



MANUALE

**EM4206/EM4207 - ADSL2/2+ modem**

[WWW.EMINENT-ONLINE.COM](http://WWW.EMINENT-ONLINE.COM)

## EM4206/EM4207 - ADSL2/2+ modem



### Attenzione

L'apertura del prodotto a scopo di riparazione è sconsigliata! La riparazione dei prodotti deve essere effettuata esclusivamente dallo staff Eminent!

## Contenuti

1.0 Condizioni di garanzia .....	2
2.0 Introduzione.....	3
2.1 Funzioni e specifiche .....	3
2.2 Contenuto della confezione .....	3
2.2 Indicatori LED del Router - spiegazione.....	3
3.0 Configurazione guidata tramite Wizard .....	4
4.0 Configurazione manuale.....	4
4.1 Connessione del Modem/Router.....	4
4.2 Configurazione manuale del router per Internet .....	4
4.2.1 Configurazione per provider PPP.....	5
4.2.2 Configurazione di provider 1483 Bridged .....	5
4.2.3 Configurazione di altri providers.....	5
5.0 Configurazione avanzata / firewall .....	6
5.1 Configurazione dell'orologio (SNTP).....	6
5.2 Port forwarding (firewall).....	6
5.3 Filtri IP .....	6
5.4 LAN Clients .....	7
5.5 Filtri Bridge .....	7
5.6 Routing Statico .....	7
5.7 Routing Dinamico .....	7
6.0 Service and Support .....	7

*On page 8 you will find the Eminent Advanced Manual for networking settings and information about home networking. (English only)*

## 1.0 Condizioni di garanzia

I 5 anni di garanzia Eminent viene applicata a tutti i prodotti a meno che non diversamente disposto all'atto dell'acquisto. Se il prodotto viene acquistato di seconda mano il periodo di garanzia parte dal momento dell'acquisto del primo possessore. La garanzia Eminent viene applicata a tutti i prodotti Eminent e alle parti che lo compongono. Alimentatori, batterie, antenne e altri prodotti non integrati o connessi direttamente al prodotto e/o ai prodotti principali dei quali, senza dubbio ragionevole, possa essere assunto che hanno una funzione diversa da quello principale non sono coperti dalla garanzia Eminent. I prodotti Eminent non sono coperti da garanzia

qualora vengano esposti ad utilizzo improprio o non corretto. La garanzia Eminent decade qualora i prodotti vengano aperti o ne venga tentata la riparazione da personale non autorizzato Eminent.

## 2.0 Introduzione

Congratulazioni per l'acquisto per uno dei prodotti ad alta qualità Eminent!

Questo prodotto è stato sottoposto a test aggiuntivi degli esperti Eminent.

Qualora vi fossero problemi di natura tecnica il prodotto Eminent è coperto da 5 anni di garanzia Eminent. Vi preghiamo di mantenere questo manuale e lo scontrino relativo all'acquisto in un luogo sicuro.

*Registri ora il prodotto sul sito [www.eminent-online.com](http://www.eminent-online.com) e riceverà gli aggiornamenti sul prodotto!*

### 2.1 Funzioni e specifiche

Con il prodotto Eminent ADSL2/2+ Modem ci si può connettere ad Internet e creare, utilizzando un solo prodotto, in modo rapido e facile una rete LAN. L'EM4206 è per linee telefoniche analogiche (RJ12) mentre l'EM4207 è per linee ISDN (RJ45)

### 2.2 Contenuto della confezione

Le seguenti parti devono essere presenti nella confezione:

- Il Router EM4206 ADSL modem/router analogico oppure l' EM4207 ADSL modem/router ISDN.
- Alimentatore.
- 01 Cavo UTP.
- 01 Cavo telefonico.
- 01 CD contenente il manuale ed il software di configurazione.

### 2.2 Indicatori LED del Router - spiegazione

<b>PWR</b>	<i>Si illumina quando il router è acceso.</i>
<b>PPP</b>	<i>Si illumina quando una si stabilisce una connessione PPP (Qualora ci si connetta ad un provider che utilizzi PPPoA o PPPoE).</i>
<b>LAN 1,2,3 and 4</b>	<i>Si illuminano quando un PC/Device viene connesso allo switch del router. I LED lampeggiano quando c'è del traffico di rete.</i>
<b>ADSL</b>	<i>Si illumina quando viene trovato un segnale ADSL sulla linea telefonica.  Può impiegare sino a 60 secondi prima che il LED si illumini ed il segnale ADSL venga trovato. Se il LED ADSL rimane spento, si prega di contattare il provider.</i>

*Se il LED lampeggia di continuo è necessario controllare che il filtro ADSL sia presente.*

## 3.0 Configurazione guidata tramite Wizard

La via più semplice per configurare il router è quella di utilizzare il software di configurazione guidata presente nel CD come spiegato di seguito. Se non si vuole utilizzare il software Wizard è possibile configurare il dispositivo manualmente.

1. Accendere il Computer.
2. Inserire il CD-ROM nel lettore del PC.
3. IL software Wizard partirà automaticamente..
4. Seguite le istruzioni che appariranno sul video sino a quando l'installazione non sarà terminata. A questo punto sarà possibile navigare.

*Se non si vuole utilizzare la configurazione automatica è possibile configurare il dispositivo manualmente come si vedrà nel capitolo 4.1.*

## 4.0 Configurazione manuale

Se si vuole configurare il router manualmente è necessario che il browser Internet sia configurato correttamente così come devono esserlo i parametri di rete. Se non si è certi fare riferimento al manuale avanzato presente nel CD-ROM.

### 4.1 Connessione del Modem/Router

1. Spegnerne il Computer.
2. Connettere il router alla presa elettrica utilizzando l'alimentatore presente nella confezione.
3. Connettere il cavo telefonico alla porta DSL del router e l'altro capo alla presa al filtro ADSL (non incluso in quanto di norma fornito dal provider).
4. Connettere il cavo LAN ad una delle 4 porte del router
5. Connettere l'altro capo alla porta di rete del computer.

### 4.2 Configurazione manuale del router per Internet

Per essere in grado di configurare il router è necessario, per prima cosa, connettere il router al PC. Seguire poi le seguenti istruzioni per connettere il router ad Internet:

1. Aprite il vostro browser (Internet Explorer, Firefox, Netscape, Safari).
2. Digitare nella barra degli indirizzi: <http://192.168.1.1>
3. Premere invio oppure vai a.
4. Digitare la username: Admin.
5. Digitare la password: Admin.
6. Premere 'Ok'.

7. Si accederà al menu di configurazione.

#### **4.2.1 Configurazione per provider PPP**

1. Clickare su 'Wizard' presente nel menu sulla sinistra
2. Clickare su 'Country'.
3. Selezionare la vostra nazione (esempio: Italia).
4. Clickare su 'ISP'.
5. Selezionare il vostro provider (e.g. 'Telecom Alice').
6. Clickare su 'Next' per continuare
7. Digita il tuo username e password relative al suo contratto ADSL nel menu 'Set PPP Password'.
8. Clickare 'Apply' per salvare i settaggi e far ripartire il router.

*Attenzione! Il restart del router può richiedere anche un minuto! Quando il router è ripartito avrete stabilito la connessione Internet.*

#### **4.2.2 Configurazione di provider 1483 Bridged**

1. Clickare su 'Wizard' presente nel menu sulla sinistra
2. Clickare su 'Country'.
3. Selezionare la vostra nazione (esempio: Italia).
4. Clickare su 'ISP'.
5. Selezionare il vostro provider (e.g. 'BabyXL').
6. Selezionare l'opzione 'DHCP' al menu 'Connection Type'.
7. Clickare su 'Next' per continuare
8. Clickare 'Apply' per salvare i settaggi e far ripartire il router.

*Attenzione! Il restart del router può richiedere anche un minuto! Quando il router è ripartito avrete stabilito la connessione Internet.*

#### **4.2.3 Configurazione di altri providers**

1. Clickare su 'Config'.
2. Clickare su 'New Connection'.
3. Inserire i parametri forniti dal provider.
4. Clickare 'Apply' per applicare i settaggi.
5. Clickare 'Save All' (colonna di sinistra) per salvarli
6. Clickare 'Save' (in basso a destra) per far ripartire il router.

*Attenzione! Il restart del router può richiedere anche un minuto! Quando il router è ripartito avrete stabilito la connessione Internet.*

## 5.0 Configurazione avanzata / firewall

Il Menu 'Advanced' permette di configurare in modo avanzato il router. Queste configurazioni necessitano di conoscenze avanzate di computer networking, sono quindi da sconsigliarsi agli utenti inesperti.

### 5.1 Configurazione dell'orologio (SNTP)

L'orologio integrato nel router può essere sincronizzato con Internet:

1. Clickare 'Advanced'.
2. Clickare 'SNTP'.
3. Abilitare 'Enable SNTP'.
4. Inserite l'indirizzo IP del "Time server" Enter the IP-address (e.g. '212.204.235.152').

Una lista completa di server è disponibile su:  
<http://ntp.isc.org/bin.view/Servers/WebHome>

### 5.2 Port forwarding (firewall)

Questo dispositivo ha un firewall integrato. Questo significa che tutto il traffico esterno non specificamente richiesto non verrà fatto passare verso o i PC connessi. Tutto il traffico normale richiesto dagli user verrà processato regolarmente verso i PC connessi al router.

I programmi che non prevedono la presenza di un firewall potrebbero non funzionare senza specifiche configurazioni.

Altre applicazioni prevedono di configurare il firewall come ad esempio E-Donkey and VNC.

Se si vuole utilizzare questo tipo di programmi è necessario per prima cosa ottenere il vostro indirizzo IP locale.

Attraverso il menu 'LAN clients' del modem router è possibile configurare i parametri necessari. Clickare 'Apply' per confermare.

Clickare 'Save Setting and Reboot' per salvare i settaggi. Clickando su 'Custom rule' è possibile creare delle regole proprie'.

### 5.3 Filtri IP

Questa opzione svolge una funzione opposta alla precedente. Con l'applicazione delle regole è possibile bloccare il traffico proveniente da certi computer'.

Questa opzione permette di bloccare richieste internet basate su indirizzi IP e numeri di porte.

## 5.4 LAN Clients

Il modem router aggiunge automaticamente i computer che richiedono un indirizzo IP presente nella lista. Questo permette di selezionarli poi nel menu del 'Port Forwarding' e 'IP Filter' menus. Quando si usa un PC con indirizzo IP fisso è necessario aggiungere questo indirizzo alla lista di 'LAN-client'. E' possibile farlo semplicemente aggiungendo il nome dell'host (nome PC) ed il relativo indirizzo IP. L'indirizzo MAC-address non è richiesto.

## 5.5 Filtri Bridge

Questo menu permette di bloccare certe tipologie di traffico dati basandosi sugli indirizzi MAC. Questa opzione è disabilitata di default.

Opzione da non utilizzare se non si è utenti esperti.

## 5.6 Routing Statico

Questo menu permette di editare una tabella di routing e di assegnare un gateway per specifici host o destinazioni.

## 5.7 Routing Dinamico

Con l'abilitazione del routing dinamico, il modem router sarà reattivo ai messaggi RIP V1 or V2. Questa tecnologia dà al modem la possibilità di trovare la via più breve per raggiungere un host o una sottorete.

**Attenzione! Il routing Dinamico è da abilitarsi solo se si è certi che il provider supporti tale opzione.**

# 6.0 Service and Support

Questo manuale è stato scritto da esperti tecnici della Eminent. Se ci fossero problemi di installazione o di utilizzo del prodotto vi preghiamo di contattare [support@eminent-online.com](mailto:support@eminent-online.com) (*English only*).

# Eminent Advanced Manual

## Table of contents

- Table of contents.....8
- Why an Eminent advanced manual? .....9
- Your tips and suggestions in the Eminent Advanced Manual?.....9
- Service and support .....9
- Networking settings for Windows 98 and Windows ME.....9
- Networking settings for Windows 2000 and Windows XP ..... 10
- Networking settings for Windows Vista..... 11
- Configuring Internet Explorer 5 and 5.5..... 11
- Configuring Internet Explorer 6.....12
- Configuring Internet Explorer 7.....12
- DHCP, Automatic allocation of IP addresses.....13
- Translating IP addresses and domain names .....13
- Using a single IP address for your entire network ..... 13
- Security for your computer and your network..... 14
- Making a computer available for Internet users in your network..... 14
- Simplifying network management.....15
- Blocking websites with explicit content .....15
- Checking data traffic at package level .....15
- Blocking a complete domain.....16
- Carrying out actions based on date or time..... 16
- A safe remote connection.....16
- Remote network management.....16
- Allocating or blocking network access .....16
- Making your wireless network secure .....17
- Expanding the range of your wireless network.....17
- Index ..... 19



## Why an Eminent advanced manual?

Eminent has developed the Eminent Advanced Manual especially for your ease of use. The Eminent Advanced Manual enables you to discover the advanced possibilities of your house network. The Eminent Advanced Manual will for example, help you setting up your firewall so your own network is optimally protected at all times. Of course, extensive consideration is also given to the protection of your wireless network.

The Eminent Advanced Manual is a wealth of information and a handy reference source. This will enable you to have access to functions previously only available to professional and highly advanced users.

## Your tips and suggestions in the Eminent Advanced Manual?

The Eminent Advanced Manual was created in cooperation with a number of satisfied Eminent users. If you would like a certain option to be included in the Eminent Advanced Manual or you have suggestions or tips regarding the Eminent Advanced Manual, you can contact [communications@eminent-online.com](mailto:communications@eminent-online.com). Your tips and suggestions will be collected and processed in the new edition of the Eminent Advanced Manual.

## Service and support

The Eminent Advanced Manual was carefully written by users and technical experts from Eminent. If you have problems installing or using the product, please contact [support@eminent-online.com](mailto:support@eminent-online.com).

## Networking settings for Windows 98 and Windows ME

1. Windows 98: Right-click 'Network neighbourhood' on your desktop.
2. Windows ME: Right-click 'My network places' on your desktop.
3. Choose 'Properties'.
4. Select 'TCP/IP'.
5. Click 'Properties'.
6. Select 'Obtain an IP Address automatically'.
7. Click the 'WINS configuration' tab.
8. Select 'Disable WINS resolution'.
9. Click the 'DNS configuration' tab.
10. Click 'Disable DNS'.

11. Click the 'Gateway' tab.
12. Remove previously installed gateways.
13. Click 'Ok'.
14. Click 'Ok' in the 'Network' window.
15. Restart your computer.
16. Click 'Start'.
17. Click 'Run'.
18. Type 'Winipcfg'.
19. Click 'Ok'.
20. Windows will show the 'IP configuration window'.
21. Select the Ethernet adapter (Networking PCI adapter) connected to the router.
22. Click 'Release all'.
23. Click 'Renew all'.
24. Click 'Ok'.

## Networking settings for Windows 2000 and Windows XP

1. Right-click 'My network places' on your desktop.
2. Choose 'Properties'.
3. Right-click 'Local area connection'.
4. Choose 'Properties'.
5. Select 'Internet protocol (TCP/IP)'.
6. Click 'Properties'.
7. Select 'Obtain an IP Address automatically'.
8. Select 'Obtain a DNS server address automatically'.
9. Click 'Ok'.
10. Windows will show the 'Local area connection properties' window.
11. Click 'Ok'.
12. Windows 2000: Close the 'Network and dial-up connections' window.
13. Windows XP: Close the 'Network connections' window.
14. Restart your computer.
15. Click 'Start'.
16. Click 'Run'.
17. Type 'cmd'.
18. Push enter on your keyboard.
19. Type 'ipconfig /release'.
20. Push enter on your keyboard.
21. Type 'ipconfig /renew'.
22. Push enter on your keyboard.
23. Type 'Exit'.
24. Push enter on your keyboard.

## Networking settings for Windows Vista

1. Click on the Windows Vista logo (start button).
2. Choose 'Configuration screen'.
3. Choose 'Show network status and –tasks'.
4. Choose 'Control network connections'.
5. Right-click on 'LAN-connection'.
6. Choose 'Connect'.
7. If windows asks for your permission: choose 'Continue'.
8. Windows Vista now connects your LAN-connection.
9. Right-click on 'LAN-connection'.
10. Choose 'Properties'.
11. If windows asks for your permission: choose 'Continue'.
12. Select 'Internet Protocol version 4 (TCP/IPv4)'.
13. Click on 'Properties'.
14. Choose 'Obtain IP Address automatically.'
15. Choose 'Obtain DNS Server address automatically'.
16. Click 'OK'.
17. Click 'Close'.
18. Windows Vista will now set-up your connection.

## Configuring Internet Explorer 5 and 5.5

1. Start Internet Explorer.
2. Click 'Stop'.
3. When asked to establish a connection, press 'Cancel'.
4. Click 'Extra'.
5. Click 'Internet options'.
6. Click the 'Connections' tab.
7. Click the 'LAN settings' tab.
8. Uncheck 'Find Explorer settings automatically'.
9. Uncheck 'Use configuration script'.
10. Uncheck 'Use proxy-server'.
11. Click 'OK'.
12. Remove dial-up connections by pressing 'Delete'.
13. Click 'Settings' to start the 'Internet' Wizard.
14. Select 'I would like to connect through a LAN network'.
15. Click 'Next'.
16. Check 'Automatically detect proxy-server'.
17. Click 'Next'.
18. Click 'No'.
19. Click 'Next'.
20. Click 'Complete'.
21. Close all Windows that are currently open.

22. Restart your PC.

## Configuring Internet Explorer 6

1. Start Internet Explorer.
2. Click 'Stop'.
3. When asked to establish a connection, press 'Cancel'.
4. Click 'Extra'.
5. Click 'Internet options'.
6. Click the 'Connections' tab.
7. Click the 'LAN settings' tab.
8. Uncheck 'Find Explorer settings automatically'.
9. Uncheck 'Use configuration script'.
10. Uncheck 'Use proxy-server'.
11. Click 'Ok'.
12. Remove dial-up connections by pressing 'Delete'.
13. Click 'Settings' to start the 'New connection' Wizard.
14. Click 'Next'.
15. Select 'Connect to the Internet'.
16. Click 'Next'.
17. Select 'I want to connect to the Internet manually'.
18. Click 'Next'.
19. Select 'Permanent broadband connection'.
20. Click 'Next'.
21. Click 'Complete'.
22. Close all Windows that are currently open.
23. Restart your PC.

## Configuring Internet Explorer 7

1. Start internet Explorer.
2. Click 'Stop'.
3. When asked to establish a connection, press 'Cancel'.
4. Click 'Extra'.
5. Click 'Internet options'.
6. Click the 'Connections' tab.
7. Click the 'LAN settings' tab.
8. Uncheck 'Find Explorer settings automatically'.
9. Uncheck 'Use configuration script'.
10. Uncheck 'Use proxy-server'.
11. Click 'Ok'.
12. Remove dial-up connections by clicking 'Delete'.
13. Click on 'Settings' (at the top).
14. Choose your type of connection.

15. Windows Vista will now set-up your connection.

## DHCP, Automatic allocation of IP addresses

For the development of DHCP (Dynamic Host Configuration Protocol), TCP/IP settings are configured manually on each TCP/IP client (such as your computer for example). This can be a difficult job if it is a big network or if something has to be changed regularly in the network. DHCP was developed to avoid always having to set up an IP address. With DHCP, IP addresses are allocated automatically when necessary and released when no longer required. A DHCP server has a series ('pool') of valid addresses that it can allocate to the client. When a client starts for example, it will send a message requesting an IP address. A DHCP server (there can be several in a network) responds by sending back an IP address and configuration details. The client will send a confirmation of receipt after which it can operate on the network.

## Translating IP addresses and domain names

IP addresses are far from user-friendly. Domain names are however easier to remember and use. The process of translating a domain name into an address that is understandable for a machine (such as your computer) is known as 'name resolution'. A 'Domain Name System' server carries out the afore-mentioned process. Thanks to DNS, you use domain names instead of IP addresses when visiting a website or sending e-mails.

Dynamic DNS or DDNS is a DNS-related option. You can still link your IP address to a domain name using DDNS if your provider works with dynamic IP addresses ('dynamic' here means that the IP addresses change frequently). After all, the IP address to which your domain name refers will also change when your provider changes your IP address. You must register with a Dynamic DNS provider such as [www.dyndns.org](http://www.dyndns.org) and [www.no-ip.com](http://www.no-ip.com) in order to use Dynamic DNS.

## Using a single IP address for your entire network

Network Address Translation (NAT) is an Internet standard with which a local network can use private IP addresses. Private IP addresses are those used within an own network. Private IP addresses are neither recognized nor used on the Internet. An IP address used on the Internet is also called a public IP address.

NAT enables you to share a single public IP address with several computers in your network. NAT ensures the computers in your network can use the Internet without any problems but users on the Internet will not have access to the computers in your

network. You will understand that NAT also offers a certain level of security partly due to the fact that private IP addresses are not visible on the Internet. Fortunately, most routers currently use NAT.

## Security for your computer and your network

A firewall can be a software- or a hardware solution placed, as it were, between the internal network and the outside world. Firewalls generally control incoming and outgoing data. Firewalls can be adjusted to stop or allow certain information from the Internet. Firewalls can also be adjusted to stop or allow requests from outside. Rules or policies are used to adjust firewalls. These state what a firewall must stop or allow and thus form a sort of filter.

Most routers have various firewall functions. The big advantage of a firewall in a router (hardware solution) is that an attack from outside is averted before reaching your network. If you wish to use a software firewall, you could for example, use the firewall built into Windows XP Service Pack 2. There are better alternatives such as the free ZoneAlarm and the commercial packages from Norman, Norton, Panda and McAfee. These commercial packages also offer protection against viruses if required.

## Making a computer available for Internet users in your network

The DMZ or DeMilitarized Zone is the zone between the outside world – the Internet – and the secure internal network. The computer placed within the DMZ is accessible via the Internet. This is in contrast to the computers that are outside the DMZ and are therefore secure. The DMZ is therefore also often used for servers that host websites. Websites must after all always be accessible via the Internet. A computer is also often placed within the DMZ if one plays a lot of online games. It is however advisable when you place a computer in the DMZ to fit a software firewall (such as the free ZoneAlarm). This is because the firewall opens all ports of the router for a computer within the DMZ. There is therefore no restriction on data transmission while this is however desirable in some situations.

Just like the DMZ function, Virtual Server enables you to make a computer, set up for example, as an FTP- or a web server, accessible from the Internet. You can state which ports in the firewall must be opened when using a Virtual Server. This is also the most important difference with the DMZ: when you place a computer in the DMZ, all ports are opened for the respective computer. If you use Virtual Server, you can open only the ports important for the respective computer.

Port Triggering or Special Apps is based on the same principle as Virtual Server. Port Triggering also enables you to make a computer within your network set up for example as an FTP- or webserver, accessible from the Internet. The ports you

allocate always remain open when you use Virtual Server. With Port Triggering however, the respective ports will only be opened if requested by the respective application.

## Simplifying network management

UPnP 'Universal Plug and Play': The name suggests that UpnP is very similar to the well-known – and notorious – 'Plug & Play'. Nothing is further from the truth. UPnP is completely different technology. The line of approach is that UPnP appliances must be able to communicate with one another via TCP/IP irrespective of the operating system, the programming language or the hardware. UPnP should make the user's life considerably easier.

As well as the products from a limited number of other manufacturers, most Eminent network manufacturers support UPnP. For more information on UPnP, visit: [www.upnp.org](http://www.upnp.org).

## Blocking websites with explicit content

Parental Control enables you to prevent one or more computers in your network from accessing the Internet. Parental Control often consists of several functions such as 'URL Blocking'. This function blocks websites by way of so-called 'keywords' or catchwords. Websites with explicit content are blocked in this way. URL Blocking is often combined with time and/or date blocks. Such blocks enable you to allow or block Internet access at certain times. You use 'rules' or 'policies' to set up your own schedule of blocks (see also 'Schedule Rule'). These rules describe exactly when and on what, a certain action, in this case, a block, must be applied.

## Checking data traffic at package level

The package filter (or 'Packet Inspection') is a programme that checks data packages while they are passing. The intelligent package filter checks the passing dataflow or business-specific definitions such as the IP- or user address, time and date, function and a number of other definitions. The package filter can best be imagined as a gatekeeper. The 'gatekeeper' screens the passers-by: 'Who are you and where are you going?' The passers-by whom the gatekeeper considers unsafe or unreliable are kept out.

You do not have to configure the package filter in most appliances. You only have the option of activating these. The use of this option is therefore also definitely recommended.

## Blocking a complete domain

A 'Domain Filter' will enable you to block an entire domain. A domain is a location on the Internet such as a website. A Domain Filter is therefore very similar to a 'URL Filter', apart from the fact that a Domain Filter blocks the entire domain. If, for example, you wish to protect your children from explicit content on a certain website, as well as blocking the website by way of catchwords (see: 'Parental Control'), you can block the entire website. You can do this using the Domain Filter.

## Carrying out actions based on date or time

You can configure when a certain option may be available using the 'Schedule Rule' function. Imagine you wish to make your 'Virtual Server' available at set times. You can use the Schedule Rule to stipulate when Internet users may approach your Virtual Server. It will then not be possible for Internet users to make a connection with your Virtual Server outside the period set. Schedule Rule is a handy option for automating certain access blocks.

## A safe remote connection

VPN (Virtual Private Networking) enables you to create a secure connection so you can, for example, use your business network while at home. A VPN connection is actually nothing more than a highly secure tunnel, which makes a connection with another computer or network via the Internet. Data sent via a VPN and received by third parties will still be unusable thanks to advanced encryption technology.

## Remote network management

The Simple Network Management Protocol (SNMP) is a control function enabling you to collect information from the router. The above-mentioned information consists of details on the number of computers connected to the router, their IP- and MAC addresses and the amount of data traffic processed when the information is requested. SNMP enables the system administrator to control the router remotely. This is often done using special applications supporting the SNMP protocol.

## Allocating or blocking network access

A MAC address is a unique code which each network product has. This code can often be found on a sticker on the product. You can also find the MAC address by clicking on 'Start', 'Execute'. Type 'CMD' and press 'Enter'. Then type 'ipconfig /all' and press 'Enter' again. The MAC address is shown under 'Physical Address'. A MAC address consists of six pairs each of two hexadecimal characters. For example, 00-0C-6E-85-03-82. MAC Address Control enables you to set up rules for MAC addresses and therefore to deny for example, certain network products access to your



network. When you use a wireless network, you can meanwhile use MAC Address Control to configure for example, your wireless network adapter to be able to connect to your network without the neighbouring network adapter being able to do so. MAC Address Control is a possibility, as well as WEP or WPA of providing extra security for your wireless network.

## Making your wireless network secure

WEP encryption is a form of security encoding the wireless signal from your wireless router or modem so the data cannot be simply intercepted by third parties. The security level is expressed in bits. 64-Bit WEP encryption is the lowest security level ranging up to 128-Bit for the highest level of security offered by WEP encryption: 256-Bit. You must enter a hexadecimal- or an ASCII series of characters in order to set up WEP encryption. Hexadecimal characters consist of the characters 'A' to 'F' and '0' to '9'. ASCII characters include all characters, including symbols. When you have selected the correct level of security and entered the key, you must also enter exactly the same key into all wireless appliances within the same network. Bear in mind that – when you activate the key in the first appliance – the connection with the network will be broken. You can re-establish the network by systematically providing all wireless appliance products with the same key.

WPA is a form of security encoding the wireless signal from your wireless router or modem so the data cannot be simply intercepted by third parties. WPA stands for 'Wi-Fi Protected Access' and is a big improvement on wireless security. WPA uses a 'Pre Shared Key (PSK)'. This is a key that must be put into operation on all appliances connected to the wireless network. This WPA key may not be any longer than 63 (random) characters and no shorter than 8 (random) characters. The best form of wireless protection is currently however formed by WPA2. The above-mentioned standard is only supported by a few manufacturers – including Eminent – and is therefore difficult to combine with other makes of wireless networks.

If you wish to use WPA or perhaps even WPA2, make sure that all appliances in your wireless network support this form of security. The combining of various types of security in a wireless network is not possible and will result in the loss of the connection.

## Expanding the range of your wireless network

WDS (Wireless Distribution System) or 'Bridging' is an option with which you can easily expand the range of your wireless network should the range of your wireless network remain limited. Appliances linked via WDS can share your Internet connection. You therefore do not need to interlink appliances sharing WDS by way of a physical connection (such as a cable). Appliances supporting WDS or Bridging

recognize one another automatically in most cases. You can use a so-called 'Range Extender' if you wish to expand your network using WDS or Bridging. This is an appliance largely similar to an 'Access Point'. The advantage of using a Range Extender rather than a second router – if the second router bridging is supported – is that a Range Extender is considerably cheaper.

# Index

Access blocks .....	16	Online games .....	14
Access Point ..... See Range Extender		Operating system .....	15
Administrator .....	16	Package filter	
Application.....	15	Packet inspection .....	15
ASCII.....	17	Packet inspection .....	15
Block .....	15	Parental Control .....	16
Bridging..... See WDS		Plug & Play.....	15
Business network .....	16	Policies..... 15. See Rules	
Data traffic.....	16	Pool.....	13
DDNS		Port Triggering.....	14
Dynamic DNS..... See DNS		Ports.....	14
DHCP		Pre Shared Key (PSK).....	17
Dynamic Host Configuration		Private IP addresses .....	13
Protocol .....	13	Programming language .....	15
DMZ		Public IP address .....	13
DeMilitarized Zone .....	14	Range .....	17
DNS		Range Extender .....	18
Domain Name System.....	13	Rules.....	15
Domain.....	16	Schedule Rule.....	15
Domain Filter.....	16	SNMP	
Domain name.....	13	Simple Network Management	
Dynamic .....	13	Protocol .....	16
Dynamic DNS.....	13	Tunnel .....	16
Explicit content .....	15	UPnP	
Firewall.....	9	Universal Plug and Play.....	15
Firewall software solution .....	14	URL Blocking .....	15
Gatekeeper .....	15	Virtual Server .....	16
Hardware .....	14	Viruses.....	14
Hexadecimal .....	16	VPN	
Key.....	17	Virtual Private Networking .....	16
Key words		WDS	
Catchwords .....	15	Wireless Distribution System .....	17
MAC address .....	16	WEP encryption.....	17
Name resolution .....	13	Wi-Fi Protected Access ..... See WPA	
NAT		WPA.....	17
Network Address Translation.....	13	WPA2.....	17

# Dichiarazione di Conformità

Per assicurarsi della sicurezza e della conformità del prodotto con le direttive e leggi create dalla commissione della comunità europea può ottenere una copia della dichiarazione di conformità del Suo prodotto inviando una mail a: [info@eminent-online.com](mailto:info@eminent-online.com). Può contattarci anche via posta a:

Eminent Computer Supplies  
Postbus 276  
6160 AG GELEEN  
The Netherlands

Si prega di indicare chiaramente 'Dichiarazione di Conformità' e il codice dell'articolo del quale vuole ottenere una copia della dichiarazione di conformità.



Trademarks: all brand names are trademarks and/or registered trademarks of their respective holders.

The information contained in this document has been created with the utmost care. No legal rights can be derived from these contents. Eminent cannot be held responsible, nor liable for the information contained in this document.



Eminent is a member of the Intronic Group