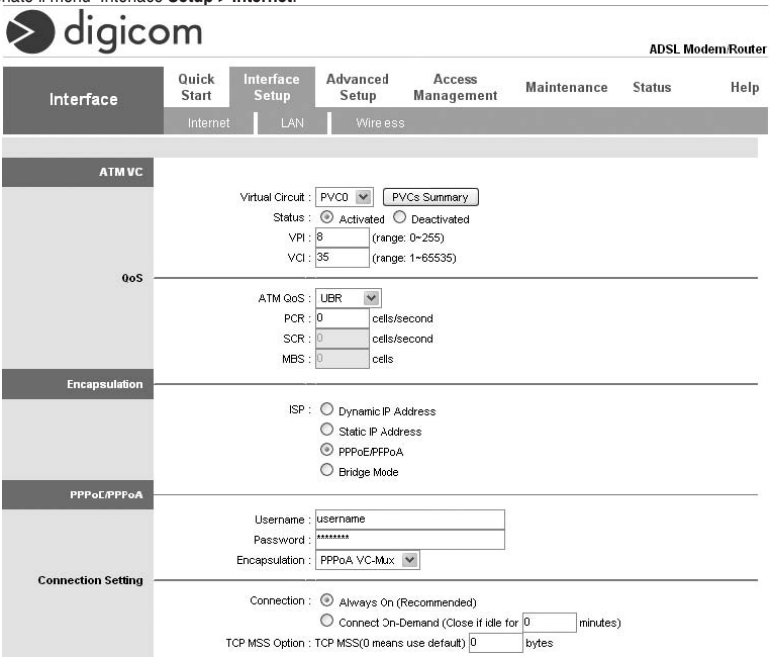
| **Tipo di contratto:** | **INTERBUSINESS: EASYNET** | | |
|---|---|---|---|
| Indirizzi IP assegnati | 80.105.107.208-215 | Network Mask | 255.255.255.248 |
| Default Gateway | 80.105.107.209 | | |
| Punto Punto | 80.105.91.254 | Network Mask | 255.255.255.252 |
| VpVc | 8/35 | | |

Con questo esempio di contratto vengono assegnati 8 IP all'utente (da 208 a 215), così suddivisi:

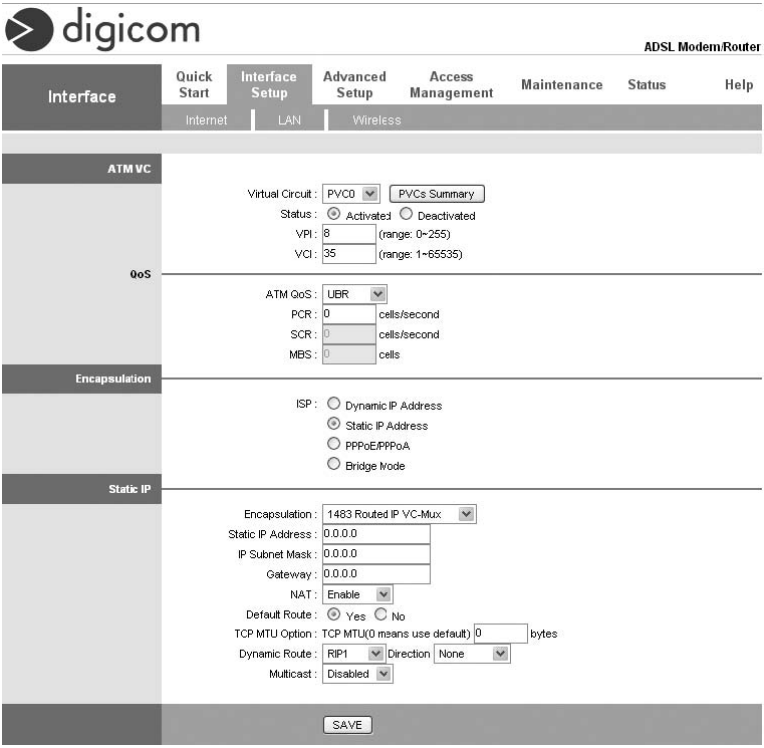
| **IP** | **Mask** | **Notes ...** |
|---|---|---|
| 80.105.107.208 | 255.255.255.248 | Subnet Address |
| 80.105.107.209 | 255.255.255.248 | Michelangelo Wave 300 |
| 80.105.107.210 | 255.255.255.248 | Computer |
| 80.105.107.211 | 255.255.255.248 | Computer |
| 80.105.107.212 | 255.255.255.248 | Computer |
| 80.105.107.213 | 255.255.255.248 | Computer |
| 80.105.107.214 | 255.255.255.248 | Computer |
| 80.105.107.215 | 255.255.255.248 | Broadcast Address |

**Se non vi venissero forniti i valori relativi al Default Gateway e alla Subnet Mask per la parte WAN (Punto-punto), vi consigliamo di utilizzare l'indirizzo precedente al Punto-punto come Gateway e 255.255.255.252 come Subnet Mask.**

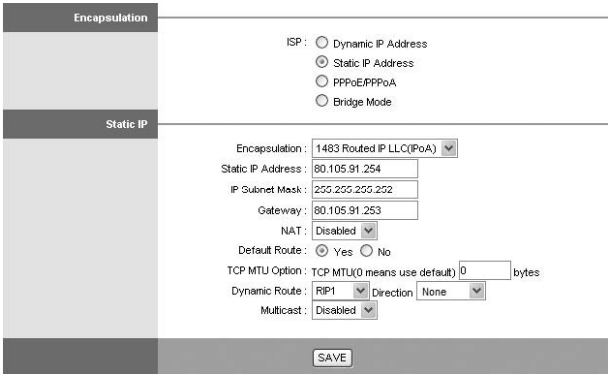
- Accedete, tramite un browser Internet (tipo Internet Explorer), al menù di configurazione di Michelangelo Wave 300 puntando sull'indirizzo IP di LAN attualmente impostato (nelle impostazioni di fabbrica Michelangelo Wave 300 è raggiungibile all'indirizzo 192.168.1.254).
- Selezionate il menù Interface **Setup > Internet**.



- Nelle impostazioni di fabbrica Michelangelo Wave 300 è preconfigurato per abbonamenti con protocollo PPPoA/PPPoE. Nel campo **ISP** della sezione **Encapsulation** selezionate la voce **Static IP Address**. Il menù di configurazione verrà modificato in automatico mostrando la seguente finestra:

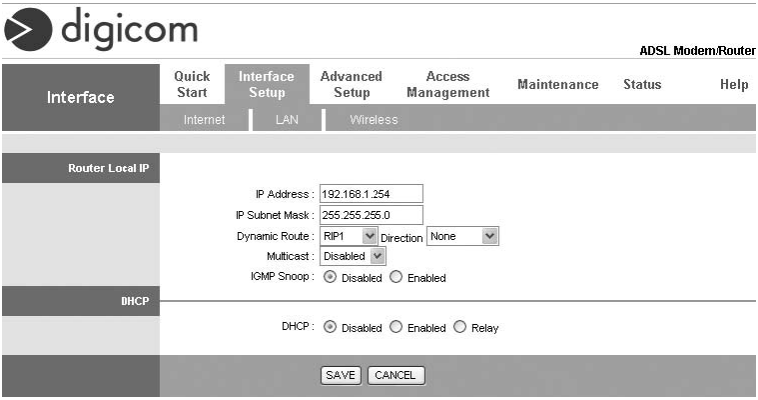



- Inserite i parametri del vostro abbonamento ADSL, come nell'esempio:

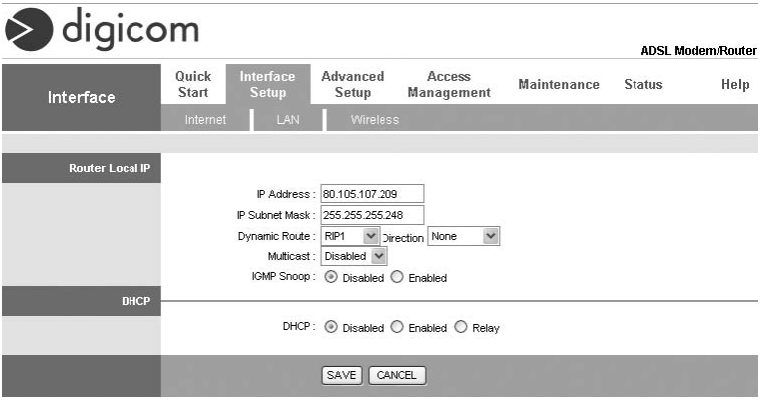



- Cliccate il pulsante "**SAVE**" per rendere effettive le nuove impostazioni. In questo modo avete configurato la sezione WAN di Michelangelo Wave 300 con l'indirizzo IP Punto-punto fornito dal provider. Per utilizzare gli IP pubblici aggiuntivi forniti è ora necessario impostare l'indirizzo del Default Gateway indicato sul contratto nella sezione di LAN di Michelangelo Wave 300.

- Entrate nel menù **Interface Setup > LAN**.

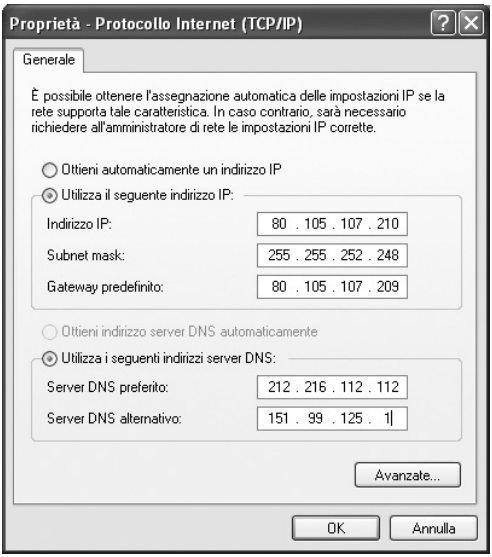



- Impostate il campo **DHCP*** su Disabled e inserite nei campi **IP Address e IP Subnet Mask** i parametri indicati nel contratto. Nell'esempio:




- A questo punto è necessario modificare l'indirizzo IP della scheda di rete del PC. Dovete impostare la scheda di rete del vostro PC con un indirizzo IP pubblico facente parte del pool assegnatovi sul contratto. Effettuate le impostazioni sulla scheda di rete come da figura e premete **OK**.

*** Fate riferimento al capitolo 4 relativo alle "Impostazioni di Sicurezza".**




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

**IP:** uno degli IP pubblici aggiuntivi liberi
**Subnet Mask:** la Subnet associata ai vostri indirizzi pubblici
**Gateway:** l'indirizzo pubblico assegnato al router (esempio 80.105.107.209)
**DNS:** gli indirizzi dei DNS forniti dal provider

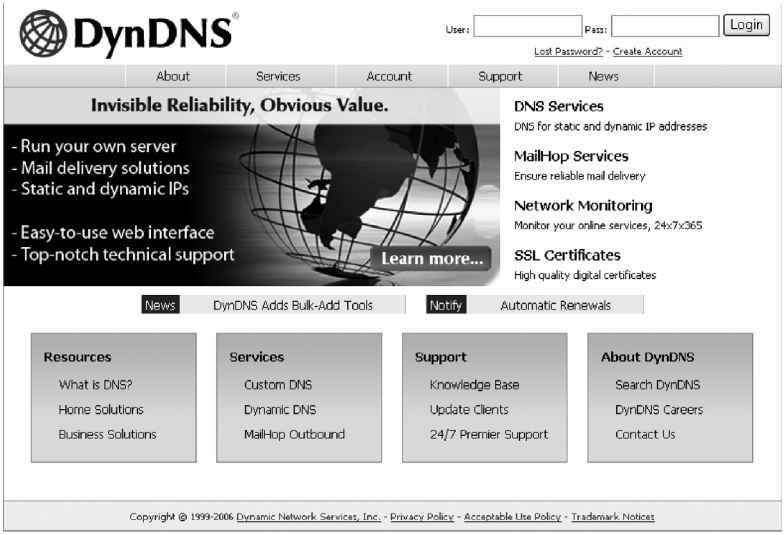
- Una volta configurata la scheda di rete del PC, avviate il browser (ad esempio Internet Explorer) per verificare che il PC navighi correttamente su Internet.

## 5.6. CREAZIONE ACCOUNT DDNS

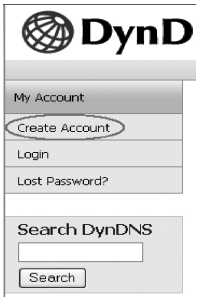
DDNS, è un servizio offerto da diversi operatori che permette ad utenti che dispongono di un abbonamento ADSL con indirizzi IP dinamici, di essere sempre raggiungibili ad un determinato indirizzo URL, indipendentemente dall'indirizzo IP pubblico momentaneamente assegnato dal provider al router ADSL.

In questa procedura verranno spiegate le fasi necessarie per la creazione e l'abilitazione di un nuovo account dyndns.org e la successiva configurazione del Michelangelo Wave 300.

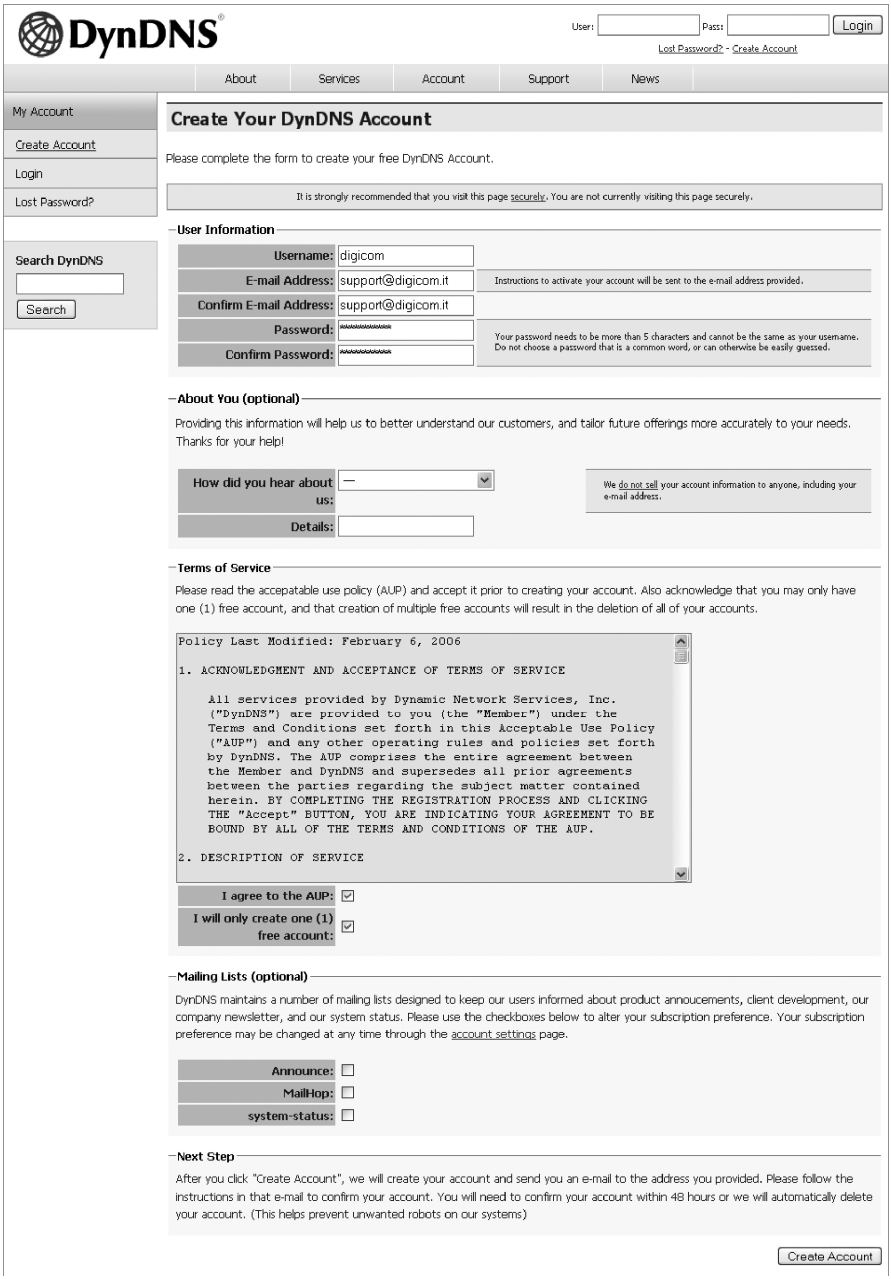
- Da browser accedete all'indirizzo **www.dyndns.com**



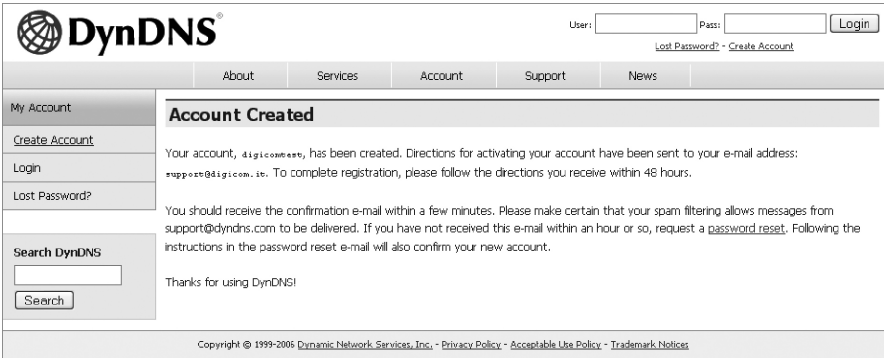

- Per creare un nuovo account, cliccate sulla voce **Account** e nella finestra successiva cliccate sulla voce **Create Account**.



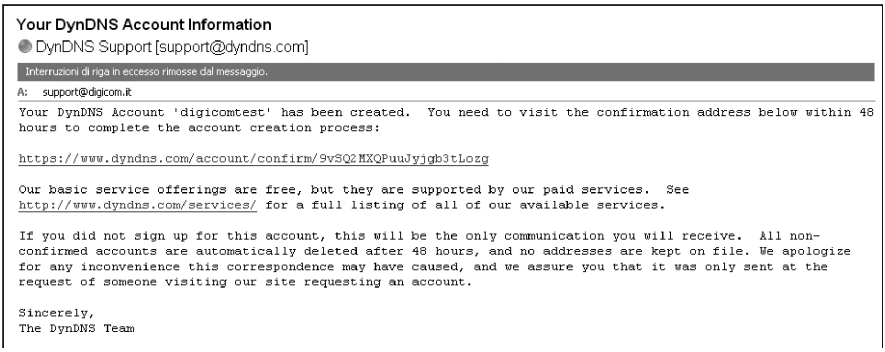

- Nella pagina successiva compilate tutti i campi obbligatori richiesti.



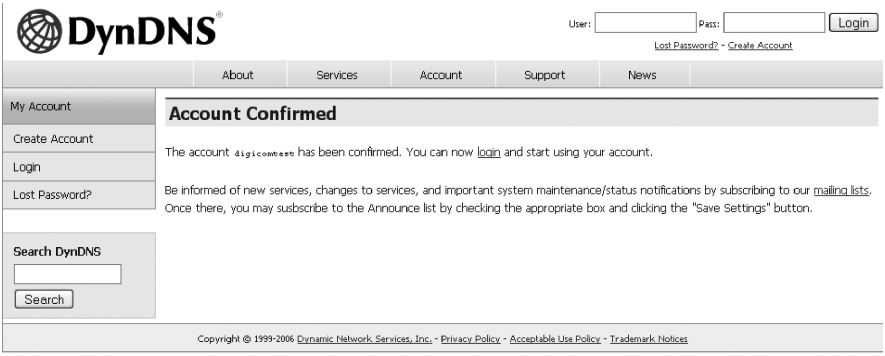

- Un messaggio di **Account Created** vi indicherà il buon fine della procedura.




- Una volta creato l'account, prima di poterlo utilizzare sarà necessario attivarlo.
  All'indirizzo e-mail che avete inserito precedentemente nel campo **E.mail Address** verrà recapitata una e-mail contenente un link per l'attivazione del vostro nuovo account DDNS.




- Cliccate sul primo link indicato nella e-mail per attivare l'account DDNS.




- Una volta attivato l'account sarà possibile configurare il Michelangelo Wave 300. Entrate nel menù di configurazione del firewall nella sezione **Access Management -> DNS** e configurate i campi secondo i parametri del vostro account e premete il pulsante **Save**.


- **Il router è ora configurato per il servizio DDNS e sarà sempre raggiungibile all'esterno, nell'esempio all'indirizzo digicom.dyndns.org**

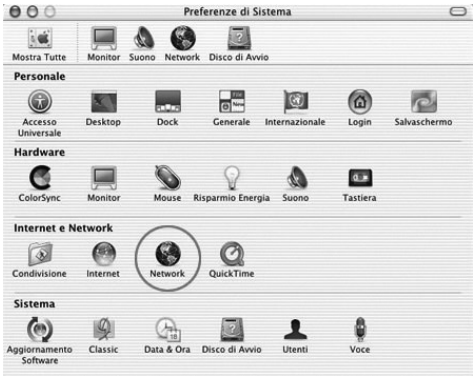
# A. CONFIGURAZIONE INDIRIZZO IP

## A.1. CONFIGURAZIONE AUTOMATICA IMPOSTAZIONI DI RETE (CLIENT DHCP)

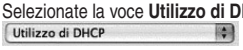
### Mac OS X

- Dal **Pannello di Controllo** selezionate la voce **Preferenze di sistema**.


- Cliccate sull'icona **Network**.




- Selezionate **Mostra: Ethernet Integrata**.
- Cliccate sul pulsante **TCP/IP**.
- Selezionate la voce **Utilizzo di DHCP**.

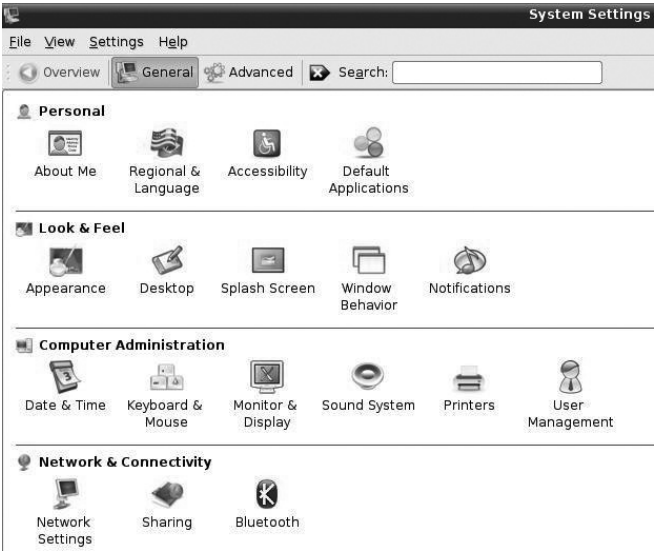



- Chiudete il pannello **Network**.

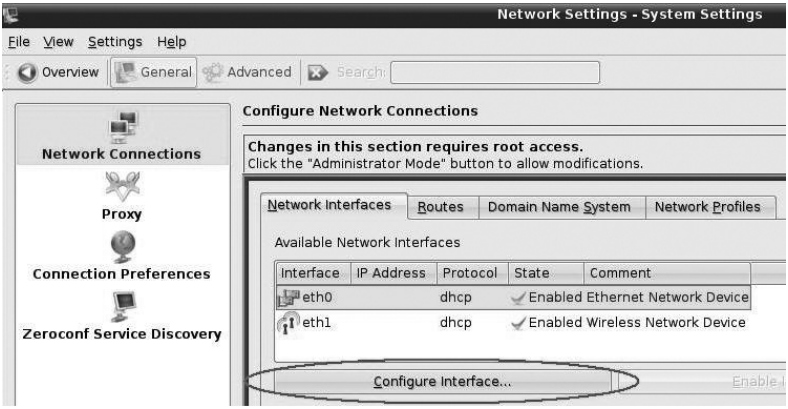
## Linux - Centro di Controllo KDE

Di seguito verranno date alcune informazioni sulla configurazione delle risorse di rete utilizzando il Centro di Controllo KDE con la distribuzione Kubuntu 6.10.

- Attivate il menù **System Settings**
- Selezionate **Network Settings** nel menù **Network & Connectivity**




- Evidenziate l'interfaccia Eth0 relativo alla scheda di rete Ethernet e premete il pulsante **Configure Interface**.




- Selezionate **Automatic**: nella modalità **DHCP** nel menù **TCP/IP Address**.


- Confermate premendo il pulsante **OK**.

## Linux - Desktop Environment Gnome

Di seguito verranno date alcune informazioni su come configurare le risorse di rete utilizzando il Desktop Environment Gnome con la distribuzione Ubuntu 6.10.

- Selezionate il menù **Rete** disponibile da **Sistema> Amministrazione**


- Selezionate la **Connessione via cavo** e premete il pulsante **Proprietà**:


- Impostate la voce **Configurazione**: nella modalità **Configurazione Automatica (DHCP)**

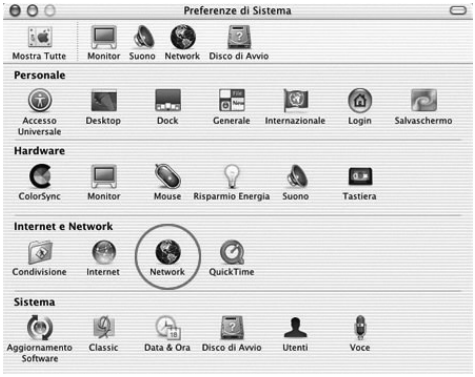

- Confermate con il pulsante **OK**.

## A.2. CONFIGURAZIONE MANUALE IMPOSTAZIONI DI RETE (INDIRIZZI IP STATICI)

### Mac OS X

- Dal **Pannello di Controllo** selezionate la voce **Preferenze di sistema**.


- Cliccate sull'icona **Network**.

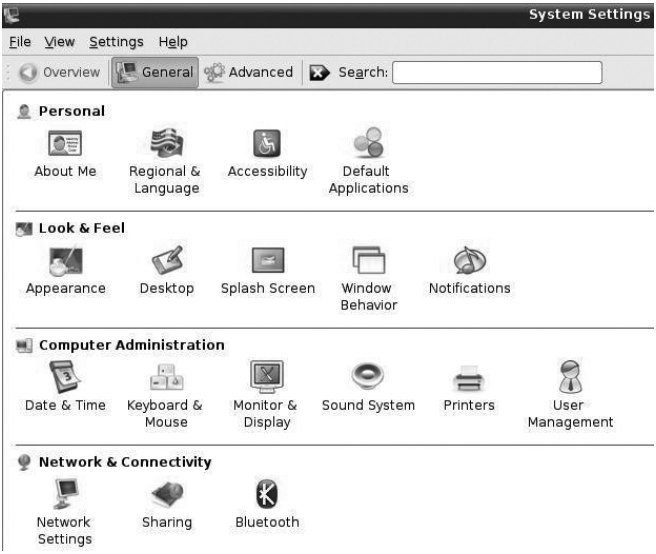



- Selezionate **Mostra: Ethernet Integrata**.
- Cliccate sul pulsante **TCP/IP**.
- Selezionate la voce **Manualmente**.
- Inserite i valori per **IP 192.168.1.2**, Maschera di sottorete (Subnet Mask) **255.255.255.0** e Router **192.168.1.254**
- Chiudete il pannello **Network**.

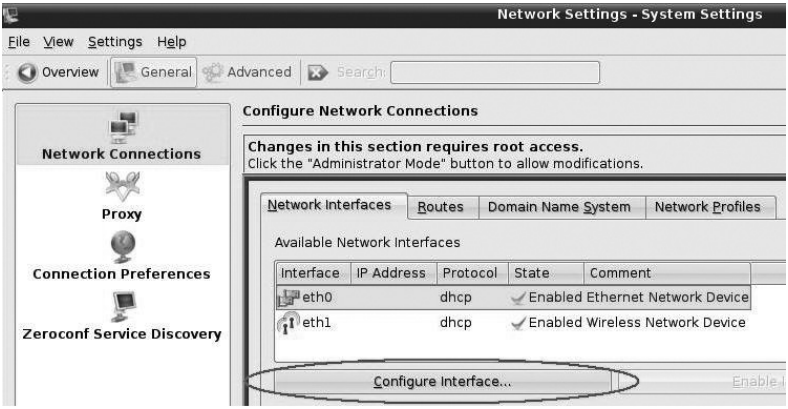
## Linux - Centro di Controllo KDE (Indirizzi IP statici)

Di seguito verranno date alcune informazioni sulla configurazione delle risorse di rete utilizzando il Centro di Controllo KDE con la distribuzione Kubuntu 6.10.

- Attivate il menù **System Settings**
- Selezionate **Network Settings** nel menù **Network & Connectivity**

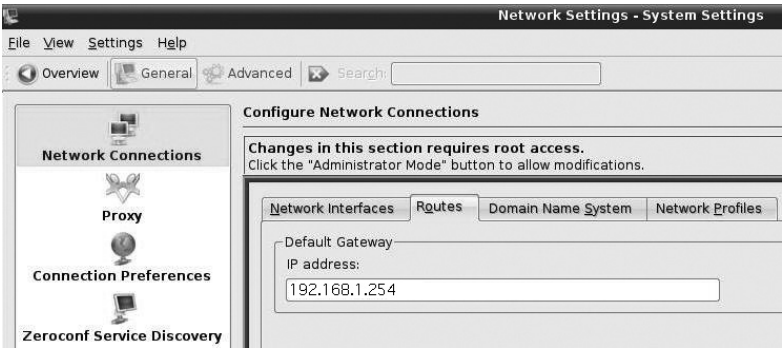



- Evidenziate l'interfaccia Eth0 relativo alla scheda di rete e premete il pulsante **Configure Interface**.

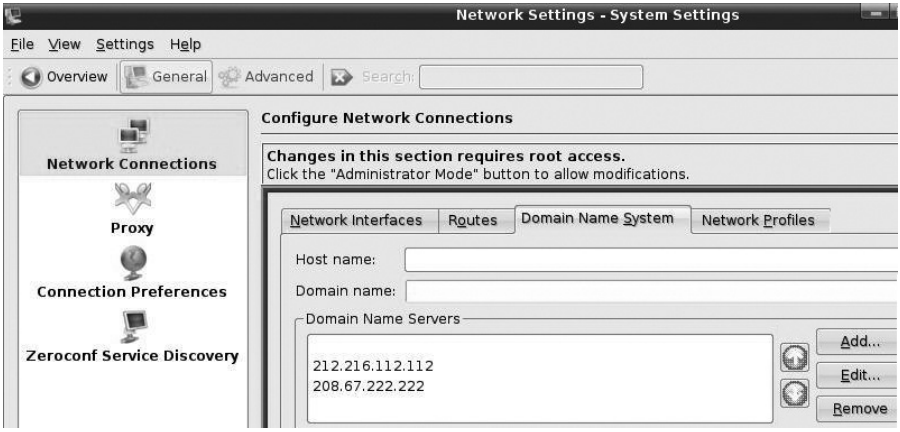



- Selezionate **Manual**: compilate i campi **IP Address** e **Netmask** come indicato nell'esempio:


- Confermate premendo il pulsante **OK**.
- Selezionate il menù a tendina **Routes** e inserite l'indirizzo IP del Default Gateway (indirizzo IP di LAN del router ADSL) come da immagine:




- Selezionate il menù a tendina **Domain Name System**, premete il pulsante **Add** e inserite l'indirizzo IP del DNS fornito dal vostro provider ADSL:



## Linux - Desktop Environment Gnome (Indirizzi IP statici)

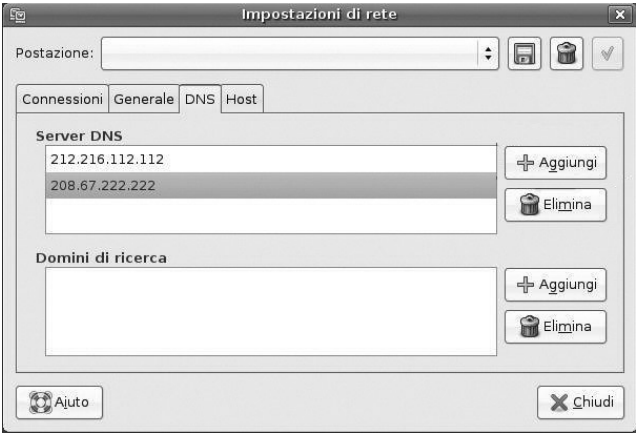
Di seguito verranno date alcune informazioni sulla configurazione delle risorse di rete utilizzando il Desktop Environment Gnome con la distribuzione Ubuntu 6.10.

- Selezionate il menù **Rete** disponibile da **Sistema > Amministrazione**


- Selezionate la **Connessione via cavo** e premete il pulsante **Proprietà**:

- Impostate la voce **Configurazione** nella modalità **Indirizzo IP statico** e compilate i campi **Indirizzo IP, Maschera di rete e indirizzo del Gateway** come da immagine:


- Confermate con il pulsante **OK**.
- Selezionate il menù a tendina **DNS**, premete il pulsante **Aggiungi** nella finestra relativa ai Server DNS e inserite gli indirizzi IP dei server DNS forniti dal vostro provider ADSL.



Italy 21010 Cardano al Campo VA
via Alessandro Volta 39
**http://www.digicom.it**