



MANUAL

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

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

# EM4206/EM4207 - ADSL2/2+ Modem



## Warnings and points of attention

Opening of the product and/or products can lead to severe injuries! Repairing of the product should be done by the qualified Eminent staff!

## Table of contents

1.0 Warranty conditions.....	2
2.0 Introduction .....	3
2.1 Functions and features .....	3
2.2 Packing contents .....	3
2.2 LED indicators on the modem router.....	3
3.0 Configuring using the installation wizard .....	4
4.0 Manually configuring the router.....	4
4.1 Connecting the modem/router .....	4
4.2 Manually configuring the modem router for the Internet .....	4
4.2.1 Configuring PPP providers.....	5
4.2.2 Configuring 1483 Bridged providers.....	5
4.2.3 Configuring other providers.....	5
5.0 Advanced settings / firewall .....	6
5.1 Configuring the clock (SNTP) .....	6
5.2 Port forwarding (firewall).....	6
5.3 IP Filters .....	7
5.4 LAN Clients .....	7
5.5 Bridge filters .....	7
5.6 Static Routing .....	7
5.7 Dynamic Routing .....	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.*

## 1.0 Warranty conditions

The five-year Eminent warranty applies for all Eminent products unless mentioned otherwise before or during the moment of purchase. When having bought a second-hand Eminent product the remaining period of warranty is measured from the moment of purchase by the product's first owner. The Eminent warranty applies to all Eminent products and parts indissolubly connected to and/or mounted on the main product. Power supply adapters, batteries, antennas and all other products not integrated in or directly connected to the main product and/or products of which, without reasonable doubt, can be assumed that wear and tear show a different pattern than the main

product are not covered by the Eminent warranty. Products are not covered by the Eminent warranty when exposed to incorrect/improper use, external influences and/or when opened by parties other than Eminent.

## 2.0 Introduction

Congratulations on your purchase of this high-quality Eminent product! This product has undergone extensive testing by Eminent's technical experts. Should you experience any problems with this product, you are covered by a five-year Eminent warranty. Please keep this manual and the receipt in a safe place.

*Register this product now on [www.eminent-online.com](http://www.eminent-online.com) and receive product updates!*

### 2.1 Functions and features

With the Eminent ADSL2/2+ Modem you can connect to the Internet and create your own wired network quick and easy. Just using one, single device. The EM4206 is suited for analogue telephone lines. The EM4207 is suited for ISDN telephone lines.

### 2.2 Packing contents

The following parts need to be present in the packing:

- EM4206 ADSL modem/router analogue or EM4207 ADSL modem/router ISDN.
- Power supply adapter.
- A UTP networking cable.
- A modular telephone cable.
- A CD-rom containing user manuals and/or software.

### 2.2 LED indicators on the modem router

<b>PWR</b>	<i>Lit when the router is turned on.</i>
<b>PPP</b>	<i>Lit when a PPP session has been established. (When connecting to a PPPoA or PPPoE provider).</i>
<b>LAN 1,2,3 and 4</b>	<i>Lit when the networking cables have been properly connected to the corresponding port on the back of the modem. Will blink when data traffic is generated.</i>
<b>ADSL</b>	<i>Lit when the ADSL signal has been found on the telephone line. It takes approximately 60 seconds to find the ADSL signal. When this LED stays off, please contact your provider. When this LED keeps blinking you need to check the ADSL line and the ADSL splitter.</i>

## 3.0 Configuring using the installation wizard

The easiest way to configure the modem router is by using the installation wizard, as explained in this chapter. If you do not wish to use the wizard as found on the CD-rom, you can also configure the modem router manually.

1. Turn on the computer.
2. Insert the enclosed CD-rom in the CD-rom player.
3. The wizard will automatically start.
4. Follow the instructions on your screen till the installation has been finished. You now have a working Internet connection.

*When you do not wish to use the CD-rom, you can also configure the modem router by hand. Please refer to paragraph 4.1 for more information.*

## 4.0 Manually configuring the router

If you wish to manually configure the router it is important that your Internet browser and network settings are configured correctly. The settings are correct by default. If you are not sure about the settings of your Internet browser and network, consult the Eminent Advanced Manual on the CD-rom.

### 4.1 Connecting the modem/router

1. Turn the computer off.
2. Connect the modem router to the wall-outlet by using the enclosed power supply adapter.
3. Connect the enclosed modular telephone cable to the DSL port on your modem router.
4. Connect the other side of the modular telephone cable to the ADSL splitter (not enclosed).
5. Connect the enclosed networking cable to one of the LAN ports on the modem router.
6. Connect the other side of the networking cable to the networking adapter in your computer.

### 4.2 Manually configuring the modem router for the Internet

To be able to configure the modem router for the Internet, you will first need to connect to the modem router. Follow the instructions below to connect to the modem router.

1. Open your browser (Internet Explorer, Firefox, Safari).
2. Type 'http://192.168.1.1' in the address bar.
3. Press the enter key or click 'Go to'.

4. Type 'Admin' at 'Username'.
5. Type 'Admin' at 'Password'.
6. Click 'Ok'.
7. You have now access to the welcome screen of the modem router.

### 4.2.1 Configuring PPP providers

1. Click 'Wizard'.
2. Click 'Wizard' in the menu on the left.
3. Click 'Country'.
4. Choose your country (e.g. 'Netherlands').
5. Click 'ISP'.
6. Choose your provider (e.g. 'ADSL KPN').
7. Click 'Next' to continue.
8. Type your ADSL username and password at 'Set PPP Password'.
9. Click 'Apply' to store the settings and restart the modem router.

*Attention! Restarting the modem router may take a minute! When the modem has been restarted you will have established an Internet connection..*

### 4.2.2 Configuring 1483 Bridged providers

1. Click 'Wizard'.
2. Click 'Wizard' in the menu on the left.
3. Click 'Country'.
4. Choose your country (e.g. 'Netherlands').
5. Click 'ISP'.
6. Choose your provider (e.g. 'BabyXL').
7. Choose 'DHCP' at 'Connection Type'.
8. Click 'Next' to continue.
9. Click 'Apply' to store the settings and restart the modem router.

*Attention! Restarting the modem router may take a minute! When the modem has been restarted you will have established an Internet connection..*

### 4.2.3 Configuring other providers

1. Click 'Config'.
2. Click 'New Connection'.
3. Submit the settings you obtained from your provider.
4. Click 'Apply'.
5. Click 'Save All' (left column).
6. Click 'Save' (down-right) to restart the modem router.

*Attention! Restarting the modem router may take a minute! When the modem has been restarted you will have established an Internet connection..*

## 5.0 Advanced settings / firewall

The 'Advanced' menu lets you modify advanced settings. These options require advanced knowledge of computer networking and are therefore not suited for novice users.

### 5.1 Configuring the clock (SNTP)

The built-in clock in the modem router can be synchronized with the Internet by following the procedure below.

1. Click 'Advanced'.
2. Click 'SNTP'.
3. Check 'Enable SNTP'.
4. Enter the IP-address of the time server (e.g. '212.204.235.152').

A complete list of addresses for time servers can be found at  
<http://ntp.isc.org/bin.view/Servers/WebHome>

### 5.2 Port forwarding (firewall)

This device has a built-in firewall. This means all external data not specifically requested will not be passing through to the computers connected to the modem router. All normal traffic, specifically requested by its users, gain access to the computers connected to the modem router.

Programs and applications that cannot be used under firewall protection will not function well, unless you specifically configure the firewall. Some examples of applications for which the firewall needs to be configured are: games you host yourself or programs such as E-Donkey and VNC.

When you wish to use applications as or similar to the programs mentioned above, you first need to obtain your local IP-address.

Through the 'LAN clients' menu in the modem router, you need to define a system. Fill out the name of the system including the IP-address. Click 'Apply' to confirm.

Click 'Save Setting and Reboot' to store the settings. When desired you can create your own rules by clicking 'Custom Rule'.

### 5.3 IP Filters

This option perform actions opposite from 'Port Forwarding'. By applying rules data traffic from a certain computer is blocked. This option allows you to block Internet requests based on port-numbers and IP-addresses.

### 5.4 LAN Clients

The modem router will add computers atomically requesting an IP-address to a list. This allows you to select them in the 'Port Forwarding' and 'IP Filter' menus. When using computers with fixed IP-addresses you manually need to assign these as a 'LAN-client'. You can do this by simply submitting the hostname and the IP-address. The MAC-address is not required.

### 5.5 Bridge filters

This menu allows you to block certain sorts of data traffic within your network based on the MAC-address. This option is disabled by default. Novice users are recommended not to use this option.

### 5.6 Static Routing

This menu allows you to edit the routing table of the modem router and assign the gateway for specific target hosts.

### 5.7 Dynamic Routing

By enabling dynamic routing you can have your modem router react to RIP V1 or V2 messages. This technology has the modem router find the shortest way to a host or subnet.

*Attention! Dynamic routing is normally not supported by Dutch providers. Only enable this option when your provider supports it and the use of this option is permitted.*

## 6.0 Service and Support

This users manual has been carefully written by Eminent's technical experts. If you have problems installing or using the product, please contact [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.....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



## 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

# Declaration of Conformity

To ensure your safety and compliance of the product with the directives and laws created by the European Commission you can obtain a copy of the Declaration of Conformity concerning your product by sending an e-mail message to: [info@eminent-online.com](mailto:info@eminent-online.com). You can also send a letter to:

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

Clearly state 'Declaration of Conformity' and the article code of the product of which you would like to obtain a copy of the Declaration of Conformity.



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 Intronics Group