



MANUAL DE USUARIO

EM4450 - Enrutador inalámbrico

WWW.EMINENT-ONLINE.COM

EM4450 - Enrutador inalámbrico



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.

Tabla de contenido

1.0 Condiciones de la garantía	3
2.0 Introducción	3
2.1 Contenido del paquete	3
3.0 Funciones y características	3
4.0 Conectar el enrutador	4
5.0 Instalar el dispositivo EM4450 mediante el CD-ROM	4
6.0 Instalar el enrutador manualmente	5
6.1 Iniciar sesión en el dispositivo EM4450	5
6.2 Configuración para una conexión a Internet DHCP	5
6.3 Configuración para una conexión a Internet con dirección IP estática	6
6.4 Configuración para una conexión a Internet PPPoE	6
6.5 Configuración para una conexión a Internet PPTP	7
7.0 Configurar la seguridad inalámbrica	7
8.0 Proteger el enrutador manualmente	8
8.1 Establecer manualmente la seguridad WPA en el enrutador	8
8.2 Establecer manualmente la seguridad WEP en el enrutador	8
9.0 Configurar la red inalámbrica en el equipo	9
10.0 Supervisión a través de la conexión a Internet	11
10.1 Habilitar el firewall	11
10.2 Denegar el acceso a Internet mediante direcciones IP	11
10.3 Denegar el acceso a Internet mediante 'Filtro de dominios'	12
10.4 Denegar el acceso a Internet mediante 'Filtro de direcciones MAC'	12
11.0 Preguntas más frecuentes	13
12.0 Servicio de atención al cliente y soporte técnico	15

On page 16 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 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 su compra ahora en www.eminent-online.com y reciba las actualizaciones del producto!

2.1 Contenido del paquete

El paquete debe contener los siguientes componentes:

- Enrutador inalámbrico EM4450
- Adaptador de alimentación
- Cable de red UTP
- CD-ROM con asistente para la instalación y manuales
- Manual

3.0 Funciones y características

El dispositivo EM4450 es ideal para crear rápidamente su propia red inalámbrica segura. Este dispositivo es una estación inalámbrica capaz de configurar una red inalámbrica disponible desde cualquier lugar de su hogar. El dispositivo EM4450 trabaja a muy alto nivel, lo que permite crear una red inalámbrica operativa, estable y sin problemas de funcionamiento. ¡Disfrute de su red inalámbrica y deje que el dispositivo EM4450 haga todo el trabajo!

- Punto de acceso de 54 Mbps integrado para establecer una red inalámbrica.
- Enrutador integrado para compartir sin esfuerzo la conexión a Internet.
- Conmutador de 4 puertos integrado para establecer una red cableada.
- Firewall integrado para proteger los datos.

4.0 Conectar el enrutador

1. Apague su PC.
2. Conecte el dispositivo EM4450 a una toma de corriente eléctrica con el adaptador de alimentación suministrado.
3. Conecte el cable de red UTP proporcionado al puerto WAN del dispositivo EM4450.
4. Conecte el otro extremo de este cable de red UTP al puerto LAN del módem existente.
5. Conecte un cable de red UTP a uno de los cuatro puertos LAN del dispositivo EM4450.
6. Conecte el otro extremo del cable de red UTP al adaptador de red de su PC.

Sugerencia: antes de empezar a instalar el dispositivo EM4450 debe asegurarse de que el enrutador está correctamente conectado a la toma de corriente eléctrica.

Puede asegurarse de ello comprobando que el indicador LED marcado con el icono de espera universal está encendido.

Asegúrese también de que el cable de red está correctamente conectado tanto al dispositivo EM4450 como al equipo. Para comprobar esta conexión, encienda su PC y asegúrese de que el indicador LED correspondiente al puerto LAN al que conectó el cable de red UTP está iluminado.

5.0 Instalar el dispositivo EM4450 mediante el CD-ROM

El dispositivo EM4450 necesita estar configurado como enrutador inalámbrico cuando lo conecte a un módem por cable o ADSL. La forma más sencilla de configurar el dispositivo EM4450 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 manualmente. Consulte el capítulo 5.2.

1. Encienda el equipo y espere a que Windows se inicie por completo.
2. Inserte el CD-ROM en la unidad de CD-ROM o DVD.
3. El asistente se iniciará automáticamente.
4. Siga las instrucciones que aparezcan en la pantalla hasta completar la instalación. Ahora ya debe tener una conexión a Internet operativa.

Sugerencia: si el CD-ROM de instalación no se inicia automáticamente, también puede iniciar el programa de instalación manualmente. Siga las instrucciones que se indican a continuación:

1. Haga clic en 'Inicio'.
2. Haga clic en 'Ejecutar'.
3. Escriba `x:\wizard\wizard.exe` (donde *x* es la letra de la unidad de CD-ROM o DVD).
4. Haga clic en 'Aceptar'.

6.0 Instalar el enrutador manualmente

Ahora revisaremos los diferentes métodos de configuración del dispositivo EM4450. Si tiene un proveedor que requiere uno de estos métodos, solamente tiene que seguir las instrucciones adjuntas para conectarse usted mismo de forma rápida y segura.

@Home, Zeelandnet, Casema Wanadoo y UPC Chello son algunos ejemplos de proveedores que usan el método de conexión DHCP.

6.1 Iniciar sesión en el dispositivo EM4450

Si desea configurar el dispositivo EM4450 manualmente es importante que el explorador de Internet y los parámetros de la red estén perfectamente configurados. Esta configuración es correcta de forma predeterminada a menos que la cambiara en el pasado.

¡Sugerencia! 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.

Puede conectarse manualmente al dispositivo EM4450 siguiendo las instrucciones que se indican a continuación.

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 del nombre de usuario.
6. Escriba 'admin' en el campo de la contraseña.
7. Haga clic en 'Aceptar'.
8. Se mostrará la página de presentación.

¡Nota! Para poder configurar el dispositivo EM4450 para el proveedor, primero tiene que establecer el método de conexión que usa el proveedor ('DHCP', 'PPPoE', 'StaticIP' o 'PPTP'). Consulte la información que le ha enviado su proveedor.

6.2 Configuración para una conexión a Internet DHCP

1. Haga clic en 'Red' en el menú de la izquierda.

2. Haga clic en 'WAN' en el menú de la izquierda.
3. Establezca la opción 'Dirección IP dinámica'.
4. Escriba el nombre de host que le proporcionó su proveedor en el campo 'Nombre de host'. Por ejemplo: CC1234567-a (solamente para una conexión a Internet @Home).
5. Haga clic en 'Clonar MAC' en el menú de la izquierda. (Solamente es necesario si su proveedor usa registro de direcciones MAC.)
6. Haga clic en el botón 'Clonar MAC'.
7. Haga clic en 'Guardar'.
8. Cierre el explorador de Internet.
9. Deje que transcurran 5 minutos y tendrá una conexión a Internet operativa.

¡Sugerencia! Si tiene un proveedor de cable como @Home, consulte el capítulo 11 si no consigue establecer correctamente una conexión operativa en 5 minutos.

6.3 Configuración para una conexión a Internet con dirección IP estática

1. Haga clic en 'Red' en el menú de la izquierda.
2. Haga clic en 'WAN' en el menú de la izquierda.
3. Seleccione 'Dirección IP estática'.
4. Escriba la dirección IP que le proporcionó su proveedor en el campo 'Nombre de dirección IP'.
5. Escriba la máscara de subred que le proporcionó su proveedor en el campo 'Máscara de subred'.
6. Escriba la dirección de la puerta de enlace que le proporcionó su proveedor en el campo 'Puerta de enlace'.
7. Escriba la dirección DNS primaria que le proporcionó su proveedor en el campo 'DNS primario'.
8. Escriba la dirección DNS secundaria que le proporcionó su proveedor en el campo 'DNS secundario'. Si no recibió una dirección DNS secundaria, puede dejar este campo en blanco.
9. Haga clic en 'Guardar'.
10. Cierre el explorador de Internet.
11. Deje que transcurran 5 minutos y tendrá una conexión a Internet operativa.

6.4 Configuración para una conexión a Internet PPPoE

1. Haga clic en 'Red' en el menú de la izquierda.
2. Haga clic en 'WAN' en el menú de la izquierda.
3. Seleccione 'PPPoE'.
4. Escriba el nombre de usuario que le proporcionó su proveedor en el campo 'Nombre de usuario'.
5. Escriba la contraseña que le proporcionó su proveedor en el campo 'Contraseña'.
6. Haga clic en 'Guardar'.

7. Cierre el explorador de Internet.
8. Deje que transcurran 5 minutos y tendrá una conexión a Internet operativa.

6.5 Configuración para una conexión a Internet PPTP

1. Haga clic en 'Red' en el menú de la izquierda.
2. Haga clic en 'WAN' en el menú de la izquierda.
3. Seleccione 'PPTP'.
4. Escriba el nombre de usuario que le proporcionó su proveedor en el campo 'Nombre de usuario'.
5. Escriba la contraseña que le proporcionó su proveedor en el campo 'Contraseña'.
6. Escriba la dirección de la puerta de enlace del módem ADSL en el campo 'Nombre o dirección IP del servidor' (para módems Speedtouch Home, 10.0.0.138 es el valor predeterminado).
7. Escriba la dirección IP del módem ADSL en el campo 'Dirección IP' (para módems Speedtouch Home, 10.0.0.138 es el valor predeterminado).
8. Escriba la máscara de subred del módem ADSL en el campo 'Máscara de subred' (para módems Speedtouch Home, 255.255.255.0 es el valor predeterminado).
9. Escriba la dirección de la puerta de enlace del módem ADSL en el campo 'Puerta de enlace' (para módems Speedtouch Home, 10.0.0.138 es el valor predeterminado).
10. Haga clic en 'Guardar'.
11. Cierre el explorador de Internet.
12. Deje que transcurran 5 minutos y tendrá una conexión a Internet operativa.

7.0 Configurar la seguridad inalámbrica

Dado que personas no autorizadas también pueden recibir la señal de una red inalámbrica, es recomendable proteger la red. Existen varios métodos de seguridad que pueden proteger la red a diferentes niveles. Para usar uno de los métodos, es obligatorio que todos los dispositivos de la red inalámbrica admitan dicho método. El método más seguro es WPA (WiFi Protected Access, es decir, Acceso protegido WiFi).

La forma más sencilla de proteger la red es usar el asistente para la instalación que se encuentra en el CD-ROM, tal y como se describe a continuación. Si no desea usar el CD-ROM para proteger la red, también puede establecer el uso de la página Web, tal y como se describe en el capítulo 8.

1. Encienda el equipo y espere a que Windows se inicie por completo.
2. Inserte el CD-ROM en la unidad de CD-ROM o DVD.
3. El asistente se iniciará automáticamente.
4. Elija su idioma y haga clic en 'Siguiente'.
5. Seleccione 'Configurar la seguridad inalámbrica' y haga clic en 'Siguiente'.

6. Siga las instrucciones que aparezcan en la pantalla hasta completar la instalación. Ahora ya debe tener una red inalámbrica segura.

¡Nota! La seguridad WPA se admite en Windows 2000 o superior. ¡Este método de seguridad no se puede usar con Windows 98 ni ME! Si no tiene Windows Vista, XP o Windows 2000, use la seguridad WEP.

8.0 Proteger el enrutador manualmente

Aparte de usar el CD-ROM, también puede establecer la seguridad manualmente. En este capítulo se explica cómo hacerlo. Eminent recomienda usar el cifrado WPA, ya que ofrece la máxima seguridad en la red inalámbrica.

8.1 Establecer manualmente la seguridad WPA en el enrutador

1. Encienda el equipo.
2. Abra el explorador de Internet (por ejemplo Internet Explorer, Netscape o Firefox).
3. Borre el contenido de la barra de direcciones y, a continuación, escriba 'http://192.168.1.1'.
4. Presione Entrar o haga clic en 'Ir'.
5. Escriba 'admin' en el campo del nombre de usuario.
6. Escriba 'admin' en el campo de la contraseña.
7. Haga clic en 'Aceptar'.
8. Se mostrará la página de presentación.
9. Haga clic en 'Inalámbrica' en el menú de la izquierda.
10. Haga clic en 'Configuración inalámbrica' en el menú de la izquierda.
11. Active la opción 'Habilitar la seguridad inalámbrica'.
12. Seleccione el método de seguridad que prefiera junto a 'Tipo de seguridad'. En este caso, elija WPA-PSK/WPA2-PSK.
13. Elija WPA-PSK junto al campo 'Opción de seguridad'.
14. Elija TKIP junto al campo 'Cifrado'.
15. Vaya a 'Clave PSK'. Aquí puede escribir un código de seguridad. Puede usar tanto números como letras. Recuerde que una clave WPA debe tener entre 8 y 63 caracteres. Puede que desee anotar el código.
16. Haga clic en 'Guardar'.
17. Haga clic en 'Aceptar' y, a continuación, en 'Aceptar' una vez más. El enrutador guardará ahora la configuración.

8.2 Establecer manualmente la seguridad WEP en el enrutador

1. Encienda el equipo.

2. Abra el explorador de Internet (por ejemplo Internet Explorer, Netscape o Firefox).
3. Borre el contenido de la barra de direcciones y, a continuación, escriba 'http://192.168.1.1'.
4. Presione Entrar o haga clic en 'Ir'.
5. Escriba 'admin' en el campo del nombre de usuario.
6. Escriba 'admin' en el campo de la contraseña.
7. Haga clic en 'Aceptar'.
8. Se mostrará la página de presentación.
9. Haga clic en 'Inalámbrica' en el menú de la izquierda.
10. Haga clic en 'Configuración inalámbrica' en el menú de la izquierda.
11. Active la opción 'Habilitar la seguridad inalámbrica'.
12. Seleccione el método de seguridad que prefiera junto a 'Tipo de seguridad'. En este caso, elija WEP.
13. Seleccione el tipo de clave que prefiera. Puede elegir una clave de 64 o de 128 bits.
14. Si elige 64 bits, escriba una contraseña que tenga exactamente 10 caracteres. Dicha contraseña puede contener tanto números como letras. Si usa letras, solamente se permiten los caracteres A a F. Si eligió 128 bits, escriba una contraseña que tenga exactamente 26 caracteres. Dicha contraseña también puede contener tanto números como letras. Si usa letras, solamente se permiten los caracteres A a F.
15. Necesitará esta clave posteriormente. Puede que le interese anotarla.
16. Haga clic en 'Guardar'.
17. Haga clic en 'Aceptar' y, a continuación, en 'Aceptar' una vez más. El enrutador guardará ahora la configuración.

¡Nota! Eminent le recomienda establecer la seguridad solamente mientras el enrutador esté conectado al equipo mediante un cable.

Aquí puede anotar el tipo de seguridad establecido, el nombre de la red y la clave de seguridad.

☐ WPA

☐ WEP

Nombre de la red: _____

Clave de seguridad: _____

9.0 Configurar la red inalámbrica en el equipo

Ahora que el enrutador se ha protegido tendrá que configurar el equipo, habilitándolo para que reconozca la red inalámbrica segura y se conecte a ella.

En este momento, Windows XP y Windows Vista son los sistemas operativos más utilizados. Ahora explicaremos cómo configurar una conexión inalámbrica usando estos sistemas.

Sugerencia: después de que el enrutador haya establecido WEP o WPA como método de seguridad, puede quitar el cable de red del equipo antes de llevar a cabo el paso 9.1.

9.1 Configurar una red inalámbrica en Windows XP

Para poder configurar una conexión inalámbrica en Windows XP es necesario seguir estas instrucciones:

1. Encienda el equipo.
2. Haga clic en 'Inicio'.
3. Vaya al 'Panel de control'.
4. Seleccione 'Conexiones de red'.
5. Ahora debería ver la conexión de red inalámbrica. Haga clic con el botón secundario en esta conexión.
6. Elija 'Ver redes inalámbricas disponibles'. Aparecerá una lista con las redes inalámbricas disponibles.
7. Seleccione su propia red en la lista.
8. Si hace clic en 'Conectar', su PC le advertirá de que esta red es segura y requiere una clave de red.
9. Escriba la clave de cifrado y haga clic en 'Conectar'.
10. Si la clave se ha insertado correctamente, después de un breve período de tiempo Windows le indicará que está conectado a la red. Ahora está conectado.

9.2 Configurar una red inalámbrica en Windows Vista

Para poder configurar una conexión inalámbrica en Windows Vista es necesario seguir estas instrucciones:

1. Haga clic en 'Inicio'.
2. Vaya al 'Panel de control'.
3. Seleccione 'Conexiones de red e Internet'.
4. Vaya a 'Centro de red'.
5. Elija 'Administrar redes inalámbricas' en la parte izquierda del menú.
6. Haga clic en 'Agregar'.
7. Elija 'Agregar una red en el alcance de este equipo' en la pantalla siguiente.
8. En esta ventana puede seleccionar su propia red.
9. Haga clic en 'Conectar'.
10. El equipo mostrará este mensaje: 'Escriba la clave de seguridad de red o frase de contraseña para...'. Escriba la clave de cifrado.
11. Haga clic en 'Conectar'. Si la clave se ha especificado correctamente, el equipo se conectará.

10.0 Supervisión a través de la conexión a Internet

El dispositivo EM4450 está equipado con un firewall avanzado. Esta función permite una supervisión prácticamente completa a través de la conexión a Internet. El firewall le permite definir configuraciones que temporalmente deshabilitan a los equipos para crear una conexión a Internet. También puede bloquear sitios Web. Este bloqueo se puede hacer temporalmente, de forma permanente o durante períodos específicos de tiempo, como por ejemplo durante el horario laboral.

10.1 Habilitar el firewall

Para configurar correctamente el firewall, primero es necesario habilitarlo. Siga estas instrucciones:

1. Abra el explorador de Internet (por ejemplo Internet Explorer, Netscape o Firefox).
2. Borre el contenido de la barra de direcciones y, a continuación, escriba 'http://192.168.1.1'.
3. Presione Entrar o haga clic en 'Ir'.
4. Escriba 'admin' en el campo del nombre de usuario.
5. Escriba 'admin' en el campo de la contraseña.
6. Haga clic en 'Aceptar'.
7. Se mostrará la página de presentación.
8. En 'Configuración avanzada', haga clic en 'Seguridad' en la parte izquierda de la pantalla.
9. Active la opción 'Habilitar firewall'.
10. Haga clic en 'Guardar'.
11. El firewall está ahora habilitado.

10.2 Denegar el acceso a Internet mediante direcciones IP

El firewall permite denegar el acceso de cualquier equipo a Internet en función de su dirección IP. Para usar esta opción es necesario habilitar la opción 'Filtro de direcciones IP'. Para habilitar esta opción, siga las instrucciones del capítulo 10.1. En el paso 8, active la opción 'Habilitar filtro de direcciones IP', seguido por los pasos 9 y 10.

1. En 'Configuración avanzada', haga clic en 'Filtro de direcciones IP' en la parte izquierda de la pantalla.
2. Haga clic en 'Agregar nuevo' en la siguiente sección.
3. Escriba los datos que desee en esta ventana.
4. Haga clic en 'Tiempo efectivo'.

En este campo puede especificar el intervalo de tiempo en el que se deniega el acceso a Internet. Si desea denegar el acceso a Internet desde las 10 en punto de la mañana hasta las 8 en punto de la tarde, escriba 1000 en el campo 'Tiempo efectivo' y 2000 en el segundo campo.

5. Escriba la dirección IP del equipo al que desea denegar el acceso a Internet en el campo 'Dirección IP LAN'. Por ejemplo '192.168.1.5'.
6. Elija 'Denegar' junto a 'Acción'.
7. Haga clic en 'Guardar'.
8. A partir de ahora, será imposible que el equipo que está usando esta dirección IP específica obtenga acceso a Internet durante el período de tiempo que especificó.

Sugerencia: en el capítulo 11 se explica cómo obtener la dirección IP de un equipo.

10.3 Denegar el acceso a Internet mediante 'Filtro de dominios'

El dispositivo EM4450 le permite denegar el acceso a ciertos dominios o sitios Web. Si no quiere que sus hijos vean ciertos sitios, puede configurar un filtro. Para usar esta opción, siga las mismas instrucciones que en el capítulo 10.1. Solamente ahora, active la opción 'Habilitar filtro de dominios' y continúe con los pasos 9 y 10.

1. Haga clic en 'Filtro de dominios' en la pantalla de la izquierda.
2. Haga clic en 'Agregar nuevo'.
3. Haga clic en 'Tiempo efectivo'.

En este campo puede especificar el intervalo de tiempo en el que se deniega el acceso a Internet. Si desea denegar el acceso a Internet desde las 10 en punto de la mañana hasta las 8 en punto de la tarde, escriba 1000 en el campo 'Tiempo efectivo' y 2000 en el segundo campo.

4. Escriba el dominio o sitio Web al que desee denegar el acceso durante el intervalo de tiempo especificado en el campo 'Nombre de dominio'. Por ejemplo, si desea denegar el acceso a www.google.com, escriba esta dirección en el campo 'Nombre de dominio'.
5. Active la opción 'Habilitado' en el campo 'Estado'.
6. Haga clic en 'Guardar'.
7. A partir de ese momento es imposible alcanzar este dominio o sitio Web durante el intervalo de tiempo especificado.

10.4 Denegar el acceso a Internet mediante 'Filtro de direcciones MAC'

Además de los métodos para restringir el acceso a Internet explicados anteriormente, hay una forma similar de denegar el acceso a Internet. Este método también es el

más efectivo. El acceso a Internet se bloquea por completo y no tiene que especificar un intervalo de tiempo. Para habilitar esta opción, siga las instrucciones del capítulo 10.1. Solamente ahora, active la opción 'Habilitar filtro de direcciones MAC' en el paso 8 y continúe con los pasos 9 y 10.

1. Haga clic en 'Filtro de direcciones MAC' en la pantalla de la izquierda.
2. Haga clic en 'Agregar nuevo'.
3. Inserte la dirección MAC específica en el campo 'Dirección MAC'.
4. En el campo 'Descripción' puede especificar una breve descripción como, por ejemplo, el nombre de quien ha establecido el bloqueo.
5. Active la opción 'Habilitado' en el campo 'Estado'.
6. Haga clic en 'Guardar'.
7. A partir de ahora, el acceso a Internet se ha bloqueado completamente para la dirección MAC especificada.

Sugerencia: en el capítulo 11 se explica cómo obtener la dirección MAC de un equipo.

11.0 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 EM4450 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: He configurado el enrutador. Todo parece correcto pero no puedo obtener acceso a Internet. Mi proveedor es Chello.

R: Asegúrese de que ha seleccionado la dirección MAC correcta durante la configuración. Si eligió la dirección MAC incorrecta, no habrá conexión a Internet.

P: He configurado el enrutador. Todo parece correcto pero no puedo obtener acceso a Internet. Mi proveedor es Chello, @Home, Casema u otro proveedor DHCP.

R: Algunas veces, el módem no concede acceso a Internet al enrutador. Siga las instrucciones siguientes para obtener acceso a Internet:

1. Apague tanto el enrutador como el módem.
2. Espere 10 minutos.
3. Encienda el módem, espere a que se haya iniciado completamente, encienda el enrutador y déjelo también que se inicie por completo.
4. Ahora la conexión debe funcionar correctamente.

P: Intenté llevar a cabo la solución explicada anteriormente, pero la conexión a Internet sigue sin funcionar. ¿Qué puedo hacer?

R: Existe otro método:

1. Inicie sesión en la página Web del enrutador con <http://192.168.1.1>.
2. Nombre de usuario: admin. Contraseña: admin
3. Ahora ha iniciado sesión en la página principal del dispositivo EM4450.
4. Desconecte el cable coaxial del módem.
5. En la sección 'WAN' de la página del enrutador, haga clic en 'Renovar'.
6. Una dirección IP del módem aparecerá en la pantalla. Esta dirección suele tener el siguiente formato: 192.168.100.x
7. Vuelva a conectar el cable coaxial al módem y espere a que el LED de conexión a Internet se ilumine.
8. Haga clic en 'Renovar' en la página del enrutador.
9. Una dirección IP, que le ha proporcionado su proveedor, debe aparecer ahora en la pantalla. Si es así, estará conectado.

P: Quiero saber mi dirección IP. ¿Cómo obtengo esta dirección?

R: Para obtener la dirección IP, siga las instrucciones que se indican a continuación.

Instrucciones para Windows XP/2000 y Windows Vista:

1. Haga clic en 'Inicio'.
2. Haga clic en 'Ejecutar'.
3. Escriba 'cmd'.
4. Presione la tecla 'Entrar' o haga clic en 'Aceptar'.
5. Escriba 'ipconfig'.
6. Presione la tecla 'Entrar'.
7. Ahora aparecerá la dirección IP.

Instrucciones para Windows 98/ME:

1. Haga clic en 'Inicio'.
2. Haga clic en 'Ejecutar'.
3. Escriba 'winipcfg'.
4. Presione la tecla 'Entrar' o haga clic en 'Aceptar'.
5. Ahora aparecerá la dirección IP o la dirección personal automática.

P: Quiero saber la dirección MAC de mi adaptador de red. ¿Cómo puedo obtener esta dirección?

R: Para obtener la dirección MAC del adaptador de red, siga las instrucciones que se indican a continuación:

Instrucciones para Windows XP/2000 y Windows Vista:

1. Haga clic en 'Inicio'.
2. Haga clic en 'Ejecutar'.
3. Escriba 'cmd'.
4. Presione la tecla 'Entrar' o haga clic en 'Aceptar'.
5. Escriba 'ipconfig /all'.
6. Presione la tecla 'Entrar'.

7. Ahora aparecerá la dirección física. Se trata de la dirección MAC del adaptador de red.

Instrucciones para Windows 98/ME:

1. Haga clic en 'Inicio'.
2. Haga clic en 'Ejecutar'.
3. Escriba 'winipcfg'.
4. Presione la tecla 'Entrar' o haga clic en 'Aceptar'.
5. Ahora aparecerá la dirección del adaptador. Se trata de la dirección MAC del adaptador de red.

P: ¿Cómo restablezco el dispositivo EM4450?

R: Puede restablecer el dispositivo EM4450 desconectando el adaptador de alimentación del enrutador. Use un prendedor para presionar el botón de restablecimiento. Vuelva a conectar el adaptador de alimentación al dispositivo EM4450 mientras mantiene presionado el botón de restablecimiento. El LED 'Sistema' se iluminará. Espere hasta que empiece a parpadear. Suelte el botón de restablecimiento. El dispositivo EM4450 se habrá restablecido y habrá recuperado la configuración de fábrica.

12.0 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.....	16
Why an Eminent advanced manual?	17
Your tips and suggestions in the Eminent Advanced Manual?.....	17
Service and support	17
Networking settings for Windows 98 and Windows ME)	17
Networking settings (Windows 2000 and Windows XP).....	18
Configuring Internet Explorer 5 and 5.5.....	19
Configuring Internet Explorer 6.....	19
DHCP, Automatic allocation of ip-addresses	20
Translating ip-adresses and domain names	20
Using a single ip-address for your entire network	20
Security for your computer and your network.....	21
Making a computer available for Internet users in your network.....	21
Simplifying network management.....	22
Blocking websites with explicit content	22
Checking data traffic at package level	22
Blocking a complete domain.....	23
Carrying out actions based on date or time.....	23
A safe remote connection.....	23
Remote network management.....	23
Allocating or blocking network access	23
Making your wireless network secure	24
Expanding the range of your wireless network.....	24
Index	26

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

Access blocks	23	Online games	21
Access Point	<i>See</i> Range Extender	Operating system	22
Administrator	23	Package filter	
Application.....	22	Packet inspection	22
ASCII.....	24	Packet inspection	22
Block	22	Parental Control	23
Bridging.....	<i>See</i> WDS	Plug & Play.....	22
Business network	23	Policies.....	22. <i>See</i> Rules
Data traffic.....	23	Pool.....	20
DDNS		Port Triggering.....	22
Dynamic DNS.....	<i>See</i> DNS	Ports.....	21
DHCP		Pre Shared Key (PSK).....	24
Dynamic Host Configuration		Private IP addresses	20
Protocol	20	Programming language	22
DMZ		Public IP address	20
DeMilitarized Zone	21	Range	24
DNS		Range Extender	25
Domain Name System.....	20	Rules.....	22
Domain.....	23	Schedule Rule.....	22
Domain Filter.....	23	SNMP	
Domain name	20	Simple Network Management	
Dynamic.....	20	Protocol	23
Dynamic DNS.....	20	Tunnel	23
Explicit content	22	UPnP	
Firewall.....	17	Universal Plug and Play.....	22
Firewall software solution	21	URL Blocking	22
Gatekeeper	22	Virtual Server	23
Hardware	21	Viruses	21
Hexadecimal	23	VPN	
Key.....	24	Virtual Private Networking	23
Key words		WDS	
Catchwords	22	Wireless Distribution System	24
MAC address	23	WEP encryption.....	24
Name resolution	20	Wi-Fi Protected Access	<i>See</i> WPA
NAT		WPA.....	24
Network Address Translation.....	20	WPA2.....	24

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