EMINENT

*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 ISDN Wireless ADSL2/2+ Modem

## Varningar och uppmärksammanden

På grund av EU-direktiv och regleringar så kan denna produkts egenskaper vara begränsade i vissa medlemsstater. Den kan även vara förbjuden att använda i vissa länder. Mer information om detta kan återfinnas under rubriken Försäkran av Överensstämmelse på sista sidan av detta dokument.

## Innehållsförteckning



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

## 1.0 Garantibestämmelser

Den femåriga garantin på Eminents produkter återfinns på alla Eminents produkter om inte annat har framgått före eller under köpet. Vid köp av begagnade

Eminentprodukter så räknas den femåriga garantin från det datum den första ägaren gjorde köpet. Garantin täcker alla Eminentprodukter, dess komponenteroch dess fasta såväl som påmonterade delar. Batteriemulatorer, batterier, antenner och övriga komponenter som inte är direkt kopplade till Eminents huvudprodukt som utan godtagbar härledning till Eminents huvudprodukt uppvisar skador täcks inte av Eminents garanti. Produkter som har blivit utsatta för en inkorrekt eller felaktig användning och/eller har blivit öppnade av annan part än Eminent täcks inte av Eminents garanti.

# 2.0 Introduktion

Låt oss gratulera dig tilll ditt köp av denna hög-kvalitativa Eminentprodukt! Denna produkt har genomgått grundlig testning av Eminents tekniska experter. Skulle du mot förmodan stöta på problem med denna produkt så är du täckt av vår femåriga Eminenttgaranti. Vänligen spara denna manual och ditt kvitto på en säker plats.

*Registrera produkten idag på www.eminent-online.com och få produktuppdateringar!*

## *2.1 Funktioner och egenskaper*

EM4219 är ett trådlöst ADSL2/2+ modem som erbjuder en stabil och trådlös internetåtkomst. Den inbyggda routern låter din dela denna internetuppkoppling med andra datorer, med nätverkskabel eller trådlös anslutning.

## *2.2 Förpackningens innehåll*

Följande ska återfinnas i förpackningen:

- EM4219, wSURF ISDN trådlöst ADSL2/2+ Modem/router.
- Strömadapter.
- Telefonsladd.
- UTP-nätverkskabel.
- CD-rom med installationsguide och manualer.
- Manual.

## *2.3 Förklaring om lysdioderna*

| | |
|---|---|
| *PWR* | *Lyser när EM4219 är igång.* |
| *WL/ACT* | *Lyser när den trådlösa accesspunkten är aktiv.* |
| *LAN1,2,3 och 4* | *Kommer konstant att llysa när en dator är ansluten till en av portarna och kommer att blinka om information tas emot eller skickas genom en av nätverkskablarna.* |
| *ADSL* | *Kommer att börja blinka 30sek efter uppstarten av EM4219 och kommer att lysa konstant när ADSL-signal har hittats (endast om ansluten till en telefonsladd med aktiv ADSL signal).* |
| *PPP* | *Om en PPPoE- eller PPPoA-anslutning har konfigurerats kommer denna lydiod att lysa när den fungerar korrekt.* |

# 3.0 Använda installationsguiden

Det enklaste sättet att installera EM4219 är med hjälp av den medföljande installationsguiden, vilket förklaras i detta kapitel. Om du ej vill använda den medföljande installationsguiden som återfinns på den medföljande CD-skivan, fortsätt till kapitel 4.

1. Starta datorn.
2. Stoppa in CD-skivan i dators CD- eller DVD-läsare.
3. Programmet kommer att startas automatiskt.
4. Följ de anvisningar som visas på skärmen till det att installationen är slutförd. Du har nu en fungerande internetanslutning.

# 4.0 Manuell installation

När du manuellt installerar EM4219 är det viktigt att kontrollera så att din webbläsare och ditt nätverk är konfigurerade på rätt sätt. Du kan utgå från att dessa inställningar är korrekta om det inte är så att du har ändrat i inställningarna själv någon gång. Titta i manualen på CD-skivan om du inte är säker på att dina inställningar är korrekta.

## *4.1 Connecting the EM4219*

1. Stäng av din dator.
2. Anslut EM4219 till elförsörjning genom att använda dig av den medföljande batteriemulatorn.
3. Anslut den medföljande telefonsladden till ADSL-porten på din EM4219.
4. Anslut den andra änden av telefonsladden till ADSL-splitten (ej medföljande).
5. Anslut en nätverksktsladd i en LAN-port på din EM4219.
6. Med den andra änden på sladden ansluter du din dators nätverkskort.

*Får min EM4219 ström? Du kan verifiera att så är fallet genom att titta om lampan märkt med 'PWR' lyser.*

*Har jag en korrekt nätverksanslutning? Starta din dator och kontrollera så att lysdioden som hör till den LAN-port du har anslutit din dator till lyser. På din dators nätverkskort bör även en lampa lysa.*

## 4.2 Konfigurera EM4219 för en anslutning mot internet

För att konfigurera EM4219 för en anslutning mot internet måste du först ansluta till EM4219. Du kan ansluta tillEM4219 på följande sätt:

1. Starta din dator.
2. Starta din webbläsare (t.ex. Internet Explorer, Netscape, Safari eller Firefox).
3. Skriv in 'http://192.168.1.1' i adressfältet.
4. Tryck Enter eller 'Gå till'.
5. Ange 'admin' i textfältet 'User Name' (OBS! Detta fält är känsligt för gemener samt versaler.).
6. Ange 'admin' i textfältet 'Password' (OBS! Detta fält är känsligt för gemener samt versaler.).
7. Klicka på 'Log in'.
8. Startsiudan visas.

*Tips! För att förhindra att personer får åtkomst till din EM4219 rekommenderar vi att du byter lösenord.*

1. *Klicka på 'Tools'.*
2. *Klicka på 'Password'.*
3. *Ange 'admin' i textfältet 'Username'.*
4. *Ange nuvarande lösenort i textfältet 'Old Password'.*
5. *Ange det nya önskade lösenordet i textfältet 'New Password'.*
6. *Ange det nya önskade lösenordet igen i textfältet 'Confirmed Password'.*
7. *Klicka på 'Submit'.*
8. *Klicka på 'Ok'.*

*Skriv ner det nya lösenordet nedan så att du lätt kommer åt det när du behöver göra ändringar i framtiden:*

*Användarnamn: admin*
*Lösenord: _____*

## 4.3 Konfiguration för PPP-internetleverantörer

1. Klicka på 'Setup Wizard'.
2. I fältet 'Country' ska du välja det land du bor i (t.ex. 'Netherlands).

3. Välj din internetleverantör i textfältet ‘ISP’.
4. Klicka på ‘Next’.
5. Ange ditt användarnamn för ADSL i textfältet ‘Username’ field.
6. Ange ditt lösenord i fältet ‘Input Password’.
7. Ange ditt lösenord, igen, i fältet ‘Confirm Password.
8. Klicka på ‘Save’ för att spara inställningarna och starta om EM4219.

## *4.4 Konfiguration för DHCP-internetleverantörer*

1. Klicka på ‘Setup Wizard’.
2. I fältet ‘Country’ ska du välja det land du bor i (t.ex. ‘Netherlands).
3. Välj din internetleverantör i textfältet ‘ISP’.
4. Välj ‘DHCP (Get IP dynamically from ISP)’ i fältet ‘Connection Type’.
5. Klicka på ‘Next’.
6. Klicka på ‘Save’ för att spara inställningarna och starta om EM4219.

## *4.5 Konfiguration för andra internetleverantörer*

Om du inte kan hitta din leverantör i installationsguidens lista ber vi dig kontakta din internetleverantör för att få rätt inställningar, ofta finns dessa på internetleverantörens hemsida. För att ställa in dessa inställningar i EM4219 gör du på följande sätt:

1. Klick ‘Advanced’.
2. Klicka på ‘WAN’.
3. Ange de inställningarna som du hittade.
4. Klicka på ‘Add’.
5. Klicka på ‘Save’ (övre högra hörnet).
6. Klicka på ‘Ok’ för att starta om EM4219.

# 5.0 Skydda det trådlösa nätverket

För att undvika att oinbjudna gäster använder sig av ditt trådlösa nätverk så rekommenderar vi starkt att du skyddar ditt trådlösa nätverk. Det finns ett antal olika sätt att skydda ditt trådlösa nätverk på. För att välja en säkerhetsmetod för ditt nätverk måste alla trådlösa enheter i nätverket ha stöd för denna metod. Det säkraste sättet för tillfället är WPA2 (WiFi Protected Access), vilket vi rekommenderar.

1. Starta din webbläsare (t.ex. Internet Explorer, Netscape, Safari eller Firefox browser.
2. Ange ‘http://192.168.1.1’ i adressfältet.
3. Tryck på tangenten Enter eller klicka på ’Gå till’.
4. Ange ‘admin’ i textfältet ‘User Name’ (Note! This field is case sensitive).
5. Ange ‘admin’ i textfältet ‘Password’ (Note! This field is case sensitive).
6. Klicka på ‘Advanced’.
7. Klicka på ‘Wireless’.

8. Klicka på ‘Security’.
9. För WPA2-skydd fortsätt till kapitel 5.1(rekommenderas), för WEP-skydd fortsätt till kapitel 5.2.

*Versioner av Windows fr.o.m. XP har stöd för WPA2-skydd. Om du har en äldre version av Windows, fortsätt till kapitel 5.2.*

## *5.1 WPA2-skydd (rekommenderas)*

1. Välj ‘WPA2 (AES)’ i fältet ‘Encryption’.
2. Välj ‘Personal (Pre-Shared Key)’ i fältet ‘WPA Authentication Mode’.
3. Välj ‘Passphrase’ i fältet ‘Pre-Shared Key Format’.
4. Ange ett lösenord i textfältet ‘Pre-Shared Key’. T.ex. ‘yourname01’. Använd inga skiljetecken och se till så att lösenordet är minst åttta tecken långt!
5. Skriv ned det valda lösenordet*.
6. Klicka på ‘Submit’.
7. Klicka på ‘Save’ (övre högra hörnet) för att spara inställningarna.

## *5.2 WEP-skydd*

1. Välj ‘WEP’ i fältet ‘Encryption’.
2. Klicka på ‘Set WEP Key’.
3. Ett nytt fönster kommer att visas.
4. Välj 64 eller 128 bit i fältet ‘Key Length’.
5. Välj ‘ASCII’ eller ‘Hex’ i fältet ‘Key Format’.
6. Välj ‘Key 1’ i fältet ‘Default Tx Key’.
7. Ange ett lösenord i fältet ‘Encryption Key 1’. Använd inga skiljetecken och se till så att lösenordet är exakt 5, 10, 13 eller 26 tecken långt, beroende på andra löseninställningar.
8. Skriv ned det valda lösenordet*.
9. Klicka på ‘Submit’.
10. Klicka på ‘Save’ (övre högra hörnet) för att spara inställningarna.

*Anslutningen bryts när skyddet (WPA2 or WEP) aktiverats i EM4219 men ännu inte har ställts in i nätverkskorten. Så fort att säkerhetsinställningarna har ställts in på nätverkskorten kommer anslutningen att repareras.*

**Skriv ned säkerhetsmetod och valt lösenord:*
☐ *WPA2* ☐ *WEP*

*Lösenord: _____*

# 6.0 Kontrollera din internetanslutning

Om du vill utöka säkerheten kring ditt trådlösa nätverk kan du ställa in “MAC Address Control” på din EM4219. MAC-adressen är en unik kod som finns till varje nätverksenhet. ”MAC Address Control” aktiverar så att du kan tillåta vissa nätverksenheter att ansluta till din nätverk, alla andra enheter nekas tillträde. Om du endast lägger till din MAC-adress kan endast du ansluta till ditt nätverk.

*MAC-adressen finns ofta på en klisterlapp på din enhet, men du kan även ta reda på den på följande sätt:*

1. *Klicka på ‘Start’.*
2. *Klicka på ‘Run’.*
3. *Skriv ‘CMD’.*
4. *Tryck på tangenten Enter.*
5. *Skriv in ‘ipconfig /all’.*
6. *Tryck på tangenten Enter.*
7. *‘Physical Address’ är MAC-adressen.*

*Tips! För din säkerhet är den inbyggda brandväggen igång från början. Vi rekommenderar även att du installerar ett antivirusprogram och uppdaterar ofta.*

## *6.1 MAC Address Control, blockera användare*

1. Öppna din webbläsare (t ex Internet Explorer, Netscape eller Firefox).
2. Skriv ‘http://192.168.1.1’ i address fältet.
3. Tryck Enter eller klicka på ‘Go to’.
4. Skriv ‘admin’ i ‘User Name’ fältet (OBS! Fältet känner av gemener och versaler).
5. Skriv ‘admin’ i ‘Password’ fältet (OBS! Fältet känner av gemener och versaler).
6. Klicka på ‘Advanced’.
7. Klicka på ‘Wireless’.
8. Klicka på ‘Access Control’ fliken.
9. Välj ‘Allow Listed’.
10. Skriv in MAC adressen för den nätverksenhet som skall ha åtkomst till ditt nätverk.
11. Klicka på ‘Submit’.
12. Repetera steg 11 och12 om du vill lägga till fler nätverksenheter till ditt nätverk.
13. Klicka på ‘Save’ (i övre högra hörnet) för att spara inställningarna.
14. Du har nu specificerat vilka nätverksenheter som har tillåtelse att ansluta till ditt nätverk.

# 7.0 WDS, utökar räckvidden i ett nätverk

WDS funktionen används först och främst för att utöka räckvidden i ett trådlöst nätverk så att hela nätverket har möjlighet att ansluta till Internet. Vid användning av WDS kan du utöka räckvidden genom att installera flera routrar som med WDS funktionen fungerar som en repeter och som en sådan förlänger den trådlösa räckvidden. Denna konfiguration kräver endast en Internet anslutning. Alla routrar som är anslutna via WDS har därmed åtkomst till Internet, så det krävs ingen anslutning av kablar till LAN eller WAN porten på dessa routrar. WDS ger dig möjligheten att trådlöst dela Internet uppkoppling med andra trådlösa routrar och accesspunkter som stödjer WDS.

## *7.1 Starta WDS funktionen på EM4219*

Här är instruktionerna för användning av WDS. I detta exempel används två trådlösa routrar, EM4219 är ansluten till internet och den andra trådlösa routern fungerar som repeter av den trådlösa signalen.

1. Starta din dator
2. Öppna din webbläsare (t ex Internet Explorer, Netscape eller Firefox).
3. Skriv ‘http://192.168.1.1’ i adress fältet.
4. Tryck Enter eller klicka på ‘Go to’.
5. Skriv ‘admin’ i ‘User Name’ fältet (OBS! Fältet känner av gemener och versaler).
6. Skriv ‘admin’ i ‘Password’ fältet (OBS! Fältet känner av gemener och versaler).
7. Klicka på ‘Log In’.
8. Routern visar nu en välkomst ruta.
9. Klicka på ‘Advanced’.
10. Klicka på ‘Wireless’.
11. Klicka på ‘Setting’.
12. Ändra ‘Mode’ till ‘WDS’.
13. Klicka på ‘Submit’.
14. Klicka på ‘Ok’.
15. Klicka på ‘WDS’ i den övre menyn.
16. Kryssa i ‘Enable WDS’.
17. Skriv in WLAN MAC adressen (BSSID) för den andra routern i ‘Add WDS AP’ fältet. Du kan finna denna MAC adress på undersidan av nämnda router.
18. Om du inte hittar denna adress, klicka på ‘Show AP’ knappen. Skriv ner BSSID för den router du vill länka via WDS, och stäng ner ‘Show Ap’ rutan.
19. Klicka på ‘Submit’.
20. Om du önskar lägga till fler routers I ditt WDS nätverk, upprepar du steg 17 och 18 för varje router.
21. Klicka på ‘Save’.
22. Klicka på ‘Ok’.

*För att etablera en WDS anslutning, måste du lägga till MAC adressen för EM4219 i den mottagande enheten. Mer information finns att finna i den mottagande enhetens manual..*

*Om ditt trådlösa nätverk är krypterat, måste du även kryptera de andra trådlösa enheterna. I WDS modus, kan enbart WEP kryptering användas. Se kapitel 5.2 för WEP kryptering.*

## *7.2 Saker att tänka på vid användning av WDS*

- Alla routers I ditt WDS nätverk måste ingå i samma IP grupp (t ex, 192.168.1.1 för router A och 192.168.1.200 för router B). Ibland måste du tilldela en statisk IP adress till en mottagande enhet.
- WEP säkerheten måste vara identisk på båda enheterna.
- Kanalen för den trådlösa anslutningen måste vara identisk.
- Namnet (SSID) för den trådlösa anslutningen behöver inte vara identiskt.
- Det är inte att rekomendera att använda sig av MAC Address Control i kombination med WDS.
- DHCP server(s) on the second (or third or fourth) router need(s) to be disabled.

*OBS! WPA2 kan inte användas för att kryptera anslutningen..*

# 8.0 Vanliga frågor

*F. Jag får följande meddelande 'The IP address of the network adapter is incorrect'. Vad skall jag göra?*

S. Meddelandet skickas när datorn inte får en korrekt IP adress från routern. Se till att alla kablar är anslutna på ett korrekt sätt. Om det blir nödvändigt, återställ fabriksinställningarna för EM4219 och försök igen. Vi rekommenderar att konfigureringen av routern sker via en ansluten kabel (ej trådlöst). Via kabelanslutningen kan du sedan konfigurera den trådlösa anslutningen som beskrivs i denna manual.

*F. Hur återställer jag inställningarna för EM4219?*

S. Du kan återställa modemet genom att följa proceduren nedan:

1. Slå på modemet och vänta på att det startar.
2. Tryck ned reset knappen bredvid on/off knappen i ungefär 20 sek, använd tex en penna.
3. Modemet är nu återställt.

*F. Den trådlösa signal är svag och o-stabil. Vad kan vara problemet?*

S. Flytta modemet till en annan plats/rum för att se om signalstyrkan ökar. Om det är möjligt, försök placera modemet i en så öppen miljö som möjligt. Nära en el-central är ingen bra plats att placera ett trådlöst modem på.

S. Du kan ändra kanal på modemet för att se om signalstyrkan ökar. Följ instruktionerna nedan:
   1. Öppna din webbläsare (t ex Internet Explorer, Netscape eller Firefox).
   2. Skriv ‘http://192.168.1.1’ i adress fältet.
   3. Tryck Enter eller klicka på ‘Go to’.
   4. Skriv ‘admin’ i ‘User Name’ fältet (OBS! Fältet känner av gemener och versaler).
   5. Skriv ‘admin’ i ‘Password’ fältet (OBS! Fältet känner av gemener och versaler).
   6. Klicka på ‘Advanced’.
   7. Klicka på ‘Wireless’.
   8. Byt ‘Channel’ till ett annat nummer, t ex 3.
   9. Klicka på ‘Submit’.
   10. Klicka på ‘Save’.
   11. Klicka på ‘Ok’.

# 9.0 Service och support

Denna användarmanual har noggrant utformats av Eminents tekniska experter. Om du stöter på problem under installationen så kan gärna kontakta oss på 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 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

# Försäkran av Överensstämmelse

För din säkerhets skull och för att uppfylla gällande direktiv skapade av EU-kommissionen kan du få en kopia av Försäkran av Överensstämmelse gällande denna produkt genom att skicka ett e-brev till: info@eminent-online.com. Du kan även skicka ett brev till:

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

Var vänlig märk brevet tydligt med 'Försäkran av Överensstämmelse' samt artikelnumret på produkten det gäller.

EMINENT

WWW.EMINENT-ONLINE.COM



CE

Eminent is a member of the Intronics Group