MANUAL DE USUARIO

EM4218 - wSURF Módem Inalámbrico ADSL2/2+

WWW.EMINENT-ONLINE.COM

EM4218 - wSURF Módem Inalámbrico ADSL2/2+

Advertencias y puntos de atención

En virtud de las leyes, directivas y normativas expuestas por el Parlamento Europeo, este dispositivo podría estar sujeto a limitaciones relativas a su uso en ciertos estados miembros de la Unión Europea. En determinados estados miembros de la Unión Europea, el uso de este producto podría estar prohibido. En la Declaración de conformidad de la última página de este documento podrá encontrar más información relacionada con esta advertencia.

Índice

On page 12 you will find the Eminent Advanced Manual for networking settings and information about home networking. (English only)

1.0 Condiciones de 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 inextricablemente 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

El dispositivo EM4218 es un módem ADSL2/2+ inalámbrico que ofrece una conexión a Internet estable e inalámbrica. El router integrado le permitirá compartir esta conexión a Internet con otros equipos, utilizando un cable de red o una conexión inalámbrica.

2.2 Contenido del paquete

El paquete contiene los siguientes artículos:

- Enrutador y módem ADSL2/2+ inalámbrico EM4218.
- Adaptador de alimentación.
- Cable telefónico modular.
- Cable de red UTP.
- CD-ROM con asistente para la instalación y manuales.
- Manual.

2.3 Explicación de los indicadores LED

PWR	*Se ilumina cuando el dispositivo EM4218 está encendido.*
WL/ACT	*Se ilumina cuando el punto de acceso inalámbrico está activo.*
LAN 1, 2, 3 y 4	*Se ilumina permanentemente cuando un equipo está conectado a uno de los puertos y parpadea si se envían o reciben datos a través de uno de los cables de red.*
ADSL	*Comienza a parpadear 30 segundos después de encender el dispositivo EM4218 y se ilumina permanentemente cuando la señal ADSL se ha detectado (solamente si está conectado a un cable telefónico con una señal ADSL activa).*
PPP	*Si se ha configurado la conexión PPPoE o PPPoA, este LED permanecerá encendido si la conexión funciona correctamente.*

3.0 Usar el asistente para la instalación

La forma más sencilla instalar el dispositivo EM4218 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 suministrado, puede continuar con el capítulo 4.

1. Encienda su PC.
2. Coloque el CD-ROM en la unidad de CD-ROM o DVD de su PC.
3. El software se iniciará automáticamente.
4. Siga los pasos que se indican en la pantalla hasta que la instalación se haya realizado. Ahora ya tiene una conexión a Internet operativa.

4.0 Instalación manual

Cuando instale manualmente el dispositivo EM4218 es importante que el explorador de Internet y la red estén correctamente configurados. A menos que la haya cambiado, la configuración es correcta. Consulte el manual del CD-ROM si tiene dudas sobre la configuración del explorador de Internet o de la red.

4.1 Conectar el dispositivo EM4218

1. Apague su equipo.
2. Conecte el dispositivo EM4218 a una toma de corriente eléctrica con el adaptador de alimentación suministrado.
3. Conecte el cable de teléfono al puerto ‘ADSL’ del dispositivo EM4218.
4. Conecte el otro extremo de dicho cable al divisor ADSL (no incluido).
5. Conecte un cable de red UTP a uno de los cuatro puertos ‘LAN’ del dispositivo EM4218.
6. Conecte el otro extremo del cable de red UTP al adaptador de red de su PC.

¿Está el dispositivo EM4218 correctamente conectado a la toma de corriente? Puede asegurarse de ello comprobando si el indicador LED ‘ALIM’ está iluminado.

¿He conseguido una conexión de red adecuada? Encienda su PC y compruebe si la luz (correspondiente al puerto LAN al que conectó el cable de red UTP) está iluminada. En el adaptador de red del equipo también se debe iluminar una luz.

4.2 Configurar el dispositivo EM4218 para una conexión a Internet

Para configurar el dispositivo EM4218 para una conexión a Internet, primero necesita conectar dicho dispositivo. Puede conectar el dispositivo EM4218 mediante el siguiente procedimiento:

1. Encienda el equipo.
2. Abra el explorador de Internet (por ejemplo Internet Explorer, Netscape o Firefox).
3. Escriba 'http://192.168.1.1' en la barra de direcciones.
4. Presione Entrar o haga clic en 'Ir'.
5. Escriba 'admin' en el campo 'Nombre de usuario' (recuerde que este campo es sensible a las mayúsculas).
6. Escriba 'admin' en el campo 'Contraseña' (recuerde que este campo es sensible a las mayúsculas).
7. Haga clic en 'Iniciar sesión'.
8. Se mostrará la página de presentación.

¡Sugerencia! Para evitar que personas no autorizadas obtengan acceso al dispositivo EM4218, es recomendable cambiar la contraseña.

1. *Haga clic en 'Herramientas'.*
2. *Haga clic en 'Contraseña'.*
3. *Escriba 'admin' en el campo 'Nombre de usuario'.*
4. *Escriba la contraseña actual en el campo 'Contraseña antigua'.*
5. *Escriba la contraseña nueva en el campo 'Contraseña nueva'.*
6. *Escriba la contraseña nueva de nuevo en el campo 'Confirmar contraseña'.*
7. *Haga clic en 'Enviar'.*
8. *Haga clic en 'Aceptar'.*

Anote la nueva contraseña para poder cambiar la configuración siempre que lo desee:

Nombre de usuario: admin
Contraseña: _____

4.3 Configuración para proveedores PPP

1. Haga clic en 'Asistente de instalación'.
2. Seleccione el país en el que viva en el campo 'País' (por ejemplo 'Holanda').
3. Escriba su contraseña de Internet en el campo 'ISP'.

4. Haga clic en ‘Siguiente’.
5. Introduzca su nombre de usuario de ADSL en el campo ‘Nombre de usuario’.
6. Introduzca su contraseña en el campo 'Introduzca su contraseña'.
7. Introduzca de nuevo la contraseña en el campo 'Confirme su contraseña'.
8. Haga clic en 'Guardar' para guardar la configuración y reiniciar el router EM4218.

4.4 Configuración para proveedores DHCP

1. Haga clic en ‘Asistente de instalación’.
2. Seleccione el país en el que viva en el campo 'País' (por ejemplo 'Holanda').
3. Escriba su contraseña de Internet en el campo 'ISP'.
4. Seleccione 'DHCP (Obtener una dirección IP dinámicamente desde el ISP)' en el campo 'Tipo de conexión'.
5. Haga clic en ‘Siguiente’.
6. Haga clic en 'Guardar' para guardar la configuración y reiniciar el router EM4218.

4.5 Configuración para otros proveedores

Si no puede encontrar su proveedor en la lista de asistentes, puede solicitar a su proveedor la configuración correcta. Siga los pasos siguientes para introducir la configuración en el EM4218:

1. Haga clic en 'Opciones avanzadas'.
2. Haga clic en ‘WAN’
3. Introduzca la configuración que le haya suministrado el proveedor.
4. Haga clic en ‘Agregar’.
5. Haga clic en 'Guardar' (esquina superior derecha).
6. Haga clic en ‘Aceptar’ para reiniciar el EM4218.

5.0 Proteger la red inalámbrica

Para impedir que huéspedes no invitados sondeen su red inalámbrica, le recomendamos que proteja dicha red. Puede proteger la red inalámbrica de varias formas. Para aplicar un método a la red es necesario que todos los dispositivos inalámbricos admitan dicho método. Recomendamos el uso de la forma de protección más robusta: WPA2 (WiFi Protected Access).

1. Abra el explorador de Internet (por ejemplo Internet Explorer, Netscape o Firefox).
2. Escriba ‘http://192.168.1.1’ en la barra de direcciones.
3. Presione Entrar o haga clic en ‘Ir’.
4. Escriba ‘admin’ en el campo ‘Nombre de usuario’ (recuerde que este campo es sensible a las mayúsculas).
5. Escriba ‘admin’ en el campo ‘Contraseña’ (recuerde que este campo es sensible a las mayúsculas).
6. Haga clic en 'Opciones avanzadas'.

7. Haga clic en ‘Inalámbrica’.
8. Haga clic en ‘Seguridad’
9. Si desea utilizar la protección WPA2, continúe con la sección 5.1 (recomendado). Si prefiere utilizar seguridad WEP, continúe con la sección 5.2.

La seguridad WPA2 es compatible con Windows XP y versiones más recientes. Si tiene una versión anterior de Windows, continúe con la sección 5.2.

5.1 Seguridad WPA2 (recomendada)

1. Seleccione ‘WPA2 (AES)’ en el campo ‘Cifrado’.
2. Seleccione ‘Personal (clave precompartida)’ en el campo ‘Modo de autenticación WPA’.
3. Seleccione ‘Frase de paso’ en el campo ‘Formato de clave precompartida’.
4. Introduzca una contraseña en el campo 'Clave precompartida'. Por ejemplo ‘sunombre01’. No use signos de puntuación y asegúrese de que la contraseña tiene al menos 8 caracteres de longitud.
5. Anote la contraseña elegida*.
6. Haga clic en ‘Enviar’.
7. Haga clic en ‘Guardar’ (esquina superior derecha) para guardar la configuración.

5.2 Seguridad WEP

1. Seleccione ‘WEP' en el campo ‘Cifrado’.
2. Haga clic en 'Definir clave WEP'.
3. Aparecerá una nueva pantalla.
4. Seleccione 64 o 129 bit en el campo 'Longitud de clave'.
5. Seleccione 'ASCII' o 'Hex' en el campo 'Formato de clave'.
6. Seleccione 'Clave 1' en el campo 'Clave de Tx predeterminada'.
7. Escriba una clave en el campo ‘Clave de cifrado 1’. No utilice ningún periférico y asegúrese de que la contraseña tiene exactamente 5, 10, 13 o 26 caracteres de longitud dependiendo de las otras claves.
8. Anote la contraseña elegida*.
9. Haga clic en ‘Enviar’.
10. Haga clic en ‘Guardar’ (esquina superior derecha) para guardar la configuración.

La conexión se pierde cuando la seguridad (WPA2 o WEP) se ha habilitado en el dispositivo EM4218 pero no en el adaptador de red inalámbrico. La conexión se reparará tan pronto como la configuración de seguridad se establezca en el adaptador de red inalámbrico.

**Anote el método de seguridad y la contraseña que ha usado:*
☐ *WPA2* ☐ *WEP*

Contraseña: _____

6.0 Controlar la conexión a Internet

Si desea expandir la seguridad de su red inalámbrica, puede configurar el control de direcciones MAC en su EM4218. Esta dirección MAC es un código exclusivo ligado a cada uno de los dispositivos de la red. El control de dirección MAC proporciona el medio de permitir a productos de red específicos conectarse a la red. Al resto de usuarios se les denegará el acceso. Si solamente agrega su propia dirección MAC, nadie, excepto usted, podrá conectarse a la red.

Con cierta frecuencia, la dirección MAC se puede encontrar en una pegatina en el dispositivo de la red. También puede encontrarla siguiendo estos pasos:

1. *Haga clic en 'Inicio'.*
2. *Haga clic en 'Ejecutar'.*
3. *Escriba 'CMD'.*
4. *Presione Entrar.*
5. *Escriba 'ipconfig /all'.*
6. *Presione Entrar.*
7. *La 'dirección física' es la dirección MAC.*

¡Sugerencia! Por su propia seguridad, el firewall está activado de forma predeterminada. También es recomendable instalar un antivirus y las actualizaciones con cierta frecuencia.

6.1 Control de dirección MAC: bloquear usuarios

1. Abra el explorador de Internet (por ejemplo Internet Explorer, Netscape o Firefox).
2. Escriba 'http://192.168.1.1' en la barra de direcciones.
3. Presione Entrar o haga clic en 'Ir'.
4. Escriba 'admin' en el campo 'Nombre de usuario' (recuerde que este campo es sensible a las mayúsculas).
5. Escriba 'admin' en el campo 'Contraseña' (recuerde que este campo es sensible a las mayúsculas).
6. Haga clic en 'Opciones avanzadas'.
7. Haga clic en 'Inalámbrica'.
8. Haga clic en la ficha 'Control de acceso'.
9. Seleccione 'Permitir en lista'.
10. Introduzca la dirección MAC del dispositivo de red para el que desee permitir el acceso a su red.
11. Haga clic en 'Enviar'.
12. Repita los pasos 11 y 12 si desea permitir el acceso de otros dispositivos a su red.
13. Haga clic en 'Guardar' (esquina superior derecha) para guardar la configuración.
14. Ya ha especificado a qué dispositivos de la red se les permite conectarse exclusivamente a la misma.

7.0 WDS: ampliar el alcance de la red

La función WDS resulta de gran utilidad para aumentar el alcance de la red inalámbrica y permitir que toda la red se conecte a Internet. Mediante WDS, puede ampliar el alcance instalando varios enrutadores que, mediante WDS, funcionan como repetidores y, como tales, amplían el alcance inalámbrico. Esta configuración solamente requiere una conexión a Internet. Todos los enrutadores conectados a través de WDS tienen acceso a Internet, por lo que no es necesario conectar los puertos LAN o WAN de los mismos mediante cables. WDS permite compartir de forma inalámbrica una conexión a Internet con otros enrutadores o puntos de acceso inalámbricos que admiten WDS.

7.1 Activar la función WDS en el dispositivo EM4218

A continuación se indican algunas instrucciones para usar el dispositivo WDS. En este ejemplo, se usarán dos enrutadores inalámbricos. El dispositivo EM4218 está conectado a Internet. El otro enrutador inalámbrico retransmite la señal inalámbrica.

1. Encienda el equipo.
2. Abra el explorador de Internet (por ejemplo Internet Explorer, Netscape o Firefox).
3. Escriba ‘http://192.168.1.1’ en la barra de direcciones.
4. Presione Entrar o haga clic en ‘Ir’.
5. Escriba ‘admin’ en el campo ‘Nombre de usuario’ (recuerde que este campo es sensible a las mayúsculas).
6. Escriba ‘admin’ en el campo ‘Contraseña’ (recuerde que este campo es sensible a las mayúsculas).
7. Haga clic en ‘Iniciar sesión’.
8. El router mostrará una pantalla de bienvenida.
9. Haga clic en 'Opciones avanzadas'.
10. Haga clic en ‘Inalámbrica’.
11. Haga clic en ‘Configuración’.
12. Defina la opción 'Modo' como 'WDS'.
13. Haga clic en ‘Enviar’.
14. Haga clic en ‘Aceptar’.
15. Haga clic en ‘WDS’ en el menú superior.
16. Active la opción ‘Habilitar WDS’.
17. Introduzca la dirección MAC WLAN (BSSID) del otro router en el campo 'Agregar AP WDS'. Encontrará esta dirección MAC en la parte inferior de dicho router.
18. Si no encuentra la dirección, haga clic en el botón 'Mostrar AP'. Anote el BSSID del router que desee enlazar por WDS y cierre la pantalla 'Mostrar AP'.
19. Haga clic en ‘Enviar’.
20. Si desea agregar más routers a su red WDS, repita los pasos 17 y 18 para cada router.
21. Haga clic en 'Guardar'.
22. Haga clic en ‘Aceptar’.

Para establecer una conexión WDS es necesario especificar la dirección MAC del dispositivo EM4218 en el dispositivo de recepción. Para obtener información, consulte el manual del dispositivo receptor.

Si la red inalámbrica es segura, también necesitará configurar la seguridad del otro dispositivo inalámbrico. En el modo WDS solamente se puede usar la seguridad WEP. Consulte el capítulo 5.2 para más información sobre seguridad WEP.

7.2 Cosas que debe tener en cuenta cuando use WDS

- Todos los enrutadores acoplados que usen WDS necesitan estar en el mismo intervalo de direcciones IP (por ejemplo, 192.168.1.1 para el router A y 192.168.1.200 para el router B). Puede ocurrir que necesite establecer una dirección IP fija en el dispositivo receptor.
- La seguridad WEP necesita ser idéntica en ambos dispositivos.
- Los canales de las conexiones inalámbricas necesitan ser idénticos.
- Los nombres (SSID) de las conexiones inalámbricas no necesitan ser idénticos.
- No es recomendable usar el control de dirección MAC junto con WDS.
- Los servidores DHCP del segundo (o tercer o cuarto) enrutador deban estar deshabilitados.

¡Atención! WPA no se puede usar cuando se protege la conexión.

8.0 Preguntas más frecuentes

P. Recibo el mensaje 'La dirección IP del adaptador de red no es correcta'. ¿Qué puedo hacer?

R. Este mensaje aparece cuando el equipo no recibió una dirección IP del enrutador. *Asegúrese de que todos los cables están correctamente conectados. Si es necesario, restablezca el dispositivo EM4218 e inténtelo de nuevo. Es recomendable configurar el enrutador con una conexión cableada (no inalámbrica).* Cuando la conexión cableada funcione correctamente, podrá configurar la conexión inalámbrica tal y como se explica en este manual.

P. ¿Cómo restablezco el dispositivo EM4218?

R. Para ello, siga el procedimiento que se indica a continuación:

1. Encienda el módem y espere a que se inicie.
2. Presione el botón de restablecimiento situado junto al botón de encendido / apagado durante unos veinte segundos utilizando un clip.
3. El módem se restaurará.

P. Mi señal inalámbrica es débil o inestable. ¿Cuál podría ser la causa?

R. Coloque el módem en otro lugar y observe si aumenta la fuerza de la señal. Es posible colocar el módem en un espacio abierto. El cuadro de alimentación, por ejemplo, no es un lugar adecuado para un módem inalámbrico.

R. Puede cambiar el canal del módem para ver si aumenta la fuerza de la señal. Siga las instrucciones que se indican a continuación:
   1. Abra el explorador de Internet (por ejemplo Internet Explorer, Netscape o Firefox).
   2. Escriba ‘http://192.168.1.1’ en la barra de direcciones.
   3. Presione Entrar o haga clic en ‘Ir’.
   4. Escriba ‘admin’ en el campo ‘Nombre de usuario’ (recuerde que este campo es sensible a las mayúsculas).
   5. Escriba ‘admin’ en el campo ‘Contraseña’ (recuerde que este campo es sensible a las mayúsculas).
   6. Haga clic en 'Opciones avanzadas'.
   7. Haga clic en ‘Inalámbrica’.
   8. Configure el 'Canal' en otro número, por ejemplo el 3.
   9. Haga clic en ‘Enviar’.
   10. Haga clic en 'Guardar'.
   11. Haga clic en ‘Aceptar’.

9.0 Servicio de atención al cliente y soporte técnico

Este manual de usuario ha sido elaborado cuidadosamente por técnicos expertos de Eminent. Si usted tiene problemas al instalar o utilizar el producto, por favor, rellene el formulario de soporte en la web www.eminent-online.com/support.

Eminent Advanced Manual

Table of contents

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 (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.

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

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-adresses 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

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 del 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.

EMINENT

WWW.EMINENT-ONLINE.COM

EM4218 | 03-2009