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

MANUAL

EM4219 - wSURF ISDN Wireless ADSL2/2+ Modem

WWW.EMINENT-ONLINE.COM

EM4219 - wSURF ISND
Wireless ADSL2/2+ Modemrouter

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

1.0 Warranty conditions

The five-year Eminent warranty applies for 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 exposed to incorrect/improper use, external influences and/or when opened by parties other than Eminent.

2.0 Introduction

Congratulations on your 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 this product now on www.eminent-online.com and receive product updates!

2.1 Functions and features

The Eminent EM4219 wSURF is a wireless ADSL2/2+ modem offering a stable, wireless Internet connection. The built-in router allows you to share this Internet connection with other computers, using a network cable or a wireless connection.

2.2 Packing contents

The following items are present in the package:

- EM4219, wSURF Wireless ADSL2/2+ modem router.
- Power adapter.
- Modular telephone cable.
- UTP network cable.
- CD-rom with installation wizard and manuals.
- Manual.

2.3 Explanation of the LED's

PWR Will be lit when the wSURF is on.
WL/ACT Will be lit when the wireless access point is active.
LAN1,2,3 and 4 Will be constantly lit when a computer is connected to one of the ports and will blink if data is sent or received through one of the network cables.
ADSL Will start to blink 30 seconds after turning on the wSURF and will be constantly lit when the ADSL signal has been detected (only if connected to a telephone cable with an active ADSL signal).
PPP If a PPPoE or PPPoA connection has been configured, this LED will be on when the connection is functioning correctly.

3.0 Using the installation wizard

The easiest way to install the wSURF is by using the installation wizard, as explained in this chapter. If you do not wish to use the wizard (found on the enclosed CD-rom) you can continue with chapter 4.

1. Turn on the computer.
2. Place the CD-rom in the CD-rom or DVD drive of your computer.
3. The software will start automatically.
4. Follow the steps on your screen until the installation is done. You now have a working Internet connection.

4.0 Manual installation

When manually installing the wSURF it is important your Internet browser and your network are correctly configured. The settings will automatically be correct, unless you changed any of the settings in the past. Consult the manual on the CD-rom, if you have doubts about the settings of your Internet browser or your network.

4.1 Connecting the wSURF

1. Turn off your computer.
2. Connect the wSURF to a power outlet using the supplied power adapter.
3. Connect the telephone cable to the 'ADSL' port of the wSURF.
4. Connect the other side of the telephone cable to the ADSL splitter (not supplied).
5. Connect a UTP network cable to one of the four 'LAN' ports of your wSURF.
6. Connect the other side of the UTP network cable to the network adapter in your computer.

Is my wSURF properly connected to the mains? You can verify this by checking if the 'PWR' LED is lit.

Have I got a proper network connection? Turn on the computer and verify if the light – corresponding with the LAN-port on which you connected the UTP networking cable – is lit. On the network adapter in your computer a light should be lit as well.

4.2 Configuring the wSURF for a connection to the Internet

To configure the wSURF for a connection to the Internet, you first need to connect to the wSURF. You can connect to the wSURF using the following procedure:

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. Enter 'admin' in the 'User Name' field (Note! This field is case sensitive).
6. Enter 'admin' in the 'Password' field (Note! This field is case sensitive).
7. Click 'Log in'.
8. The opening page is shown.

Hint! To prevent unauthorised people gaining access to your wSURF it is recommended to change your password.

Click 'Tools'.
Click 'Password'.
Choose 'admin' in the 'Username' field.
Enter the current password in the 'Old Password' field.
Enter the new password in the 'New Password' field.
Enter the new password again in the 'Confirmed Password' field.
Click 'Submit'.
Click 'Ok'.

Write down the new password to be able to change settings in the future:

User Name: *admin*
Password: _____

4.3 Configuration for PPP providers

1. Click 'Setup Wizard'.
2. Select the country where you live in the 'Country' field (For instance 'Netherlands).
3. Select your Internet provider in the 'ISP' field.
4. Click 'Next'.
5. Enter your ADSL username in the 'Username' field.
6. Enter your password in the 'Input Password' field.

7. Enter your password once more in the ‘Confirm Password’ field.
8. Click ‘Save’ to save the settings and restart the wSURF.

4.4 Configuration for DHCP providers

1. Click ‘Setup Wizard’.
2. Select the country where you live in the ‘Country’ field (For instance ‘Netherlands).
3. Select your Internet provider in the ‘ISP’ field.
4. Select ‘DHCP (Get IP dynamically from ISP)’ in the ‘Connection Type’ field.
5. Click ‘Next’.
6. Click ‘Save’ to save the settings and restart the wSURF.

4.5 Configuration for other providers

If you can not find your provider in the Wizard list, you can ask your provider for the correct settings. Follow the procedure below to enter these settings into the wSURF:

1. Click ‘Advanced’.
2. Click ‘WAN’.
3. Enter the settings given to you by the provider.
4. Click ‘Add’.
5. Click ‘Save’ (upper right corner).
6. Click ‘Ok’ to reboot the wSURF.

5.0 Securing the wireless network

To avoid having uninvited guests probing your wireless network we strongly recommend securing your wireless network. You can protect your wireless network in a number of ways. To apply a method to your network, it is necessary for all the wireless devices to support this method. We recommend to set the strongest form of protecting: WPA2 (WiFi Protected Access).

1. Open your Internet browser (for instance Internet Explorer, Netscape or Firefox).
2. Enter ‘http://192.168.1.1’ in the address bar.
3. Press Enter or click ‘Go to’.
4. Enter ‘admin’ in the ‘User Name’ field (Note! This field is case sensitive).
5. Enter ‘admin’ in the ‘Password’ field (Note! This field is case sensitive).
6. Click ‘Advanced’.
7. Click ‘Wireless’.
8. Click ‘Security’.
9. For WPA2 security continue with section 5.1 (recommended), for WEP security continue with section 5.2.

WPA2 security is supported by Windows XP and newer Windows versions. If you have an older Windows version, then continue with section 5.2.

5.1 WPA2 security (recommended)

1. Select 'WPA2 (AES)' in the 'Encryption' field.
2. Select 'Personal (Pre-Shared Key)' in the 'WPA Authentication Mode' field.
3. Select 'Passphrase' in the 'Pre-Shared Key Format' field.
4. Enter a password in the 'Pre-Shared Key' field. For instance 'yourname01'. Do not use any peripherals and make sure the password is at least 8 characters long!
5. Write down the chosen password*.
6. Click 'Submit'.
7. Click 'Save' (upper right corner) to save the settings.

5.2 WEP security

1. Select 'WEP' in the 'Encryption' field.
2. Click 'Set WEP Key'.
3. A new screen will appear.
4. Select 64 or 128 bit in the 'Key Length' field.
5. Select 'ASCII' or 'Hex' in the 'Key Format' field.
6. Select 'Key 1' in the 'Default Tx Key' field.
7. Enter a password in the 'Encryption Key 1' field. Do not use any peripherals and make sure the password is exactly 5, 10, 13 or 26 characters long, depending on the other key settings.
8. Write down the chosen password *.
9. Click 'Submit'.
10. Click 'Save' (upper right corner) to save the settings.

The connection is lost when the security (WPA2 or WEP) has been enabled in the wSURF and not yet in the wireless network adapter. As soon as the security settings are set in the wireless network adapter, the connection will be repaired.

**Write down the security method you used and the password:*
☐ *WPA2* ☐ *WEP*

Password: _____

6.0 Control your Internet connection

If you want to expand the security of your wireless network you can set MAC Address Control on your wSURF. This MAC address is a unique code attached to each and every network device. MAC Address Control enables you to allow specified network

products to connect to your network. All other users will be denied access. If you only add your own MAC address, nobody but you can connect to your network.

Often the MAC address can be found on a sticker on the network device. You can also find it by following these steps:

Click 'Start'.
Click 'Run'.
Type 'CMD'.
Press Enter.
Type 'ipconfig /all'.
Press Enter.
'Physical Address' is the MAC address.

Hint! For your safety the Firewall is turned on by default. We also recommend you to install a virus scanner and update regularly.

6.1 MAC Address Control, block users

1. Open your Internet browser (for instance Internet Explorer, Netscape or Firefox).
2. Enter 'http://192.168.1.1' in the address bar.
3. Press Enter or click 'Go to'.
4. Enter 'admin' in the 'User Name' field (Note! This field is case sensitive).
5. Enter 'admin' in the 'Password' field (Note! This field is case sensitive).
6. Click 'Advanced'.
7. Click 'Wireless'.
8. Click the 'Access Control' tab.
9. Select 'Allow Listed'.
10. Enter the MAC address of the network device that wish to allow access to your network.
11. Click 'Submit'.
12. Repeat steps 11 and 12 if you wish to allow other network devices to your network.
13. Click 'Save' (upper right corner) to save the settings.
14. You have now specified which network devices are allowed to connect to your network.

7.0 WDS, extend the range of the network

The WDS function is primarily useful to increase the range of the wireless network and allow your entire network to connect to the Internet. Using WDS you can extend the range by installing several routers which, through WDS, work as a repeater and as such extend the wireless range. This configuration only requires one Internet connection. All routers connected through WDS have Internet access, so there is no need to connect the LAN or WAN ports of the routers by using cables. WDS allows

you to wirelessly share an Internet connection with other wireless routers or access points that support WDS.

7.1 Turn on the WDS function of the wSURF

These are the instructions for use of WDS. In this example two wireless routers will be used, the wSURF is connected to the Internet. The other wireless router repeats the wireless signal.

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. Enter 'admin' in the 'User Name' field (Note! This field is case sensitive).
6. Enter 'admin' in the 'Password' field (Note! This field is case sensitive).
7. Click 'Log In'.
8. The router will display a welcome screen.
9. Click 'Advanced'.
10. Click 'Wireless'.
11. Click 'Setting'.
12. Set 'Mode' to 'WDS'.
13. Click 'Submit'.
14. Click 'Ok'.
15. Click 'WDS' in the upper menu.
16. Check 'Enable WDS'.
17. Enter the WLAN MAC address (BSSID) of the other router in the 'Add WDS AP' field. You may find this MAC address on the bottom of said router.
18. If you cannot find this address, click the 'Show AP' button. Note down the BSSID of the router you wish to link over WDS, and close the 'Show Ap' screen.
19. Click 'Submit'.
20. If you wish to add more routers to your WDS network, repeat steps 17 and 18 for each router.
21. Click 'Save'.
22. Click 'Ok'.

To establish a WDS connection, you will need to enter the MAC address of the wSURF into the receiving device. For more information you will need to refer to the manual of the receiving device.

If your wireless network is secured, you will also need to configure the security of your other wireless device. In WDS modus, only WEP security can be used. See chapter 5.2 for WEP security.

7.2 Things to keep in mind when using WDS

- All routers in your WDS network need to be in the same IP range (for instance, 192.168.1.1 for router A and 192.168.1.200 for router B). Sometimes you will need to set a fixed IP address on the receiving device.
- WEP security needs to be identical on both devices.
- The channels of the wireless connections need to be identical.
- The names (SSID) of the wireless connections do not need to be identical.
- It is not recommended to use MAC Address Control in combination with WDS.
- DHCP server(s) on the second (or third or fourth) router need(s) to be disabled.

Attention! WPA2 can not be used when securing the connection.

8.0

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 wSURF 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. How do I reset the wSURF?

A. You can reset the modem by following the procedure below:
   1. Turn on the modem and wait for it to boot.
   2. Press down the reset button next to the on/off button for about twenty seconds, using a paperclip
   3. The modem has been reset.

Q. My wireless signal is weak or unstable. What could be the cause?

A. Take the modem to another location and see if the signal strength increases. If possible place the modem in an open space. The mains box for instance is not a good place for a wireless modem.

A. You can change the channel of the modem to see if the signal strength increases. Follow the instructions below:
   1. Open your Internet browser (for instance Internet Explorer, Netscape or Firefox).
   2. Enter 'http://192.168.1.1' in the address bar.
   3. Press Enter or click 'Go to'.

4. Enter ‘admin’ in the ‘User Name’ field (Note! This field is case sensitive).
5. Enter ‘admin’ in the ‘Password’ field (Note! This field is case sensitive).
6. Click ‘Advanced’.
7. Click ‘Wireless’.
8. Set ‘Channel’ to another number, for instance 3.
9. Click ‘Submit’.
10. Click ‘Save’.
11. Click ‘Ok’.

9.0 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

Why an Eminent advanced manual?

Eminent has developed the Eminent Advanced Manual especially for your ease of use. The Eminent Advanced Manual enables you to discover the advanced possibilities of your house network. The Eminent Advanced Manual will for example, help you setting up your firewall so your own network is optimally protected at all times. Of course, extensive consideration is also given to the protection of your wireless network.

The Eminent Advanced Manual is a wealth of information and a handy reference source. This will enable you to have access to functions previously only available to professional and highly advanced users.

Your tips and suggestions in the Eminent Advanced Manual?

The Eminent Advanced Manual was created in cooperation with a number of satisfied Eminent users. If you would like a certain option to be included in the Eminent Advanced Manual or you have suggestions or tips regarding the Eminent Advanced Manual, you can contact communications@eminent-online.com. Your tips and suggestions will be collected and processed in the new edition of the Eminent Advanced Manual.

Service and support

The Eminent Advanced Manual was carefully written by users and technical experts from Eminent. If you have problems installing or using the product, please contact support@eminent-online.com.

Networking settings for Windows 98 and Windows ME

1. Windows 98: Right-click 'Network neighbourhood' on your desktop.
2. Windows ME: Right-click 'My network places' on your desktop.
3. Choose 'Properties'.
4. Select 'TCP/IP'.
5. Click 'Properties'.
6. Select 'Obtain an IP Address automatically'.
7. Click the 'WINS configuration' tab.
8. Select 'Disable WINS resolution'.
9. Click the 'DNS configuration' tab.
10. Click 'Disable DNS'.

11. Click the 'Gateway' tab.
12. Remove previously installed gateways.
13. Click ‘Ok’.
14. Click ‘Ok’ in the 'Network' window.
15. Restart your computer.
16. Click 'Start'.
17. Click 'Run'.
18. Type 'Winipcfg'.
19. Click ‘Ok’.
20. Windows will show the 'IP configuration window'.
21. Select the Ethernet adapter (Networking PCI adapter) connected to the router.
22. Click 'Release all'.
23. Click 'Renew all'.
24. Click ‘Ok’.

Networking settings for Windows 2000 and Windows XP

1. Right-click 'My network places' on your desktop.
2. Choose 'Properties'.
3. Right-click 'Local area connection'.
4. Choose 'Properties'.
5. Select 'Internet protocol (TCP/IP)'.
6. Click 'Properties'.
7. Select 'Obtain an IP Address automatically'.
8. Select 'Obtain a DNS server address automatically'.
9. Click ‘Ok’.
10. Windows will show the 'Local area connection properties' window.
11. Click ‘Ok’.
12. Windows 2000: Close the 'Network and dial-up connections' window.
13. Windows XP: Close the 'Network connections' window.
14. Restart your computer.
15. Click 'Start'.
16. Click 'Run'.
17. Type 'cmd'.
18. Push enter on your keyboard.
19. Type 'ipconfig /release'.
20. Push enter on your keyboard.
21. Type 'ipconfig /renew'.
22. Push enter on your keyboard.
23. Type 'Exit'.
24. Push enter on your keyboard.

Networking settings for Windows Vista

1. Click on the Windows Vista logo (start button).
2. Choose ‘Configuration screen’.
3. Choose ‘Show network status and –tasks’.
4. Choose ‘Control network connections’.
5. Right-click on ‘LAN-connection’.
6. Choose ‘Connect.
7. If windows asks for your permission: choose ‘Continue’
8. Windows Vista now connects your LAN-connection.
9. Right-click on ‘LAN-connection’.
10. Choose ‘Properties’.
11. If windows asks for your permission: choose ‘Continue’.
12. Select ‘Internet Protocol version 4 (TCP/IPv4)’.
13. Click on ‘Properties’.
14. Choose ‘Obtain IP Address automatically.’
15. Choose ‘Obtain DNS Server address automatically’.
16. Click ‘OK’.
17. Click ‘Close’.
18. Windows Vista will now set-up your connection.

Configuring Internet Explorer 5 and 5.5

1. Start Internet Explorer.
2. Click ‘Stop’.
3. When asked to establish a connection, press ‘Cancel’.
4. Click ‘Extra’.
5. Click ‘Internet options’.
6. Click the ‘Connections’ tab.
7. Click the ‘LAN settings’ tab.
8. Uncheck ‘Find Explorer settings automatically’.
9. Uncheck ‘Use configuration script’.
10. Uncheck ‘Use proxy-server’.
11. Click ‘Ok’.
12. Remove dial-up connections by pressing ‘Delete’.
13. Click ‘Settings’ to start the ‘Internet’ Wizard.
14. Select ‘I would like to connect through a LAN network’.
15. Click ‘Next’.
16. Check ‘Automatically detect proxy-server’.
17. Click ‘Next’.
18. Click ‘No’.
19. Click ‘Next’.
20. Click ‘Complete’.
21. Close all Windows that are currently open.

22. Restart your PC.

Configuring Internet Explorer 6

1. Start Internet Explorer.
2. Click ‘Stop’.
3. When asked to establish a connection, press ‘Cancel’.
4. Click ‘Extra’.
5. Click ‘Internet options’.
6. Click the ‘Connections’ tab.
7. Click the ‘LAN settings’ tab.
8. Uncheck ‘Find Explorer settings automatically’.
9. Uncheck ‘Use configuration script’.
10. Uncheck ‘Use proxy-server’.
11. Click ‘Ok’.
12. Remove dial-up connections by pressing ‘Delete’.
13. Click ‘Settings’ to start the ‘New connection’ Wizard.
14. Click ‘Next’.
15. Select ‘Connect to the Internet’.
16. Click ‘Next’.
17. Select ‘I want to connect to the Internet manually’.
18. Click ‘Next’.
19. Select ‘Permanent broadband connection’.
20. Click ‘Next’.
21. Click ‘Complete’.
22. Close all Windows that are currently open.
23. Restart your PC.

Configuring Internet Explorer 7

1. Start internet Explorer.
2. Click ‘Stop’.
3. When asked to establish a connection, press ‘Cancel’.
4. Click ‘Extra’.
5. Click ‘Internet options’.
6. Click the ‘Connections’ tab.
7. Click the ‘LAN settings’ tab.
8. Uncheck ‘Find Explorer settings automatically’.
9. Uncheck ‘Use configuration script’.
10. Uncheck ‘Use proxy-server’
11. Click ‘Ok’.
12. Remove dial-up connections by clicking ‘Delete’.
13. Click on ‘Settings’ (at the top).
14. Choose your type of connection.

15. Windows Vista will now set-up your connection.

DHCP, Automatic allocation of IP addresses

For the development of DHCP (Dynamic Host Configuration Protocol), TCP/IP settings are configured manually on each TCP/IP client (such as your computer for example). This can be a difficult job if it is a big network or if something has to be changed regularly in the network. DHCP was developed to avoid always having to set up an IP address. With DHCP, IP addresses are allocated automatically when necessary and released when no longer required. A DHCP server has a series ('pool') of valid addresses that it can allocate to the client. When a client starts for example, it will send a message requesting an IP address. A DHCP server (there can be several in a network) responds by sending back an IP address and configuration details. The client will send a confirmation of receipt after which it can operate on the network.

Translating IP addresses and domain names

IP addresses are far from user-friendly. Domain names are however easier to remember and use. The process of translating a domain name into an address that is understandable for a machine (such as your computer) is known as 'name resolution'. A 'Domain Name System' server carries out the afore-mentioned process. Thanks to DNS, you use domain names instead of IP addresses when visiting a website or sending e-mails.

Dynamic DNS or DDNS is a DNS-related option. You can still link your IP address to a domain name using DDNS if your provider works with dynamic IP addresses ('dynamic' here means that the IP addresses change frequently). After all, the IP address to which your domain name refers will also change when your provider changes your IP address. You must register with a Dynamic DNS provider such as www.dyndns.org and www.no-ip.com in order to use Dynamic DNS.

Using a single IP address for your entire network

Network Address Translation (NAT) is an Internet standard with which a local network can use private IP addresses. Private IP addresses are those used within an own network. Private IP addresses are neither recognized nor used on the Internet. An IP address used on the Internet is also called a public IP address.

NAT enables you to share a single public IP address with several computers in your network. NAT ensures the computers in your network can use the Internet without any problems but users on the Internet will not have access to the computers in your network. You will understand that NAT also offers a certain level of security partly due to the fact that private IP addresses are not visible on the Internet.

Fortunately, most routers currently use NAT.

Security for your computer and your network

A firewall can be a software- or a hardware solution placed, as it were, between the internal network and the outside world. Firewalls generally control incoming and outgoing data. Firewalls can be adjusted to stop or allow certain information from the Internet. Firewalls can also be adjusted to stop or allow requests from outside. Rules or policies are used to adjust firewalls. These state what a firewall must stop or allow and thus form a sort of filter.

Most routers have various firewall functions. The big advantage of a firewall in a router (hardware solution) is that an attack from outside is averted before reaching your network. If you wish to use a software firewall, you could for example, use the firewall built into Windows XP Service Pack 2. There are better alternatives such as the free ZoneAlarm and the commercial packages from Norman, Norton, Panda and McAfee. These commercial packages also offer protection against viruses if required.

Making a computer available for Internet users in your network

The DMZ or DeMilitarized Zone is the zone between the outside world – the Internet – and the secure internal network. The computer placed within the DMZ is accessible via the Internet. This is in contrast to the computers that are outside the DMZ and are therefore secure. The DMZ is therefore also often used for servers that host websites. Websites must after all always be accessible via the Internet. A computer is also often placed within the DMZ if one plays a lot of online games. It is however advisable when you place a computer in the DMZ to fit a software firewall (such as the free ZoneAlarm). This is because the firewall opens all ports of the router for a computer within the DMZ. There is therefore no restriction on data transmission while this is however desirable in some situations.

Just like the DMZ function, Virtual Server enables you to make a computer, set up for example, as an FTP- or a web server, accessible from the Internet. You can state which ports in the firewall must be opened when using a Virtual Server. This is also the most important difference with the DMZ: when you place a computer in the DMZ, all ports are opened for the respective computer. If you use Virtual Server, you can open only the ports important for the respective computer.

Port Triggering or Special Apps is based on the same principle as Virtual Server. Port Triggering also enables you to make a computer within your network set up for example as an FTP- or webserver, accessible from the Internet. The ports you allocate always remain open when you use Virtual Server. With Port Triggering

however, the respective ports will only be opened if requested by the respective application.

Simplifying network management

UPnP 'Universal Plug and Play': The name suggests that UpnP is very similar to the well-known – and notorious – 'Plug & Play'. Nothing is further from the truth. UPnP is completely different technology. The line of approach is that UPnP appliances must be able to communicate with one another via TCP/IP irrespective of the operating system, the programming language or the hardware. UPnP should make the user's life considerably easier.
As well as the products from a limited number of other manufacturers, most Eminent network manufacturers support UPnP. For more information on UPnP, visit: www.upnp.org.

Blocking websites with explicit content

Parental Control enables you to prevent one or more computers in your network from accessing the Internet. Parental Control often consists of several functions such as 'URL Blocking'. This function blocks websites by way of so-called 'keywords' or catchwords. Websites with explicit content are blocked in this way. URL Blocking is often combined with time and/or date blocks. Such blocks enable you to allow or block Internet access at certain times. You use 'rules' or 'policies' to set up your own schedule of blocks (see also 'Schedule Rule'). These rules describe exactly when and on what, a certain action, in this case, a block, must be applied.

Checking data traffic at package level

The package filter (or 'Packet Inspection') is a programme that checks data packages while they are passing. The intelligent package filter checks the passing dataflow or business-specific definitions such as the IP- or user address, time and date, function and a number of other definitions. The package filter can best be imagined as a gatekeeper. The 'gatekeeper' screens the passers-by: 'Who are you and where are you going?' The passers-by whom the gatekeeper considers unsafe or unreliable are kept out.

You do not have to configure the package filter in most appliances. You only have the option of activating these. The use of this option is therefore also definitely recommended.

Blocking a complete domain

A 'Domain Filter' will enable you to block an entire domain. A domain is a location on the Internet such as a website. A Domain Filter is therefore very similar to a 'URL

Filter', apart from the fact that a Domain Filter blocks the entire domain. If, for example, you wish to protect your children from explicit content on a certain website, as well as blocking the website by way of catchwords (see: 'Parental Control'), you can block the entire website. You can do this using the Domain Filter.

Carrying out actions based on date or time

You can configure when a certain option may be available using the 'Schedule Rule' function. Imagine you wish to make your 'Virtual Server' available at set times. You can use the Schedule Rule to stipulate when Internet users may approach your Virtual Server. It will then not be possible for Internet users to make a connection with your Virtual Server outside the period set. Schedule Rule is a handy option for automating certain access blocks.

A safe remote connection

VPN (Virtual Private Networking) enables you to create a secure connection so you can, for example, use your business network while at home. A VPN connection is actually nothing more than a highly secure tunnel, which makes a connection with another computer or network via the Internet. Data sent via a VPN and received by third parties will still be unusable thanks to advanced encryption technology.

Remote network management

The Simple Network Management Protocol (SNMP) is a control function enabling you to collect information from the router. The above-mentioned information consists of details on the number of computers connected to the router, their IP- and MAC addresses and the amount of data traffic processed when the information is requested. SNMP enables the system administrator to control the router remotely. This is often done using special applications supporting the SNMP protocol.

Allocating or blocking network access

A MAC address is a unique code which each network product has. This code can often be found on a sticker on the product. You can also find the MAC address by clicking on 'Start', 'Execute'. Type 'CMD' and press 'Enter'. Then type 'ipconfig /all' and press 'Enter' again. The MAC address is shown under 'Physical Address'. A MAC address consists of six pairs each of two hexadecimal characters. For example, 00-0C-6E-85-03-82. MAC Address Control enables you to set up rules for MAC addresses and therefore to deny for example, certain network products access to your network. When you use a wireless network, you can meanwhile use MAC Address Control to configure for example, your wireless network adapter to be able to connect to your network without the neighbouring network adapter being able to do so. MAC

Address Control is a possibility, as well as WEP or WPA of providing extra security for your wireless network.

Making your wireless network secure

WEP encryption is a form of security encoding the wireless signal from your wireless router or modem so the data cannot be simply intercepted by third parties. The security level is expressed in bits. 64-Bit WEP encryption is the lowest security level ranging up to 128-Bit for the highest level of security offered by WEP encryption: 256-Bit. You must enter a hexadecimal- or an ASCII series of characters in order to set up WEP encryption. Hexadecimal characters consist of the characters 'A' to 'F' and '0' to '9'. ASCII characters include all characters, including symbols. When you have selected the correct level of security and entered the key, you must also enter exactly the same key into all wireless appliances within the same network. Bear in mind that – when you activate the key in the first appliance – the connection with the network will be broken. You can re-establish the network by systematically providing all wireless appliance products with the same key.

WPA is a form of security encoding the wireless signal from your wireless router or modem so the data cannot be simply intercepted by third parties. WPA stands for 'Wi-Fi Protected Access' and is a big improvement on wireless security. WPA uses a 'Pre Shared Key (PSK)'. This is a key that must be put into operation on all appliances connected to the wireless network. This WPA key may not be any longer than 63 (random) characters and no shorter than 8 (random) characters. The best form of wireless protection is currently however formed by WPA2. The above-mentioned standard is only supported by a few manufacturers – including Eminent – and is therefore difficult to combine with other makes of wireless networks.

If you wish to use WPA or perhaps even WPA2, make sure that all appliances in your wireless network support this form of security. The combining of various types of security in a wireless network is not possible and will result in the loss of the connection.

Expanding the range of your wireless network

WDS (Wireless Distribution System) or 'Bridging' is an option with which you can easily expand the range of your wireless network should the range of your wireless network remain limited. Appliances linked via WDS can share your Internet connection. You therefore do not need to interlink appliances sharing WDS by way of a physical connection (such as a cable). Appliances supporting WDS or Bridging recognize one another automatically in most cases. You can use a so-called 'Range Extender' if you wish to expand your network using WDS or Bridging. This is an appliance largely similar to an 'Access Point'. The advantage of using a Range

Extender rather than a second router – if the second router bridging is supported – is that a Range Extender is considerably cheaper.

Index

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.

WWW.EMINENT-ONLINE.COM

Eminent is a member of the Intronics Group