EMINENT

MANUAL

EM4450 - Wireless Router

WWW.EMINENT-ONLINE.COM

EM4450 - Wireless Router

Warnings and points of attention

Due to laws, directives and regulations set out by the European Parliament, this device could be subject to limitations concerning its use in certain European member states. In certain European member states the use of this product could be prohibited. More information regarding this warning can be found in the Declaration of Conformity on the last page of this document.

Table of contents

On page 15 you will find the Eminent Advanced Manual for networking settings and information about home networking.

1.0 Warranty conditions

The five-year Eminent warranty applies to all Eminent products unless mentioned otherwise before or during the moment of purchase. When having bought a second-

hand Eminent product the remaining period of warranty is measured from the moment of purchase by the product's first owner. The Eminent warranty applies to all Eminent products and parts inextricably connected to and/or mounted on the main product. Power supply adapters, batteries, antennas and all other products not integrated in or directly connected to the main product and/or products of which, without reasonable doubt, can be assumed that wear and tear show a different pattern than the main product are not covered by the Eminent warranty. Products are not covered by the Eminent warranty when subjected to incorrect/improper use, external influences and/or when opened by parties other than Eminent.

2.0 Introduction

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

Register your purchase now on www.eminent-online.com and receive product updates!

2.1 Packing contents

The following parts need to be present in the packing:

- EM4450, wireless router.
- Power adapter.
- UTP network cable.
- CD-rom with installation wizard and manuals.
- Manual.

3.0 Functions and features

The EM4450 is ideal for quickly creating your own secured wireless network. The EM4450 is a wireless station, able to setup a wireless network available from every point in your house. The EM4450 performs on a very high level which enables you to build a stable and smoothly operating wireless network. Enjoy your network and let the EM4450 do all the work

- Built in 54Mbps access point for establishing a wireless network.
- Built in router for effortlessly sharing your internet connection.
- Built in 4 port switch for establishing a wired network.
- Built in Firewall to protect your data.

4.0 Connecting the router

1. Turn off your computer.
2. Connect the EM4450 to a power outlet using the provided power adapter.
3. Connect the provided UTP network cable to the WAN port of the EM4450.
4. Connect the other end of this UTP network cable to the LAN port of your existing modem.
5. Connect a UTP network cable to one of the four LAN ports of your EM4450.
6. Connect the other end of this UTP network cable to the network adapter of your computer.

Hint: Before you begin installing the EM4450 you need to make sure the router is correctly connected to the power outlet. You can check this by verifying that the LED marked with the universal stand-by icon is lit.
Also make sure your network cable is correctly connected to both the EM4450 and your computer. To check this, start up your computer and make sure the LED that corresponds with the LAN port to which you connected the UTP network cable is lit.

5.0 Installing the EM4450 using the CD-rom

The EM4450 needs to be configured as a wireless router when connecting it to a cable or ADSL modem. The easiest way to configure the EM4450 is by using the installation wizard, as explained in this chapter. If you do not wish to use the wizard on the CD-rom, you can also configure the router manually. See chapter 5.2.

1. Turn on your computer and wait until Windows has completely started up.
2. Insert the CD-rom into the CD-rom or DVD drive.
3. The wizard will automatically start.
4. Follow the on-screen instructions until the installation is complete. You should now have a working Internet connection.

Hint: If the installation CD-rom does not start automatically, you can also start the installation program manually. Follow the instructions below:
1. *Click 'Start'.*
2. *Click 'Run'.*
3. *Type x:\wizard\wizard.exe (x is the drive letter of your CD-rom or DVD station).*
4. *Click 'OK'.*

6.0 Manually installing the router

We will now review the different methods of setting up your EM4450. If you have a provider that requires one of these methods you will only need to follow the accompanying instructions to get yourself online fast and safe!

Examples of providers that use the DHCP connection method are: @Home, Zeelandnet, Casema Wanadoo and UPC Chello

6.1 Logging into the EM4450

If you wish to manually configure the EM4450 it is important that your Internet browser and network settings are configured correctly. The settings are correct by default, unless you made changes in the past.

Hint! If you are not sure about the settings of your Internet browser and network, consult the Eminent Advanced Manual on the CD-rom.

You can manually connect to the EM4450 by following the instructions below.

1. Turn on your computer.
2. Open your Internet browser (for instance Internet Explorer, Netscape or Firefox).
3. Enter 'http://192.168.1.1' in the address bar.
4. Press Enter or click 'Go to'.
5. Type 'admin' in the username field.
6. Type 'admin' in the password field.
7. Click 'Ok'.
8. The opening page is shown.

Note! To be able to configure the EM4450 for your provider you will first need to establish which connection method your provider uses ('DHCP', 'PPPoE', 'StaticIP' or 'PPTP'). Consult the information you have received from your provider.

6.2 Configuration for a DHCP Internet connection

1. Click 'Network' in the left menu.
2. Click 'WAN' in the left menu.
3. Select 'Dynamic IP'.
4. Enter the hostname you received from your provider in the 'Hostname' field. For instance: CC1234567-a (Only for an @Home Internet connection).
5. Click 'MAC Clone' in the left menu. (Required only if your provider uses MAC address registration.)
6. Click the 'Clone MAC' button.
7. Click 'Save'.
8. Close your Internet browser.
9. Within 5 minutes you will have a working Internet connection.

Hint! If you have a cable provider such as @Home, see chapter 11 if you do not succeed in establishing a working connection within 5 minutes.

6.3 Configuration for a Static IP Internet connection

1. Click ‘Network’ in the left menu.
2. Click ‘WAN’ in the left menu.
3. Select ‘Static IP’.
4. Enter the IP address you received from your provider in the ‘IP Address’ field.
5. Enter the subnet mask you received from your provider in the ‘Subnet Mask’ field.
6. Enter the gateway address you received from your provider in the ‘Gateway’ field.
7. Enter the primary DNS address you received from your provider in the ‘Primary DNS’ field.
8. Enter the secondary DNS address you received from your provider in the ‘Secondary DNS’ field. If you did not receive a secondary DNS address you can leave this field blank.
9. Click ‘Save’.
10. Close your Internet browser.
11. Within 5 minutes you will have a working Internet connection.

6.4 Configuration for a PPPoE Internet connection

1. Click ‘Network’ in the left menu.
2. Click ‘WAN’ in the left menu.
3. Select ‘PPPoE’.
4. Enter the username you received from your provider in the ‘User Name’ field.
5. Enter the password you received from your provider in the ‘Password’ field.
6. Click ‘Save’.
7. Close your Internet browser.
8. Within 5 minutes you will have a working Internet connection.

6.5 Configuration for a PPTP Internet connection

1. Click ‘Network’ in the left menu.
2. Click ‘WAN’ in the left menu.
3. Select ‘PPtP’.
4. Enter the username you received from your provider in the ‘User Name’ field.
5. Enter the password you received from your provider in the ‘Password’ field.
6. Enter the gateway address of your ADSL modem in the ‘Server IP Address/Name’ field (For Speedtouch Home modems this is 10.0.0.138 by default).
7. Enter the IP address of your ADSL modem in the ‘IP Address’ field (For Speedtouch Home modems this is 10.0.0.150 by default).
8. Enter the subnet mask of your ADSL modem in the ‘Subnet Mask’ field (For Speedtouch Home modems this is 255.255.255.0 by default).

9. Enter the gateway address of your ADSL modem in the ‘Gateway’ field (For Speedtouch Home modems this is 10.0.0.138 by default).
10. Click ‘Save’.
11. Close your Internet browser.
12. Within 5 minutes you will have a working Internet connection.

7.0 Wireless security configuration

Because unauthorized people can also receive the signal of a wireless network it is recommended you secure your network. There are several security methods that can secure your network on different levels. To use a method it is mandatory that all wireless network devices support this method. The strongest method is WPA (WiFi Protected Access).

The easiest way to secure your network is by using the installation wizard on the CD-rom as outlined below. If you do not wish to use CD-rom to secure your network, you can also set the using the web page, as described in chapter 8.

1. Turn on your computer and wait until Windows has completely started up.
2. Insert the CD-rom into the CD-rom or DVD drive.
3. The wizard will automatically start.
4. Choose your language and click ‘Next’.
5. Select ‘Configure wireless security’ and click ‘Next’.
6. Follow the on-screen instructions until the installation is complete. You should now have a secured wireless network.

Note! WPA security is supported by Windows 2000 or higher. This security method can not be used with Windows 98 and ME! If you do not have Windows Vista, XP or Windows 2000, then use WEP security.

8.0 Manually securing the router

Apart from using the CD-rom, you can also set the security manually. This chapter explains how to accomplish this. Eminent suggests using WPA encryption, as it offers the most security on your wireless network.

8.1 Manually setting WPA security in the router

1. Turn on your computer.
2. Open your Internet browser (for instance Internet Explorer, Netscape or Firefox).
3. Clear the address bar, then enter ‘http://192.168.1.1’
4. Press Enter or click ‘Go to’.
5. Type ‘admin’ in the username field.
6. Type ‘admin’ in the password field.
7. Click ‘Ok’.

8. The opening page is shown.
9. Click ‘Wireless’ in the left menu.
10. Click ‘Wireless Settings’ in the left menu.
11. Check ‘Enable Wireless Security’.
12. Select the preferred security method near ‘Security Type’, in this case WPA-PSK/WPA2-PSK
13. Choose WPA-PSK near the ‘Security Option’ field.
14. Choose TKIP near the ‘Encryption’ field.
15. Go to ‘PSK Pass phrase’. Here you can enter a security code. You can use both numbers and letters. Keep in mind that a WPA key requires at least 8 characters and has a maximum of 63 characters. You may want to write down the code.
16. Click ‘Save’.
17. Click ‘OK’, then click ‘OK’ again. The router will now save the settings.

8.2 Manually setting WEP security in the router

1. Turn on your computer.
2. Open your Internet browser (for instance Internet Explorer, Netscape or Firefox).
3. Clear the address bar, then enter ‘http://192.168.1.1’.
4. Press Enter or click ‘Go to’.
5. Type ‘admin’ in the username field.
6. Type ‘admin’ in the password field.
7. Click ‘Ok’.
8. The opening page is shown.
9. Click ‘Wireless’ in the left menu.
10. Click ‘Wireless Settings’ in the left menu.
11. Check ‘Enable Wireless Security’.
12. Select the preferred security method near ‘Security Type’, in this case WEP.
13. Select the preferred Key Type: You can choose between 64bit or 128bit.
14. If you chose 64bit, enter a password consisting of exactly 10 characters. These can be both numbers and letters. If you use letters, you can only use A to F. If you chose 128bit, enter a password consisting of exactly 26 characters. These can also be both numbers and letters. If you use letters, you can only use A to F.
15. You will need this key later on. You may want to write it down.
16. Click ‘Save’.
17. Click ‘OK’, then click ‘OK’ again. The router will now save the settings.

Note! Eminent recommends you to set the security only while the router is connected to the computer using a cable.

Here you can write down the security type you set, the network name and the security key.

☐ *WPA* ☐ *WEP*

Network name: _____

Security key: _____

9.0 Configuring the wireless network on the computer

Now that the router has been secured you will need to configure the computer, enabling it to recognize and connect to the secured wireless network.
Windows XP and Windows Vista are at this moment the most commonly used operating systems. We will explain how to setup a wireless connection using these systems.

Hint: After the router has been set to WEP or WPA security you can remove the network cable from your computer before proceeding with step 9.1.

9.1 Configuring a wireless network under Windows XP

To be able to setup a wireless connection under Windows XP you will need to follow these instructions:

1. Turn on your computer.
2. Click 'Start'.
3. Go to 'Control Panel'.
4. Select 'Network Connections'.
5. You should now be able to see your wireless network connection. Right click this connection.
6. Choose 'View available wireless networks'. A list with available wireless networks will now be shown.
7. Select your own network from this list.
8. If you click 'Connect' your computer will warn you that this network is secured and requires a network key.
9. Enter the encryption key and click 'Connect'.
10. If the key has been entered correctly, after a short amount of time Windows will tell you that you are connected to the network. You are now online.

9.2 Configuring a wireless network under Windows Vista

To be able to setup a wireless connection under Windows Vista you will need to follow these instructions:

1. Click 'Start'.
2. Go to 'Control Panel'.
3. Select 'Network and Internet Connections'.
4. Go to 'Network Centre'.

5. Choose ‘Manage Wireless Networks’ in the left part of the menu.
6. Here you need to click ‘Add’.
7. In the next screen choose ‘Add a network that is in range of this computer’.
8. In this window you can select your own network.
9. Click ‘Connect’
10. Your computer will show this message: ‘Type the network security or pass phrase for ….. ’. Enter your encryption key.
11. Click ‘Connect’. If the key has been entered correctly, your computer will be connected and you will be online.

10.0 Supervision over the Internet connection

The EM4450 is equipped with an advanced firewall. This allows an almost complete supervision over the Internet connection. The firewall enables you to make settings which temporarily disable computers to make a connection to the Internet. You can also block websites. This can be done temporarily, permanently or for specific time periods, such as during office hours.

10.1 Enabling the firewall

To correctly configure the firewall we will first need to enable it. Follow these instructions:

1. Open your Internet browser (for instance Internet Explorer, Netscape or Firefox).
2. Clear the address bar and enter ’http://192.168.1.1’.
3. Press Enter or click ‘Go to’.
4. Type ‘admin’ in the username field.
5. Type ‘admin’ in the password field.
6. Click ‘OK’.
7. The opening page is shown.
8. Click ‘Security’ under ‘Advanced Settings’ on the left part of the screen.
9. Check ‘Enable Firewall’.
10. Click ‘Save’.
11. The firewall is now enabled.

10.2 Denying Internet access using IP addresses

The firewall allows you to deny any computer access to the internet on bases of its IP address. To use this option you will need to enable ‘IP address filtering’. To enable this option follow the instructions as in chapter 10.1. In step 8, check ‘Enable IP address filtering’, followed by steps 9 and 10.

1. Click ‘IP Address Filtering’ under ‘Advanced Settings’ in the left part of the screen.
2. Click ‘Add New’ in the next screen.

3. Enter the required data in this Window.
4. Click 'Effective time'.

In this field you can specify the time frame in which Internet access is denied. If you want to deny Internet access from 10 o'clock in the morning to 8 o'clock in the evening, enter 1000 in the 'Effective time' field and 2000 in the second field.

5. Enter the IP address of the computer which you want to deny Internet access in the 'LAN IP Address' field. For instance '192.168.1.5'.
6. Choose 'Deny' near 'Action'.
7. Click 'Save'.
8. It is now impossible for the computer that is using this specific IP address to gain access to the Internet during the time frame as specified by you.

Hint: Chapter 11 explains how to obtain the IP address of a computer.

10.3 Denying Internet access using 'Domain Filtering'.

The EM4450 enables you to deny access to certain domains or websites. If you do not want your son or daughter to view certain sites you can configure a filter. To use this option, follow the same instructions as in chapter 10.1. Only now check 'Enable Domain Filtering' in step 8, followed by steps 9 and 10.

1. Click 'Domain Filtering' in the left screen.
2. Click 'Add New'.
3. Click 'Effective time'.

In this field you can specify the time frame in which Internet access is denied. If you want to deny Internet access from 10 o'clock in the morning to 8 o'clock in the evening, enter 1000 in the 'Effective time' field and 2000 in the second field.

4. Enter the domain or website to which you want to deny access during the specified time frame in the 'Domain Name' field. For instance, if you want to deny access to www.google.com, then enter this address in the 'Domain Name' field.
5. Check 'Enabled' in the 'Status' field.
6. Click 'Save'.
7. It is now impossible to reach this domain or website during the specified time frame.

10.4 Denying Internet access using 'MAC Address Filtering'

Apart from the methods to restrict Internet access as explained above, there is another way to deny Internet access. This method is also the most effective. Access to the Internet is completely blocked and you do not need to specify a time frame. To

enable this option, follow the instructions as in chapter 10.1. Only now check ‘Enable Mac-address filtering’ in step 8, followed by steps 9 and 10.

1. Click‘ MAC Filtering’ in the left screen.
2. Click ‘Add New’.
3. Enter the specific MAC address in the ‘MAC Address’ field.
4. You can enter a short description, for instance the name of who has been blocked, in the ‘Description’ field.
5. Check ‘Enabled’ in the ‘Status’ field.
6. Click ‘Save’.
7. From now on access to the Internet has been completely blocked for the specified MAC address.

Hint: Chapter 11 explains how to obtain the MAC address of a computer.

11.0 Frequently asked questions

Q: I receive the message ‘The IP address of the network adapter is incorrect’. What can I do?
A: This message appears when the computer did not receive a correct IP address from the router. Make sure all cables are correctly connected. If necessary, reset the EM4450 and try again. It is recommended that you configure the router using a cabled connection (not wireless). When the cabled connection is working properly you can setup the wireless connection as explained in this manual.

Q: I have configured the router. Everything seems fine but I cannot gain access to the Internet. My provider is Chelllo.
A: Make sure you selected the correct MAC address during configuration. If you chose the wrong MAC address, there is not connection to the Internet.

Q: I have configured the router. Everything seems fine but I cannot gain access to the Internet. My provider is Chelllo /@Home/Casema or another DHCP provider.
A: Sometimes the modem does not grant the router access to the Internet. Follow the instructions below to gain access to the Internet:
1. Turn off both the router and modem.
2. Wait for 10 minutes.
3. Turn on the modem, wait until it has booted completely, then turn on the router and let it also boot completely.
4. The connection should now be working properly.

Q: I tried the solution as explained above, but the Internet connection is still not working. What can I do?
A: There is another method:
1. Log in to the webpage of the router with http://192.168.1.1
2. Username: admin, Password: admin

3. You are now logged in to the main page of the EM4450.
4. Disconnect the coax cable from your modem.
5. Click ‘Renew’ under ‘WAN’ in the page of the router.
6. An IP address of the modem will appear on screen. Often this address is something like: 192.168.100.x
7. Reconnect the coax cable to your modem, and wait until the Online/Internet LED is lit.
8. Click ‘Renew’ in the router page.
9. An IP address, given to you by your provider, should now appear on your screen. If so, you are online.

Q: I want to now my IP address. How do I obtain this address?
A: To obtain your IP address, follow the instructions below.

Instructions for Windows XP/2000 and Windows Vista:
1. Click ‘Start’.
2. Go to ‘Run’.
3. Enter ‘cmd’.
4. Press the ‘Enter’ key or click ‘OK’
5. Enter ‘ipconfig’.
6. Press the ‘Enter’ key.
7. You will now see the IP address.

Instructions for Windows98/ME:
1. Click ‘Start’.
2. Go to ‘Run’.
3. Enter ‘winipcfg’.
4. Press the ‘Enter’ key or click ‘OK’.
5. You will now see the IP address or Automatic Personal Address.

Q: I want to know the MAC address of my network adapter. How can I obtain this address?
A: To obtain the MAC address of your network adapter, follow the instructions below:

Instructions for Windows XP/2000 and Windows Vista:
1. Click ‘Start’.
2. Go to ‘Run’.
3. Enter ‘cmd’
4. Press the ‘Enter’ key or click ‘OK’
5. Enter ‘ipconfig /all’.
6. Press the ‘Enter’ key.
7. You will now see the physical address. This is the MAC address of your network adapter.

Instructions for Windows98/ME:

1. Click ‘Start’.
2. Go to ‘Run’.
3. Enter ‘winipcfg’.
4. Press the ‘Enter’ key or click ‘OK’.
5. You will now see the adapter address. This is the MAC address of your network adapter.

Q: How do I reset the EM4450?
A: You can reset the EM4450 by disconnecting the power adapter from the router. Use a paperclip to click the reset button. Reconnect the power adapter to the EM4450, while holding down the reset button. The ‘Sys’ LED will light up. Wait until it starts to blink. Let go of the reset button. The EM4450 has now been reset and back to default settings.

12.0 Service and support

This users manual has been carefully written by Eminent’s technical experts. If you have problems installing or using the product, please contact support@eminent-online.com.

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

Declaration of Conformity

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

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

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

EMINENT

WWW.EMINENT-ONLINE.COM

CE

Eminent is a member of the Intronics Group