

EMINENT



MODE D'EMPLOI

EM4206/EM4207 - Modem ADSL2/2+

WWW.EMINENT-ONLINE.COM

EM4206/EM4207 - Modem ADSL2/2+



Avertissements et points à surveiller

L'ouverture du produit et/ou des produits peut entraîner de graves lésions! Faites toujours faire vos réparations par le personnel qualifié d'Eminent!

Sommaire

1.0 Conditions de garantie	2
2.0 Introduction	3
2.1 Fonctions et caractéristiques	3
2.2 Contenu du conditionnement	3
2.3 Explications des lampes témoins	3
3.0 Configuration via le programme d'installation	4
4.0 Installer le routeur manuellement	4
4.1 Installer le routeur/modem	4
4.2 Configurer le routeur-modem manuellement pour l'internet	5
4.2.1 Configuration pour des fournisseurs d'accès PPP	5
4.2.2 Configuration pour fournisseurs d'accès 1483 Bridged	5
4.2.3 Configuration pour les autres fournisseurs d'accès	6
5.0 Parapètres avancés / Coupe-feu	6
5.1 Le réglage de l'horloge (SNTP)	6
5.2 Port Forwarding (Coupe-feu)	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	8
6.0 Service et support	8

On page 9 you will find the Eminent Advanced Manual for networking settings and information about home networking. (English only)

1.0 Conditions de garantie

Une période de garantie de cinq ans est accordée pour tous les produits Eminent, sauf indication contraire au moment de l'achat. Lors de l'achat d'un produit Eminent en seconde main, la période de garantie est maintenue compte tenu de la date d'achat par le premier propriétaire.

Le règlement de garantie Eminent est d'application sur tous les produits et les éléments Eminent qui sont indissociablement liés au produit concerné. Les alimentations, les piles, les batteries, les antennes et tous les autres produits qui ne sont pas intégrés ni directement liés au produit principal ou les produits dont il peut

être raisonnablement accepté qu'ils connaissent une usure différente de celle du produit principal ne tombent pas sous le règlement de garantie Eminent. La garantie est annulée en cas d'utilisation erronée ou illicite, d'influences externes et/ou en cas d'ouverture du boîtier du produit concerné par des parties autres qu'Eminent.

2.0 Introduction

Félicitation pour l'achat de ce produit Eminent de haute qualité! Ce produit a été amplement testé par les experts techniques d'Eminent. Si, malgré tous nos soins, ce produit présentait un quelconque défaut, vous pouvez faire appel durant cinq ans à la garantie Eminent. Conservez donc soigneusement ce manuel ensemble avec la preuve d'achat.

Enregistrez votre achat maintenant sur www.eminent-online.com et recevez les mises à jour du produit!

2.1 Fonctions et caractéristiques

Le modem ADSL2/2+ d'Eminent vous permet de réaliser rapidement et facilement une connexion avec l'internet et d'installer un réseau avec fil à l'aide d'un seul appareil! Le EM4206 convient pour l'ADSL par une ligne téléphonique analogique. Le EM4207 convient pour l'ADSL par une ligne téléphonique ISDN.

2.2 Contenu du conditionnement

Les éléments suivants sont présents dans votre boîte:

- Modem/routeur ADSL analogique EM4206 ou modem/routeur ADSL ISDN EM4207.
- Adaptateur réseau.
- Un câble UTP "droit".
- Un câble de téléphone modulaire.
- Un manuel d'utilisation.

2.3 Explications des lampes témoins

PWR	<i>Brûle lorsque le routeur est allumé.</i>
PPP	<i>Indique qu'une session PPP a été créée. (Lors de l'utilisation d'un fournisseur d'accès PPPoA ou PPPoE.)</i>
LAN 1,2,3 et 4	<i>Ces témoins brûlent lorsque les câbles réseau sont connectés au routeur. Ces témoins clignotent lorsqu'il y a une circulation de données sur le câble réseau concerné.</i>
ADSL	<i>Ce témoin brûle en permanence lorsque le signal ADSL a été détecté sur la ligne de téléphone. 60 secondes peuvent se passer avant que ce témoin brûle en permanence. Si ce témoin continue</i>

à clignoter, vous devez contrôler la ligne ADSL et le splitter. Le modem ne reçoit pas un signal correct.

3.0 Configuration via le programme d'installation

La manière la plus simple d'installer le routeur est d'utiliser le programme d'installation tel que décrit dans ce chapitre. Si lors de l'installation, vous ne désirez pas faire usage du programme sur le CD-rom qui vous a été livré, vous pouvez également installer le routeur manuellement.

1. Allumez votre ordinateur.
2. Placez le CD-rom dans le lecteur de CD-rom.
3. Le programme d'installation est lancé.
4. Suivez les étapes à l'écran jusqu'à la fin de l'installation. Dès à présent, votre liaison internet est opérationnelle.

Si vous ne désirez pas faire usage du programme sur le CD-rom, vous pouvez également installer le routeur manuellement. Passez au point 4. 1.

4.0 Installer le routeur manuellement

Pour l'installation manuelle du routeur-modem, il est important que votre navigateur internet et votre réseau soient bien configurés. Les installations sont automatiquement bonnes, à moins que vous n'ayez changé quelque chose auparavant. Consultez le manuel Eminent Advanced sur le CD-rom si vous avez des doutes quant à l'installation correcte de votre navigateur internet et de votre réseau.

4.1 Installer le routeur-modem

1. Eteignez votre ordinateur.
2. Connectez le routeur-modem au moyen de l'adaptateur pour réseau électrique à une prise.
3. Connectez le câble réseau modulaire à la porte DSL de votre routeur-modem.
4. Connectez l'autre côté du câble de téléphone modulaire au splitter ADSL (Ce splitter n'est pas livré).
5. Connectez le câble de réseau à une des quatre portes "LAN" de votre routeur-modem.
6. Connectez l'autre côté de ce câble réseau à l'adaptateur de réseau de votre ordinateur

4.2 Configurer le routeur-modem manuellement pour l'internet

Afin de pouvoir configurer le routeur-modem pour une liaison à l'internet, vous devez d'abord établir la liaison avec votre routeur. Vous faites la liaison avec le routeur en suivant la procédure ci-dessous.

1. Ouvrez votre navigateur internet (Internet Explorer, Firefox, Safari).
2. Tapez "http://192.168.1.1" dans la barre d'adresse
3. Appuyez sur la touche enter ou cliquez sur "Allez vers".
4. Le nom d'utilisateur est réglé par défaut sur "Admin".
5. Le mot de passe est réglé par défaut sur "Admin".
6. Cliquez sur "Ok".
7. Vous avez à présent accès à l'écran d'accueil du routeur-modem.

4.2.1 Configuration pour des fournisseurs d'accès PPP

1. Cliquez en haut dans le menu sur "Wizard".
2. Cliquez dans le menu de gauche sur "Wizard".
3. Cliquez sur "Country".
4. Choisissez votre pays (Par exemple: Belgium).
5. Cliquez sur "ISP".
6. Choisissez votre fournisseur d'accès (Par exemple "ADSL KPN").
7. Cliquez sur "Next" pour continuer.
8. Remplissez auprès de "Set PPP Password" votre nom d'utilisateur ADSL et votre mot de passe.
9. Cliquez sur "Apply" pour enregistrer les paramètres et redémarrer votre routeur-modem.

Attention! Le démarrage du routeur-modem peut durer quelques minutes! Lorsque le routeur-modem a entièrement démarré, la liaison internet est opérationnelle.

4.2.2 Configuration pour fournisseurs d'accès 1483 Bridged

1. Cliquez en haut dans le menu sur "Wizard".
2. Cliquez dans le menu de gauche sur "Wizard".
3. Cliquez sur "Country".
4. Choisissez votre pays (Par exemple: Belgium).
5. Cliquez sur "ISP".
6. Choisissez votre fournisseur d'accès (Par exemple "BabyXL").
7. Auprès de "Connection Type" choisissez "DHCP" par défaut.
8. Cliquez sur "Next" pour poursuivre.
9. Cliquez sur "Apply" pour enregistrer les paramètres et redémarrer votre routeur-modem.

Attention! Le démarrage du routeur-modem peut durer quelques minutes! Lorsque le routeur-modem a entièrement démarré, la liaison internet est opérationnelle.

4.2.3 Configuration pour les autres fournisseurs d'accès

Consultez les données de connexion de votre fournisseur d'accès.

1. Cliquez en haut dans le menu sur "Config".
2. Cliquez sur "New Connection".
3. Remplissez les données que vous avez reçues de votre fournisseur d'accès.
4. Cliquez sur "Apply".
5. Cliquez sur "Save All" (Colonne de gauche).
6. Cliquez sur "Save" (en bas à droite) pour redémarrer votre routeur-modem.

Attention! Le démarrage du routeur-modem peut durer quelques minutes! Lorsque le routeur-modem a entièrement démarré, la liaison internet est opérationnelle.

5.0 Paramètres avancés / Coupe-feu

Le menu "Advanced" vous permet de modifier certains paramètres avancés. Un certain nombre de ces options exigent une connaissance très spécifique des réseaux et elles ne conviennent donc pas pour des utilisateurs débutants.

5.1 Le réglage de l'horloge (SNTP)

L'horloge intégrée de votre routeur-modem peut être synchronisée avec internet.

1. Cliquez sur "Advanced".
2. Cliquez sur "SNTP"
3. Cochez "Enable SNTP".

Remplissez l'adresse IP d'un time-server (par exemple "212.204.235.152").

Vous trouverez une liste complète des time-servers sur:

<http://ntp.isc.org/bin/view/Servers/WebHome>

5.2 Port Forwarding (Coupe-feu)

Cet appareil dispose d'un coupe-feu intégré. Cela signifie que toutes les données externes qui n'ont pas été demandées ne sont pas transmises par le routeur vers les ordinateurs "derrière" ce routeur. La circulation normale que vous demandez vous-même est envoyée simplement.

Les programmes qui ne peuvent pas être utilisés derrière un coupe-feu ne fonctionneront pas bien, à moins que vous n'ayez configuré le coupe-feu dans le

routeur. Quelques exemples de programmes pour lesquels vous devez régler le coupe-feu sont des jeux que vous hébergez vous-même ou des programmes tels que Edonkey, VNC etc.

Si vous désirez utiliser de telles applications, vous devez d'abord connaître votre adresse IP locale.

Via le menu "LAN clients" dans le routeur, vous devez définir un système. Vous remplissez le nom du système ainsi que l'adresse IP. Cliquez sur "apply" pour le confirmer.

Ensuite, via le menu "port forwarding", vous pouvez appliquer des règles sur cette adresse IP. Vous choisissez dans le menu l'adresse IP du LAN et la catégorie, vous choisissez la règle et vous cliquez sur "add" pour le mettre dans le menu de droite. Cliquez sur "Apply" pour confirmer la modification.

Cliquez ensuite sur "Save setting and reboot" pour enregistrer le réglage.

5.3 IP Filters

Cette option est exactement l'inverse de Port Forwarding. En appliquant les règles, la circulation est explicitement retenue pour certains ordinateurs.

Cette option vous permet donc de limiter la circulation internet sur base des numéros de porte et des adresse IP.

5.4 LAN Clients

Le routeur-modem ajoutera les ordinateurs qui demandent automatiquement une adresse IP comme clients à cette liste, de sorte que vous puissiez les sélectionner dans les menus Port Forwarding et IP Filter. Cependant, si votre ordinateur utilise des adresses IP fixes, vous devez les ajouter manuellement comme LAN-client. Il suffit de remplir le hostname et l'adresse IP, l'adresse MAC n'est pas nécessaire.

5.5 Bridge filters

Via ce menu, il est possible, sur base d'une adresse MAC, de bloquer certains types précis de circulation dans votre réseau. Cette option est éteinte par défaut, son utilisation est déconseillée pour des utilisateurs débutants.

5.6 Static Routing

Via ce menu, vous pouvez adapter le tableau de routage de votre routeur-modem et indiquer le gateway pour des hosts cibles spécifiques.

5.7 Dynamic Routing

En enclenchant Dynamic routing, vous pouvez faire réagir le routeur-modem aux messages RIP V1 ou V2. De ce fait, le routeur peut détecter la route la plus courte vers un host ou subnet dans un réseau adéquat.

Attention! Les fournisseurs d'accès internet néerlandais ne soutiennent généralement pas cette option. N'enclenchez cette option que si votre fournisseur la soutient et qu'il en permet l'utilisation.

6.0 Service et support

Ce manuel a été rédigé soigneusement par les experts techniques de Eminent.

Si, malgré tout, vous rencontrez des problèmes lors de l'installation ou de l'utilisation de ce produit Eminent en question, vous pouvez envoyer un email à support@eminent-online.com (*English only*).

Vous pouvez également téléphoner au numéro du service d'assistance Eminent. Tél: 0900-70090. (45ct par minute, frais d'utilisation de votre téléphone portable non compris.)

Eminent Advanced Manual

Table of contents

- Table of contents.....9
- Why an Eminent advanced manual?10
- Your tips and suggestions in the Eminent Advanced Manual?.....10
- Service and support10
- Networking settings for Windows 98 and Windows ME.....10
- Networking settings for Windows 2000 and Windows XP11
- Networking settings for Windows Vista.....12
- Configuring Internet Explorer 5 and 5.5.....12
- Configuring Internet Explorer 6.....13
- Configuring Internet Explorer 7.....13
- DHCP, Automatic allocation of IP addresses.....14
- Translating IP addresses and domain names14
- Using a single IP address for your entire network14
- Security for your computer and your network.....15
- Making a computer available for Internet users in your network.....15
- Simplifying network management.....16
- Blocking websites with explicit content16
- Checking data traffic at package level16
- Blocking a complete domain.....17
- Carrying out actions based on date or time.....17
- A safe remote connection.....17
- Remote network management.....17
- Allocating or blocking network access17
- Making your wireless network secure18
- Expanding the range of your wireless network.....18
- Index20

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. 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.

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 and 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.

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	17	Online games	15
Access Point See Range Extender		Operating system	16
Administrator	17	Package filter	
Application.....	16	Packet inspection	16
ASCII.....	18	Packet inspection	16
Block	16	Parental Control	17
Bridging..... See WDS		Plug & Play.....	16
Business network	17	Policies..... 16. See Rules	
Data traffic.....	17	Pool.....	14
DDNS		Port Triggering.....	15
Dynamic DNS..... See DNS		Ports.....	15
DHCP		Pre Shared Key (PSK).....	18
Dynamic Host Configuration		Private IP addresses	14
Protocol	14	Programming language	16
DMZ		Public IP address	14
DeMilitarized Zone	15	Range	18
DNS		Range Extender	19
Domain Name System.....	14	Rules.....	16
Domain.....	17	Schedule Rule.....	16
Domain Filter.....	17	SNMP	
Domain name.....	14	Simple Network Management	
Dynamic	14	Protocol	17
Dynamic DNS.....	14	Tunnel	17
Explicit content	16	UPnP	
Firewall.....	10	Universal Plug and Play.....	16
Firewall software solution	15	URL Blocking	16
Gatekeeper	16	Virtual Server	17
Hardware	15	Viruses.....	15
Hexadecimal	17	VPN	
Key.....	18	Virtual Private Networking	17
Key words		WDS	
Catchwords	16	Wireless Distribution System	18
MAC address	17	WEP encryption.....	18
Name resolution	14	Wi-Fi Protected Access See WPA	
NAT		WPA.....	18
Network Address Translation.....	14	WPA2.....	18

Déclaration de Conformité

Pour vous assurer d'un produit fiable conforme aux directives établies par la Commission Européenne, vous pouvez demander une copie de la Déclaration de Conformité relative à votre produit en envoyant un email à : info@eminent-online.com. Vous pouvez aussi envoyer une lettre à :

Eminent Computer Supplies
Postbus 276
6160 AG GELEEN
Pays-Bas

Veuillez mentionner clairement dans ce cas 'Déclaration de Conformité' et le numéro d'article du produit pour lequel vous demandez la Déclaration de Conformité.



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