



MANUAL

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

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

# EM4206/EM4207 - ADSL2/2+ Modem



## Warnungen und Punkte zur Beachtung

Das Öffnen des Produktes und/oder Produkte kann zu schweren Verletzungen führen! Reparaturen des Produktes sollte nur von qualifizierten Eminent Technikern durchgeführt werden!

## Inhaltsverzeichnis

1.0 Garantiebedingungen .....	2
2.0 Einleitung .....	3
2.1 Funktionen und Features .....	3
2.2 Verpackungsinhalt .....	3
2.2 LED-Indikatoren des Modemrouters .....	3
3.0 Konfiguration mit Installationsassistent .....	4
4.0 Manuelle Konfiguration des Routers .....	4
4.1 Modemrouter anschließen .....	4
4.2 Modemrouter manuell für das Internet konfigurieren .....	4
4.2.1 PPP Provider konfigurieren .....	5
4.2.2 1483 Bridged Provider konfigurieren .....	5
4.2.3 Andere Provider konfigurieren .....	5
5.0 Erweiterte Einstellungen (Advanced) / Firewall .....	6
5.1 Uhr einstellen (SNTP) .....	6
5.2 Port Forwarding (Firewall) .....	6
5.3 IP Filter .....	7
5.4 LAN Clients .....	7
5.5 Bridge Filter .....	7
5.6 Static Routing .....	7
5.7 Dynamic Routing .....	7
6.0 Service und Support .....	7

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

## 1.0 Garantiebedingungen

Die fünfjährige Eminent-Garantie gilt für alle Eminent Produkte, außer vor oder während des Kaufs wurde eine andere Übereinkunft erwähnt. Beim Kauf eines Eminent Produktes aus zweiter Hand ergibt sich die verbleibende Garantiezeit aus dem Kaufdatum des ersten Besitzers. Die Eminent Garantie gilt für alle Eminent Produkte und Teile, die unlöslich mit dem Hauptprodukt verbunden bzw. auf diesem montiert sind. Netzteile, Batterien, Antennen und andere Produkte, die nicht im Hauptprodukt integriert sind bzw. mit diesem verbunden sind und/oder Produkte, bei denen normaler Verschleiß zweifelsfrei nach anderem Muster verläuft als bei dem

Hauptprodukt, sind nicht von der Eminent Garantie gedeckt. Produkte sind nicht von der Eminent Garantie gedeckt, wenn diese inkorrekt/unsachgemäß verwendet, externen Einflüssen ausgesetzt oder von unbefugten Personen geöffnet wurden.

## 2.0 Einleitung

Glückwunsch zu Ihrem Kauf dieses hoch qualitativen Eminent Produktes! Dieses Produkt wurde von Eminent's technischen Experten ausgiebig getestet. Sollten Sie mit diesem Produkt Probleme haben, sind Sie mit einer fünfjährigen Eminent Garantie geschützt. Bitte bewahren Sie dieses Handbuch und den Kaufbeleg sicher auf.

*Registrieren sie dieses Produkt jetzt auf [www.eminent-online.com](http://www.eminent-online.com) und erhalten Sie Produkt Updates!*

### 2.1 Funktionen und Features

Mit dem Eminent ADSL2/2+ Modem können Sie mit dem Internet verbinden und schnell und einfach ihr eigenes Kabelnetzwerk aufbauen. Alles mit einem einzigen Gerät. Das EM4206 ist für analoge Telefonleitungen geeignet. Das EM4207 ist für ISDN-Telefonleitungen geeignet.

### 2.2 Verpackungsinhalt

Prüfen Sie, dass die folgenden Artikel enthalten sind:

- EM4206 analoger ADSL-Modemrouter oder EM4207 ISDN ADSL-Modemrouter.
- Netzteil.
- Ein UTP-Netzwerkkabel.
- Ein Telefonkabel.
- Eine CD-ROM mit Benutzerhandbuch und/oder Software.

### 2.2 LED-Indikatoren des Modemrouters

<b>PWR</b>	<i>Leuchtet, wenn Router eingeschaltet ist.</i>
<b>PPP</b>	<i>Leuchtet, wenn eine PPP-Session begonnen hat. (Bei Verbindung mit einem PPPoA oder PPPoE Provider.)</i>
<b>LAN 1,2,3 und 4</b>	<i>Leuchtet, wenn die Netzwerkkabel ordnungsgemäß mit denen entsprechenden Anschlüssen an der Rückseite des Modems verbunden sind. Blinkt, wenn Daten ausgetauscht werden.</i>
<b>ADSL</b>	<i>Leuchtet, wenn das ADSL-Signal in der Telefonleitung erkannt wurde. Für die Erkennung des ADSL-Signals werden ca. 60 Sekunden benötigt. Leuchtet diese LED nicht, wenden Sie sich bitte an Ihren Provider. Hört die LED nicht auf zu blinken, überprüfen Sie die ADSL-Leitung und den ADSL-Verteiler.</i>

## 3.0 Konfiguration mit Installationsassistent

Die einfachste Art, den Modemrouter zu konfigurieren, ist mithilfe des Installationsassistenten, wie in diesem Kapitel beschrieben. Wenn sie nicht den Assistenten auf der CD-ROM verwenden möchten, können Sie den Modemrouter auch manuell konfigurieren.

1. Schalten Sie den Computer ein.
2. Legen Sie die beiliegende CD-ROM in das CD-ROM-Laufwerk.
3. Der Assistent startet automatisch.
4. Befolgen Sie die Anweisungen auf Ihrem Bildschirm, bis die Installation beendet ist. Jetzt sind sie mit dem Internet verbunden.

*Wenn Sie die CD-ROM nicht verwenden möchten, können Sie den Modemrouter auch manuell konfigurieren. Siehe Kapitel 4.1 für weitere Informationen.*

## 4.0 Manuelle Konfiguration des Routers

Wenn Sie den Router manuell konfigurieren möchten, ist es wichtig, dass ihr Internet Browser und Netzwerkeinstellungen korrekt konfiguriert sind. Die Einstellungen sind per Default korrekt. Wenn Sie sich bei den Einstellungen ihres Internetbrowsers und Netzwerks nicht sicher sind, siehe das Eminent Handbuch auf der CD-ROM.

### 4.1 Modemrouter anschließen

1. Schalten Sie den Computer aus.
2. Verbinden Sie den Modemrouter mithilfe des beiliegenden Netzteils mit einer Steckdose.
3. Verbinden Sie das beiliegende Telefonkabel mit dem DSL-Anschluss Ihres Modemrouters.
4. Verbinden Sie das andere Ende des Telefonkabels mit dem ADSL-Verteiler (nicht im Lieferumfang).
5. Verbinden Sie das beiliegende Netzkabel mit einem der LAN-Anschlüsse am Modemrouter.
6. Verbinden Sie das andere Ende des Netzkabels mit dem Netzwerkanschluss Ihres Computers.

### 4.2 Modemrouter manuell für das Internet konfigurieren

Um den Modemrouter für das Internet zu konfigurieren, müssen Sie zuerst eine Verbindung mit dem Modemrouter herstellen. Befolgen Sie die unten stehenden Anweisungen, um eine Verbindung mit dem Modemrouter herzustellen.

1. Öffnen Sie Ihren Browser (Internet Explorer, Firefox, Safari).
2. Geben Sie „http://192.168.1.1“ in das Adressfeld ein.
3. Drücken Sie die Eingabetaste oder klicken Sie „Go to“.

4. Geben Sie als „Username“ (Benutzername) „Admin“ ein.
5. Geben Sie als „Password“ (Kennwort) „Admin“ ein.
6. Klicken „OK“.
7. Die Willkommens-Anzeige des Modemrouters erscheint.

#### 4.2.1 PPP Provider konfigurieren

1. Klicken Sie „Wizard“ (Assistent).
2. Klicken Sie „Wizard“ (Assistent) im Menü auf der linken Seite.
3. Klicken Sie „Country“ (Land).
4. Wählen Sie Ihr Land (z.B. „Germany“ – Deutschland).
5. Klicken Sie „ISP“.
6. Wählen Sie Ihren Provider (z.B. „ADSL KPN“).
7. Klicken Sie „Next“ (Weiter), um fortzufahren.
8. Geben Sie Ihren ADSL-Benutzernamen (username) und Kennwort (password) unter „Set PPP Password“ (PPP-Kennwort einstellen) ein.
9. Klicken Sie „Apply“ (Übernehmen), um die Einstellungen zu speichern und den Modemrouter neu zu starten.

**Achtung!** Ein Neustart des Modemrouters kann eine Minute in Anspruch nehmen!  
 Nachdem das Modem neu gestartet wurde, ist Ihre Internetverbindung hergestellt..

#### 4.2.2 1483 Bridged Provider konfigurieren

1. Klicken Sie „Wizard“ (Assistent).
2. Klicken Sie „Wizard“ (Assistent) im Menü auf der linken Seite.
3. Klicken Sie „Country“ (Land).
4. Wählen Sie Ihr Land (z.B. „Germany“ – Deutschland).
5. Klicken Sie „ISP“.
6. Wählen Sie Ihren Provider (z.B. „BabyXL“).
7. Wählen Sie „DHCP“ unter „Connection Type“ (Verbindungstyp).
8. Klicken Sie „Next“ (Weiter), um fortzufahren.
9. Klicken Sie „Apply“ (Übernehmen), um die Einstellungen zu speichern und den Modemrouter neu zu starten.

**Achtung!** Ein Neustart des Modemrouters kann eine Minute in Anspruch nehmen!  
 Nachdem das Modem neu gestartet wurde, ist Ihre Internetverbindung hergestellt..

#### 4.2.3 Andere Provider konfigurieren

1. Klicken Sie „Config“ (konfigurieren).
2. Klicken Sie „New Connection“ (Neue Verbindung).
3. Geben Sie die von Ihrem Provider angegebenen Einstellungen ein.
4. Klicken Sie „Apply“ (Übernehmen).
5. Klicken Sie „Save All“ (Alles speichern) (linke Spalte).

6. Klicken Sie „Save“ (Speichern) (unten rechts), um den Modemrouter erneut zu starten.

**Achtung! Ein Neustart des Modemrouters kann eine Minute in Anspruch nehmen! Nachdem das Modem neu gestartet wurde, ist Ihre Internetverbindung hergestellt..**

## 5.0 Erweiterte Einstellungen (Advanced) / Firewall

Im Menü „Advanced“ (Erweitert) können Sie erweiterte Einstellungen vornehmen. Für diese Einstellungen benötigen Sie fortgeschrittene Kenntnisse von Computernetzwerken. Diese Einstellungen sind für Einsteiger nicht geeignet.

### 5.1 Uhr einstellen (SNTP)

Die interne Uhr des Modemrouters kann mit dem Internet synchronisiert werden. Gehen Sie dabei folgendermaßen vor.

1. Klicken Sie „Advanced“ (Erweitert).
2. Klicken Sie „SNTP“.
3. Markieren Sie „Enable SNTP“ (SNTP aktivieren).
4. Geben Sie die IP-Adresse des Zeitserver ein (z.B. „212.204.235.152“).

Eine Liste mit Adressen von Zeitservern finden Sie unter <http://ntp.isc.org/bin.view/Servers/WebHome>.

### 5.2 Port Forwarding (Firewall)

Dieses Gerät hat eine interne Firewall. D.h., alle externen Daten, die nicht spezifisch angefordert wurden, werden nicht an die am Modemrouter angeschlossenen Computer weitergegeben. Aller normaler Datenverkehr, speziell vom Benutzer angefordert, wird an die am Modemrouter angeschlossenen Computer weitergegeben.

Programme und Anwendungen, die unter dem Schutz einer Firewall nicht verwendet werden können, funktionieren nur ordnungsgemäß, wenn Sie die Firewall entsprechend einstellen. Einige Beispiele für Anwendungen, bei denen die Firewall eingestellt werden muss: Spiele, die von Ihnen gehostet werden oder Programme wie E-Donkey und VNC.

Wenn Sie diese oder ähnliche Anwendungen und Programme verwenden möchten, müssen Sie zuerst ihre lokale IP-Adresse wissen.

Im Menü „LAN clients“ des Modemrouters müssen Sie ein System definieren. Geben Sie den Namen des Systems einschließlich der IP-Adressen ein. Klicken Sie „Apply“ (Übernehmen) zur Bestätigung.

Klicken Sie „Save Setting and Reboot“ (Einstellungen speichern und neu starten), um die Einstellungen zu speichern. Wenn gewünscht, können Sie unter „Custom Rule“ (Benutzerdefinierte Regeln) Ihre eigenen Regeln erstellen.

### 5.3 IP Filter

Diese Option ist das Gegenteil von „Port Forwarding“. Mit dieser Option können Sie Datenverkehr von bestimmten Computern blockieren. Anhand von Port-Nummern und IP-Adressen können Sie Datenzugang blockieren.

### 5.4 LAN Clients

Der Modemrouter fügt Computer, die eine IP Adresse beantragen, automatisch einer Liste hinzu. Dadurch können sie die Computer in den Menüs „Port Forwarding“ und „IP Filter“ auswählen. Wenn Sie Computer mit statischen IP Adressen verwenden, müssen Sie diese manuell als ein „LAN client“ festlegen. Geben Sie dafür einfach Hostname und IP-Adresse ein. Die MAC-Adresse wird nicht benötigt.

### 5.5 Bridge Filter

In diesem Menü können Sie aufgrund von MAC-Adressen Datenverkehr in ihrem Netzwerk blockieren. Diese Option ist per Default deaktiviert. Diese Option ist nicht für Einsteiger geeignet.

### 5.6 Static Routing

In diesem Menü können Sie die Routingtabelle des Modemrouters bearbeiten und speziellen Hosts ein Gateway zuweisen.

### 5.7 Dynamic Routing

Durch Aktivieren von Dynamic Routing kann Ihr Modemrouter auf RIP V1 oder V2 Nachrichten reagieren. Mithilfe dieser Technologie findet der Modemrouter den kürzesten Weg zu einem Host oder Subnetz.

**Achtung! Dynamic Routing wird von niederländischen Providern nicht unterstützt. Aktivieren Sie diese Option nur, wenn sie von Ihrem Provider unterstützt wird und die Verwendung dieser Option erlaubt ist.**

## 6.0 Service und Support

Dieses Benutzerhandbuch wurde von Eminent's technischen Experten sorgfältig geschrieben. Wenn Sie bei der Installation oder Verwendung des Produktes Probleme haben, wenden Sie sich bitte an [support@eminent-online.com](mailto:support@eminent-online.com).

# 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.....15
- 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 .....16
- Expanding the range of your wireless network.....17
- Index .....18



## 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.....	14	Packet inspection .....	15
ASCII.....	17	Packet inspection .....	15
Block .....	15	Parental Control .....	15
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 .....	17
Domain Name System.....	13	Rules.....	15
Domain.....	15	Schedule Rule.....	15
Domain Filter.....	15	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.....	16
Name resolution .....	13	Wi-Fi Protected Access .....	See WPA
NAT		WPA.....	17
Network Address Translation.....	13	WPA2.....	17

# Konformitätserklärung

Um Ihre Sicherheit und die Konformität des Produktes mit den Direktiven und Vorschriften der EU-Kommission sicherzustellen, können Sie eine Kopie der Konformitätserklärung für dieses Produkt anfordern, indem Sie eine E-Mail schreiben an: [info@eminent-online.com](mailto:info@eminent-online.com). Oder schicken Sie einen Brief an:

Eminent Computer Supplies  
P.O. Box 276  
6160 AG Geleen  
The Netherlands

Geben Sie deutlich „Declaration of Conformity“ (Konformitätserklärung) und die Artikelnummer des Produktes an, für dass Sie eine Konformitätserklärung anfordern möchten.



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