



MANUAL DE USUARIO

EM4206/EM4207 - Módem ADSL2/2+

WWW.EMINENT-ONLINE.COM

EM4206/EM4207 - Módem ADSL2/2+



Advertencias y puntos de atención

¡La apertura de uno o varios productos puede causar graves daños personales! ¡El producto solamente puede ser reparado por técnicos profesionales de Eminent!

Tabla de contenido

1.0 Condiciones de la garantía	2
2.0 Introducción.....	3
2.1 Funciones y características	3
2.2 Contenido del paquete.....	3
2.2 Indicadores LED del enrutador y módem	3
3.0 Configurar mediante el asistente para la instalación	4
4.0 Configurar el enrutador manualmente.....	4
4.1 Conectar el enrutador y módem.....	4
4.2 Configurar el enrutador y módem manualmente para Internet	5
4.2.1 Configurar proveedores PPP	5
4.2.2 Configurar proveedores 1483 Bridged	5
4.2.3 Configurar otros proveedores	6
5.0 Configuración avanzada y firewall	6
5.1 Configurar el reloj (SNTP).....	6
5.2 Reenvío de puerto (firewall).....	6
5.3 Filtros de direcciones IP	7
5.4 Clientes LAN	7
5.5 Filtros de puente.....	7
5.6 Enrutamiento estático	7
5.7 Enrutamiento dinámico	7
6.0 Servicio de atención al cliente y soporte técnico	8

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

1.0 Condiciones de la garantía

La garantía de Eminent de cinco años se aplica a todos los productos de Eminent a menos que se indique lo contrario antes o durante el momento de la compra. Si ha adquirido un producto de Eminent de segunda mano, el período restante de la garantía se contará desde el momento en el que el primer propietario del producto lo adquiriera. La garantía de Eminent se aplica a todos los productos de Eminent y a las partes indisolublemente conectadas al producto principal y/o montadas en éste. Los adaptadores de fuente de alimentación, las baterías, las antenas y el resto de productos no integrados en el producto principal o no conectados directamente a

éste, y/o los productos de los que, sin duda razonable, se pueda asumir que el desgaste y rotura muestran un patrón diferente al producto principal, no están cubiertos por la garantía de Eminent. Los productos no están cubiertos por la garantía de Eminent cuando se usan de manera incorrecta e inapropiada, se exponen a influencias externas o los abren terceras partes que no son Eminent.

2.0 Introducción

¡Enhorabuena por la compra de este producto de Eminent de alta calidad! Este producto ha sido sometido a un exigente proceso de pruebas por parte de técnicos expertos de Eminent. Si tiene problemas con este producto, tenga en cuenta que le ampara una garantía de Eminent de cinco años. Conserve este manual y el recibo de compra en un lugar seguro.

¡Registre este producto ahora en www.eminent-online.com y reciba las actualizaciones del mismo!

2.1 Funciones y características

Con el Módem ADSL2/2+ de Eminent puede conectarse a Internet y crear su propia red cableada de forma rápida y sencilla. Solamente tiene que usar un dispositivo. El dispositivo EM4206 está diseñado para líneas telefónicas analógicas. El dispositivo EM4207 está diseñado para líneas telefónicas RDSI.

2.2 Contenido del paquete

El paquete debe contener los siguientes componentes:

- Módem y enrutador ADSL EM4206 analógico, o módem y enrutador EM4207 ADSL RDSI.
- Adaptador de fuente de alimentación.
- Cable de red UTP.
- Cable telefónico modular.
- CD-ROM con los manuales de usuario y/o el software.

2.2 Indicadores LED del enrutador y módem

ALIM	Se ilumina cuando el enrutador está encendido.
PPP	Se ilumina cuando se ha establecido una sesión PPP. (Cuando se establece conexión con un proveedor PPPoA o PPPoE).
LAN 1,2,3 y 4	Se ilumina cuando los cables de red se han conectado correctamente al puerto correspondiente situado en la parte posterior del módem. Parpadeará cuando se genere tráfico de datos.
ADSL	Se ilumina cuando se ha encontrado la señal ADSL en la línea telefónica.

El dispositivo tarda aproximadamente 60 segundos en encontrar la señal ADSL. Cuando este indicador LED permanezca apagado, póngase en contacto con su proveedor. Cuando este indicador LED parpadee será necesario comprobar la línea ADSL y el divisor ADSL.

3.0 Configurar mediante el asistente para la instalación

La forma más sencilla de configurar el enrutador y módem es mediante el asistente para la instalación, tal y como se explica en este capítulo. Si no desea usar el asistente que se encuentra en el CD-ROM, también puede configurar el enrutador y módem manualmente.

1. Encienda su PC.
2. Inserte el CD-ROM incluido en el reproductor de CD-ROM.
3. El asistente se iniciará automáticamente.
4. Siga las instrucciones de la pantalla hasta que el asistente para la instalación haya finalizado. Ahora ya tiene una conexión a Internet operativa.

Si no desea usar el CD-ROM, también puede configurar el enrutador y módem manualmente. Consulte el párrafo 4.1 para obtener más información.

4.0 Configurar el enrutador manualmente

Si desea configurar el enrutador manualmente es importante que el explorador de Internet y los parámetros de la red estén perfectamente configurados. Los valores predeterminados de la configuración son correctos. Si no está seguro de la configuración del explorador de Internet y de la red, consulte el Manual avanzado de Eminent que encontrará en el CD-ROM.

4.1 Conectar el enrutador y módem

1. Apague su PC.
2. Conecte el enrutador y módem a la toma de corriente eléctrica mediante el adaptador de fuente de alimentación suministrado.
3. Conecte el cable de teléfono modular suministrado al puerto DSL del enrutador y módem.
4. Conecte el otro extremo de dicho cable al divisor ADSL (no incluido).
5. Conecte un cable de red incluido a uno de los puertos LAN del enrutador y módem.
6. Conecte el otro extremo del cable de red al adaptador de red del equipo.

4.2 Configurar el enrutador y módem manualmente para Internet

Para poder configurar el enrutador y módem para Internet, primero necesita conectar dicho enrutador y módem. Siga las instrucciones que se indican a continuación para conectar el enrutador y módem:

1. Abra el explorador (Internet Explorer, Firefox o Safari).
2. Escriba 'http://192.168.1.1' en la barra de direcciones.
3. Presione la tecla Entrar o haga clic en 'Ir'.
4. Escriba 'Admin' en el campo 'Nombre de usuario'.
5. Escriba 'Admin' en el campo 'Contraseña'.
6. Haga clic en 'Aceptar'.
7. Ahora tendrá acceso a la pantalla de bienvenida del enrutador y módem.

4.2.1 Configurar proveedores PPP

1. Haga clic en 'Asistente'.
2. Haga clic en 'Asistente' en el menú de la izquierda.
3. Haga clic en 'País'.
4. Elija el país (por ejemplo 'Países Bajos').
5. Haga clic en 'ISP'.
6. Elija el proveedor (por ejemplo 'ADSL KPN').
7. Haga clic en 'Siguiendo' para continuar.
8. Escriba su nombre de usuario y contraseña ADSL en el campo 'Establecer contraseña PPP'.
9. Haga clic en 'Aplicar' para almacenar la configuración y reiniciar el enrutador y módem.

¡Atención! ¡El reinicio del enrutador y módem puede tardar un minuto! Cuando el módem se haya reiniciado se habrá establecido una conexión a Internet.

4.2.2 Configurar proveedores 1483 Bridged

1. Haga clic en 'Asistente'.
2. Haga clic en 'Asistente' en el menú de la izquierda.
3. Haga clic en 'País'.
4. Elija el país (por ejemplo 'Países Bajos').
5. Haga clic en 'ISP'.
6. Elija el proveedor (por ejemplo 'BabyXL').
7. Elija 'DHCP' en el campo 'Tipo de conexión'.
8. Haga clic en 'Siguiendo' para continuar.
9. Haga clic en 'Aplicar' para almacenar la configuración y reiniciar el enrutador y módem.

¡Atención! ¡El reinicio del enrutador y módem puede tardar un minuto! Cuando el módem se haya reiniciado se habrá establecido una conexión a Internet.

4.2.3 Configurar otros proveedores

1. Haga clic en 'Config'.
2. Haga clic en 'Nueva conexión'.
3. Presente la configuración que obtuvo de su proveedor.
4. Haga clic en 'Aplicar'.
5. Haga clic en 'Guardar todo' (columna de la izquierda).
6. Haga clic en 'Guardar' (abajo a la derecha) para reiniciar el enrutador y módem.

¡Atención! ¡El reinicio del enrutador y módem puede tardar un minuto! Cuando el módem se haya reiniciado se habrá establecido una conexión a Internet.

5.0 Configuración avanzada y firewall

El menú 'Opciones avanzadas' le permite modificar la configuración avanzada. Estas opciones requieren un conocimiento avanzado de la interconexión en red del equipo y, por lo tanto, no son adecuadas para usuarios noveles.

5.1 Configurar el reloj (SNTP)

El reloj integrado en el enrutador y módem se puede sincronizar con Internet realizando el siguiente procedimiento.

1. Haga clic en 'Opciones avanzadas'.
2. Haga clic en 'SNTP'.
3. Active la opción 'Habilitar SNTP'.
4. Escriba la dirección IP del servidor de tiempo (por ejemplo '212.204.235.152').

En <http://ntp.isc.org/bin.view/Servers/WebHome> puede encontrar una lista completa de servidores de tiempo.

5.2 Reenvío de puerto (firewall)

Este dispositivo tiene un firewall integrado. Esto significa que todos los datos externos no específicamente solicitados no pasarán a través de los equipos conectados al enrutador y módem. Todo el tráfico normal, específicamente solicitado por sus usuarios, logrará entrar en los equipos conectados al enrutador y módem.

Los programas y aplicaciones que no se puedan usar bajo la protección del firewall no funcionarán bien, a menos que configure específicamente el firewall. Algunos ejemplos de aplicaciones para las que el firewall necesita configurarse son: juegos que hospeda el usuario o programas como E-Donkey y VNC.

Cuando desea usar aplicaciones como los programas mencionados anteriormente o similares a ellos, primero debe obtener una dirección IP local.

Mediante el menú 'Clientes LAN' del enrutador y módem debe definir un sistema. Rellene el nombre del sistema, incluida la dirección IP. Haga clic en 'Aplicar' para confirmar.

Haga clic en 'Guardar configuración y reiniciar' para almacenar la configuración. Cuando lo desee, puede crear sus propias reglas haciendo clic en 'Regla personalizada'.

5.3 Filtros de direcciones IP

Esta opción realiza acciones contrarias al 'Reenvío de puerto'. Mediante la aplicación de reglas, se bloquea el tráfico de datos de un cierto equipo. Esta opción le permite bloquear solicitudes de Internet basadas en números de puerto y direcciones IP.

5.4 Clientes LAN

El enrutador y módem agregará a la lista equipos que soliciten automáticamente una dirección IP. De esta forma, puede seleccionarlos en los menús 'Reenvío de puerto' y 'Filtro de direcciones IP'. Cuando use equipos con direcciones IP fijas, puede que tenga que asignar estas direcciones como un 'cliente LAN' manualmente. Puede hacer esto presentando simplemente el nombre de host y la dirección IP. La dirección MAC no es necesaria.

5.5 Filtros de puente

Este menú le permite bloquear ciertos tipos de tráfico de datos dentro de la red basándose en la dirección MAC. Esta opción está deshabilitada de forma predeterminada. Es recomendable que los usuarios noveles no usen esta opción.

5.6 Enrutamiento estático

Este menú le permite editar la tabla de enrutamiento del enrutador y módem y asignar la puerta de enlace para hosts de destino específicos.

5.7 Enrutamiento dinámico

Si habilita el enrutamiento dinámico, podrá hacer que el enrutador y módem reaccione a mensajes V1 o V2 RIP. Esta tecnología hace que el enrutador y módem busque el camino más corto a un host o subred.

¡Atención! Los proveedores holandeses normalmente no admiten el enrutamiento dinámico. Habilite esta opción únicamente cuando el proveedor la admita y se permita su uso.

6.0 Servicio de atención al cliente y soporte técnico

Este manual del usuario ha sido redactado con sumo cuidado por técnicos expertos de Eminent. Si tiene problemas al instalar o usar este producto, póngase en contacto con support@eminent-online.com.

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

Declaración de Conformidad

Para asegurar su seguridad y conformidad del producto con las directivas y leyes creadas por la Comisión de la Comunidad Europea, puede obtener una copia de la declaración de la conformidad referente a su producto enviando un e-mail a: info@eminent-online.com. Puedes enviar también una carta a:

Eminent Computer Supplies
Postbus 276
6160 AG GELEEN
Holanda

Indicar claramente 'Declaración de Conformidad' y el código de artículo del cual quisieras obtener una copia del declaración de la conformidad.



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