

**EMINENT**



HANDLEIDING

**EM4206/EM4207 - ADSL2/2+ Modem**

[WWW.EMINENT-ONLINE.COM](http://WWW.EMINENT-ONLINE.COM)

## EM4206/EM4207 - ADSL2/2+ Modem



### Waarschuwingen en aandachtspunten

Het openen van het product en/of de producten kan leiden tot ernstige verwondingen!  
Laat reparatie altijd uitvoeren door gekwalificeerd personeel van Eminent!

### Inhoudsopgave

1.0 Garantievoorwaarden .....	2
2.0 Introductie .....	3
2.1 Functies en kenmerken .....	3
2.2 Inhoud van de verpakking.....	3
2.3 Uitleg van de lampjes .....	3
3.0 Configuratie via de installatiewizard.....	4
4.0 De modemrouter handmatig aansluiten .....	4
4.1 Het aansluiten van de modem/router .....	4
4.2 De modemrouter handmatig configureren voor het internet .....	4
4.2.1 Configuratie voor PPP providers .....	5
4.2.2 Configuratie voor 1483 Bridged providers .....	5
4.2.3 Configuratie voor overige providers .....	5
5.0 Geavanceerde instellingen / Firewall .....	6
5.1 Het instellen van de klok (SNTP) .....	6
5.2 Port Forwarding (Firewall).....	6
5.3 IP Filters .....	7
5.4 LAN Clients .....	7
5.5 Bridge filters .....	7
5.6 Static Routing .....	7
5.7 Dynamic Routing .....	7
6.0 Service en ondersteuning .....	7

*Eminent Advanced Manual voor netwerkinstellingen en uitgebreide informatie over thuisnetwerken vanaf pagina 9.*

### 1.0 Garantievoorwaarden

De garantietermijn van vijf jaar geldt voor alle Eminent producten, tenzij anders aangegeven op het moment van aankoop. Bij aankoop van een tweedehands Eminent product resteert de garantieperiode gemeten vanaf het moment van de aankoop door de eerste eigenaar.

De Eminent garantieregeling is van toepassing op alle Eminent producten en onderdelen onlosmakelijk verbonden met het betreffende product. Voedingen, batterijen, accu's, antennes en alle andere producten niet geïntegreerd in of direct verbonden met het hoofdproduct of producten waarvan redelijkerwijs mag worden

aangenomen dat deze een ander slijtagepatroon kennen dan het hoofdproduct vallen derhalve niet onder de Eminent garantieregeling. De garantie vervalt tevens bij onjuist of oneigenlijk gebruik, externe invloeden en/of bij opening van de behuizing van het betreffende product door partijen anders dan Eminent.

## 2.0 Introductie

Gefeliciteerd met de aankoop van dit hoogwaardige Eminent product! Dit product is door de technische experts van Eminent uitgebreid getest. Mocht dit product ondanks alle zorg problemen vertonen, dan kun je een beroep doen op de vijf jaar Eminent garantie. Bewaar deze handleiding samen met het bewijs van aankoop daarom zorgvuldig.

*Registreer je aankoop nu op [www.eminent-online.com](http://www.eminent-online.com) en ontvang product updates!*

### 2.1 Functies en kenmerken

Met het Eminent ADSL2/2+ modem ben je in staat om snel en eenvoudig verbinding te maken met het internet en een bedraad netwerk op te zetten met behulp van slechts één enkel apparaat! De EM4206 is geschikt voor ADSL over een analoge telefoonlijn. De EM4207 is geschikt voor ADSL over een ISDN telefoonlijn.

### 2.2 Inhoud van de verpakking

De volgende onderdelen dienen in het pakket aanwezig te zijn:

- EM4206 ADSL modem/router analoog of EM4207 ADSL modem/router ISDN.
- Lichtnet adapter.
- Een 'rechte' UTP kabel.
- Modulaire telefoon kabel.
- Gebruikershandleiding.

### 2.3 Uitleg van de lampjes

PWR	Gaat branden als de router aan staat.
PPP	Geeft aan dat er een PPP sessie tot stand is gebracht. (bij gebruik van een PPPoA of PPPoE provider.)
LAN 1,2,3 en 4	Deze lampjes gaan branden als de netwerk kabels op de router correct zijn aangesloten. Deze lampjes gaan knipperen als er data verkeer is over de desbetreffende netwerkkabel.
ADSL	Dit lampje brandt continue als het ADSL signaal op de telefoonlijn is gevonden. Het kan circa 60 seconden duren voordat dit lampje continue gaat branden. Als dit lampje blijft knipperen of uit blijft, dien je de ADSL lijn en de splitter te controleren. Het modem ontvangt geen correct signaal.

## 3.0 Configuratie via de installatiewizard

De makkelijkste manier om de router te installeren is met behulp van de installatiewizard, zoals staat beschreven in dit hoofdstuk. Indien je bij de installatie van de modemrouter geen gebruik wilt maken van de wizard op de meegeleverde CD-rom, kun je de modemrouter ook handmatig installeren.

1. Schakel je computer in.
2. Plaats de cd-rom in de cd-rom speler.
3. De wizard wordt gestart.
4. Volg de stappen op het scherm totdat de installatie voltooid is. Je hebt nu een werkende internetverbinding.

*Indien je geen gebruik wenst te maken van de installatie CD-rom, kun je de modemrouter ook handmatig instellen. Ga hiervoor verder met punt 4.1.*

## 4.0 De modemrouter handmatig aansluiten

Voor de handmatige installatie van de modem router is het van belang dat je internetbrowser en je netwerk goed zijn geconfigureerd. De instellingen staan automatisch goed, tenzij je in het verleden iets hebt veranderd. Kijk in de Eminent Advanced Manual op de cd-rom als je twijfelt of je internetbrowser en je netwerk goed zijn ingesteld.

### 4.1 Het aansluiten van de modem/router

1. Schakel je computer uit.
2. Sluit de modemrouter met de meegeleverde lichtnetadapter aan op het stopcontact.
3. Sluit de meegeleverde modulaire kabel aan op de DSL poort van de modemrouter.
4. Sluit de andere kant van de modulaire telefoonkabel aan op de ADSL splitter (Deze splitter is niet meegeleverd).
5. Sluit de meegeleverde netwerkkabel aan op een van de vier LAN-poorten van je modemrouter.
6. Sluit de andere kant van de netwerkkabel aan op de netwerkadapter van je computer.

### 4.2 De modemrouter handmatig configureren voor het internet

Om de modemrouter te kunnen configureren voor verbinding met het internet, dien je eerst verbinding te maken met de router. Je maakt verbinding met de router door de onderstaande procedure te volgen.

1. Open je internet browser (Internet Explorer, Firefox, Safari).
2. Typ in de adresbalk: 'http://192.168.1.1'.
3. Druk op de enter-toets of klik op 'Ga naar'.
4. De gebruikersnaam is standaard ingesteld op 'Admin'.
5. Het wachtwoord is standaard ingesteld op 'Admin'.
6. Klik op 'Ok'.
7. Je hebt nu toegang tot het welkomsscherm van de modemrouter.

#### 4.2.1 Configuratie voor PPP providers

1. Klik boven in het menu op 'Wizard'.
2. Klik in het linker menu op 'Wizard'.
3. Klik op 'Country'.
4. Kies je land (Bijvoorbeeld 'Netherlands').
5. Klik op 'ISP'.
6. Kies je provider (Bijvoorbeeld 'ADSL KPN').
7. Klik op 'Next' om verder te gaan.
8. Bij 'Set PPP Password' vul je de ADSL-gebruikersnaam en wachtwoord in.
9. Klik op 'Apply' om de instellingen op te slaan en de modemrouter te herstarten.

*Let op! Het opstarten van de modemrouter kan enige ogenblikken duren! Wanneer de modemrouter volledig is opgestart beschik je over een internetverbinding.*

#### 4.2.2 Configuratie voor 1483 Bridged providers

1. Klik boven in het menu op 'Wizard'.
2. Klik in het linker menu op 'Wizard'.
3. Klik op 'Country'.
4. Kies je land (Bijvoorbeeld 'Netherlands').
5. Klik op 'ISP'.
6. Kies je provider (Bijvoorbeeld 'BabyXL').
7. Bij 'Connection Type' kies je 'DHCP' als standaard.
8. Klik op 'Next' om verder te gaan.
9. Klik op 'Apply' om de instellingen op te slaan en de modemrouter te herstarten.

*Let op! Het opstarten van de modemrouter kan enige ogenblikken duren! Wanneer de modemrouter volledig is opgestart beschik je over een internetverbinding.*

#### 4.2.3 Configuratie voor overige providers

Raadpleeg de verbindingsgegevens van je internetprovider.

1. Klik op boven in het menu op 'Config'.

2. Klik op 'New Connection'.
3. Vul de gegevens die je van je internetprovider ontvangen hebt in.
4. Klik op 'Apply'.
5. Klik op 'Save All' (Linker kolom).
6. Klik op 'Save' (rechtsonder) om de modemrouter opnieuw op te starten.

*Let op! Het opstarten van de modemrouter kan enige ogenblikken duren! Wanneer de modemrouter volledig is opgestart beschik je over een internetverbinding.*

## 5.0 Geavanceerde instellingen / Firewall

Het menu 'Advanced' stelt je in staat een aantal geavanceerde instellingen te wijzigen. Een aantal van deze opties vereist zeer specifieke kennis van netwerken en is hierdoor niet geschikt voor beginnende gebruikers.

### 5.1 Het instellen van de klok (SNTP)

De ingebouwde klok in de modemrouter kan worden gesynchroniseerd met het internet.

1. Klik op 'Advanced'.
2. Klik op 'SNTP'
3. Vink 'Enable SNTP' aan.

Vul het IP-adres van een time-server in (bijvoorbeeld '212.204.235.152').

Een volledige lijst met adressen van time-servers vind je op:

<http://ntp.isc.org/bin/view/Servers/WebHome>

### 5.2 Port Forwarding (Firewall)

Dit apparaat beschikt over een ingebouwde firewall. Dit houdt in dat alle externe data waarom niet wordt gevraagd, niet door de router wordt doorgestuurd naar de computers "achter de router". Alle normale verkeer waar je zelf om vraagt, wordt gewoon doorgestuurd.

Programma's die niet geschikt zijn voor gebruik achter een firewall zullen niet goed werken, tenzij je de firewall in de router configureert.

Enkele voorbeelden van programma's waarvoor je de firewall zult moeten instellen zijn bijv. spelletjes die je zelf host, of programma's zoals Edonkey, VNC enzovoort.

Wil je dergelijke applicaties gebruiken, dan dien je eerst je lokale IP-adres te achterhalen.

Via het menu 'LAN clients' in de router, dien je een systeem te definiëren. Je vult de naam van het systeem in, alsmede het IP-adres. Klik op 'apply' om dit te bevestigen.

Hierna kun je via het menu 'port forwarding' rules toepassen op dat IP-adres. Je kiest in het menu voor het LAN IP adres, de categorie, kiest de regel en klikt op 'add' om deze in het rechtermenu te zetten. Klik op 'Apply' om de wijziging te bevestigen.

Klik hierna op 'Save setting and reboot' om de instellingen op te slaan.

### 5.3 IP Filters

Deze optie is exact het omgekeerde van Port Forwarding. Door het toepassen van de regels wordt nu voor bepaalde computers juist het verkeer expliciet tegengehouden. Je kan door deze optie dus het internetverkeer gaan beperken, op basis van poortnummers en IP-adressen.

### 5.4 LAN Clients

De modemrouter zal computers die automatisch een IP-adres opvragen toevoegen als client in deze lijst, zodat je ze kunt selecteren in de Port Forwarding en IP Filter menu's. Als je echter computers met vaste IP-adressen gebruikt, dien je deze handmatig als LAN-client toe te voegen. Dit kan door eenvoudig de hostname en het IP-adres in te vullen, het MAC-adres is niet verplicht.

### 5.5 Bridge filters

Via dit menu is het mogelijk om op basis van MAC-adres een aantal gedefinieerde types verkeer te blokkeren binnen je netwerk. Deze optie staat standaard uit, gebruik ervan wordt afgeraden voor beginnende gebruikers.

### 5.6 Static Routing

Via dit menu kun je de routetabel van je modemrouter bijwerken en voor specifieke doelhosts de gateway opgeven.

### 5.7 Dynamic Routing

Door Dynamic routing in te schakelen kun je de modemrouter op RIP V1 of V2 berichten laten reageren. Hierdoor kan de router in een geschikt netwerk, de kortste route naar een host of subnet ontdekken.

*Let op! Nederlandse internetproviders ondersteunen deze optie over het algemeen niet. Schakel deze optie alleen in als je provider het ondersteunt en het gebruik ervan heeft toegestaan.*

## 6.0 Service en ondersteuning

Deze handleiding is door de technische experts van Eminent met zorg opgesteld.

Mocht je desondanks problemen ervaren bij de installatie of in het gebruik van je Eminent product, dan kun je een email sturen naar [support@eminent-online.com](mailto:support@eminent-online.com). Je kunt tevens gebruik maken van het Eminent servicenummer. Bel 0900-EMINENT (0900-3646368) of, in geval je woonachtig bent in Vlaanderen 0900-70090. (45ct per minuut exclusief de kosten voor het gebruik van je mobiele telefoon.



# Eminent Advanced Manual

## Inhoudsopgave

Inhoudsopgave.....	9
Waarom een Eminent Advanced Manual? .....	10
Uw tips en suggesties in de Eminent Advanced Manual? .....	10
Service en ondersteuning.....	10
Netwerkinstellingen voor Windows 98 en ME .....	10
Netwerkinstellingen voor Windows 2000 en XP .....	11
Netwerkinstellingen voor Windows Vista .....	12
Het instellen van Internet Explorer 5 en 5.5 .....	12
Het instellen van Internet Explorer 6.....	13
Het instellen van Internet Explorer 7.....	13
DHCP, het automatisch toekennen van IP adressen .....	14
Het vertalen van IP-adressen en domeinnamen .....	14
Een enkel publiek IP-adres gebruiken voor uw gehele netwerk .....	15
Beveiliging voor uw computer en uw netwerk .....	15
Een computer binnen uw netwerk beschikbaar stellen voor internetgebruikers .....	16
Het vereenvoudigen van netwerkbeheer .....	16
Websites met expliciete inhoud blokkeren .....	17
Dataverkeer op pakketniveau controleren .....	17
Een compleet domein blokkeren.....	17
Acties uitvoeren op basis van tijd of datum .....	17
Een veilige verbinding op afstand .....	18
Het op afstand beheren van een netwerk .....	18
Netwerktoegang toewijzen of blokkeren .....	18
Uw draadloze netwerk beveiligen .....	18
Het bereik van uw draadloze netwerk uitbreiden.....	19
Index .....	20

## Waarom een Eminent Advanced Manual?

Eminent heeft de Eminent Advanced Manual speciaal ontwikkeld voor uw gemak! De Eminent Advanced Manual stelt u in staat om de geavanceerde mogelijkheden van uw thuisnetwerk te ontdekken. Zo helpt de Eminent Advanced Manual u bijvoorbeeld op weg bij het instellen van uw firewall zodat u te allen tijde beschikt over optimale beveiliging van uw eigen netwerk. Natuurlijk komt ook de beveiliging van uw draadloze netwerk uitgebreid aan bod. Met de Eminent Advanced Manual beschikt u over een schat aan informatie en over een handig naslagwerk. Zo beschikt u op een eenvoudige manier over functies die voorheen enkel beschikbaar waren voor professionele en ver gevorderde gebruikers.

## Uw tips en suggesties in de Eminent Advanced Manual?

De Eminent Advanced Manual is tot stand gekomen in samenwerking met een aantal tevreden Eminent gebruikers. Wilt u graag dan een bepaalde optie wordt opgenomen in de Eminent Advanced Manual of heeft u suggesties of tips met betrekking tot de Eminent Advanced Manual dan kunt u een bericht sturen naar [communications@eminent-online.com](mailto:communications@eminent-online.com). Uw tips en suggesties zullen worden verzameld en worden verwerkt in de nieuwe editie van de Eminent Advanced Manual.

## Service en ondersteuning

De Eminent Advanced Manual is met zorg opgesteld door gebruikers en technische experts van Eminent. Mocht u desondanks problemen ervaren bij de installatie of in het gebruik van uw Eminent product, dan kunt u een bericht sturen naar [support@eminent-online.com](mailto:support@eminent-online.com).

U kunt tevens gebruik maken van het Eminent servicenummer. Bel 0800-EMINENT (0800-3646368). Vlaamse gebruikers bellen 0800-50150. Met uw mobiele telefoon belt u 0900-EMINENT (0900-3646368) of, in geval u woonachtig bent in Vlaanderen 0900-70090. 45ct per minuut exclusief de kosten voor het gebruik van uw mobiele telefoon.

## Netwerkinstellingen voor Windows 98 en ME

1. Voor Windows 98: Klik met de rechter muisknop op 'Netwerkomgeving' op het bureaublad.
2. Voor Windows ME: Klik met de rechter muisknop op 'Mijn netwerklocaties' op het bureaublad.
3. Kies 'Eigenschappen'.
4. Selecteer 'TCP/IP' van uw netwerkkaart.

5. Klik op 'Eigenschappen'.
6. Kies 'Automatisch een IP adres verkrijgen'.
7. Klik op het tabblad 'WINS configuratie'.
8. Kies 'WINS omzetting uitschakelen'.
9. Klik op tabblad 'DNS configuratie'.
10. Kies 'DNS uitschakelen'.
11. Klik op tabblad 'Gateway'.
12. Verwijder eventueel geïnstalleerde gateways.
13. Klik op 'Ok'.
14. Klik op 'Ok' in het scherm 'Netwerk'.
15. Start uw computer opnieuw op.
16. Klik op 'Start'.
17. Klik op 'Uitvoeren'.
18. Type 'winipcfg'.
19. Klik op 'Ok'.
20. Windows toont het scherm 'IP configuratie'.
21. Selecteer de op het Eminent apparaat aangesloten Ethernet adapter (netwerkkkaart).
22. Klik op 'Alle vrijgeven'.
23. Klik op 'Alle vernieuwen'.
24. Klik op 'Ok'.

## Netwerkinstellingen voor Windows 2000 en XP

1. Klik met de rechter muisknop op 'Mijn netwerkklocaties' op het bureaublad.
2. Kies 'Eigenschappen'.
3. Klik met de rechter muisknop op 'LAN-verbinding'.
4. Kies 'Eigenschappen'.
5. Selecteer 'internet protocol (TCP/IP)'.
6. Klik op 'Eigenschappen'.
7. Kies 'Automatisch een IP adres laten toewijzen'.
8. Kies 'Automatisch een DNS serveradres laten toewijzen'.
9. Klik op 'Ok'.
10. Windows toont het scherm 'Eigenschappen voor LAN-verbinding'.
11. Klik op 'Ok'.
12. Windows 2000: Sluit het scherm 'Netwerk- en inbelverbindingen'.
13. Windows XP: Sluit het scherm 'Netwerkverbindingen'.
14. Start uw computer opnieuw op.
15. Klik op 'Start'.
16. Klik op 'Uitvoeren'.
17. Type 'cmd'.
18. Druk op de enter-toets.
19. Type 'ipconfig /release'.

20. Druk op de enter-toets.
21. Type 'ipconfig /renew'.
22. Druk op de enter-toets.
23. Type 'exit'.
24. Druk op de enter-toets.

## Netwerkinstellingen voor Windows Vista

1. Klik op het Windows Vista logo (startknop).
2. Kies 'Configuratiescherm'.
3. Kies 'Netwerkstatus en -taken weergeven'.
4. Kies 'Netwerkverbindingen beheren'.
5. Klik met de rechter muisknop op 'LAN-verbinding'.
6. Kies 'Inschakelen'.
7. Indien er om uw toestemming gevraagd wordt: kies 'Doorgaan'.
8. Windows Vista schakelt nu de verbinding in.
9. Klik met de rechter muisknop op 'LAN-verbinding'.
10. Kies 'Eigenschappen'.
11. Indien er om uw toestemming gevraagd wordt: kies 'Doorgaan'.
12. Selecteer 'Internet Protocol versie 4 (TCP/IP/IPv4)'.
13. Klik op 'Eigenschappen'.
14. Kies 'Automatisch een IP-adres laten toewijzen'.
15. Kies 'Automatisch een DNS-serveradres laten toewijzen'.
16. Klik op 'OK'.
17. Klik op 'Sluiten'.
18. Windows Vista stelt nu de verbinding opnieuw in.

## Het instellen van Internet Explorer 5 en 5.5

1. Start Internet Explorer.
2. Klik op 'Stop' of wacht tot er wordt aangegeven dat de pagina niet kan worden gevonden.
3. Als wordt gevraagd om verbinding te maken kunt u dit annuleren.
4. Klik op 'Extra'.
5. Klik op 'Internet-opties'.
6. Klik op het tabblad 'Verbindingen'.
7. Klik op 'LAN-instellingen'.
8. Schakel het vinkje bij 'Instellingen van Internet Explorer automatisch vinden' aan.
9. Schakel het vinkje bij 'Automatisch configuratie script gebruiken' uit.
10. Schakel het vinkje bij 'Proxy server gebruiken' uit.
11. Klik op 'OK'.
12. Verwijder eventuele inbelverbindingen met de knop 'Verwijderen'.
13. Klik op 'Instellingen' (helemaal bovenaan) om de wizard Internet te starten.
14. Kies de laatste optie (Ik wil verbinding maken via een LAN netwerk).

15. Klik op 'Volgende'.
16. Selecteer 'Ik maak een verbinding via een LAN netwerk'.
17. Klik op 'Volgende'.
18. Plaats een vinkje bij 'Proxyserver automatisch opsporen'.
19. Klik op 'Volgende'.
20. Selecteer 'Nee'.
21. Klik op 'Volgende'.
22. Klik op 'Voltooien'.
23. Sluit alle vensters en herstart uw computer.

## Het instellen van Internet Explorer 6

1. Start Internet Explorer.
2. Klik op 'Stop' of wacht tot er wordt aangegeven dat de pagina niet kan worden gevonden.
3. Als wordt gevraagd om verbinding te maken kunt u dit annuleren.
4. Klik op 'Extra'.
5. Klik op 'internet-opties'.
6. Klik op het tabblad 'Verbindingen'.
7. Klik op 'LAN-instellingen'.
8. Schakel het vinkje bij 'Instellingen van Internet Explorer automatisch vinden' aan.
9. Schakel het vinkje bij 'Automatisch configuratie script gebruiken' uit.
10. Schakel het vinkje bij 'Proxy server gebruiken' uit.
11. Klik op 'Ok'.
12. Verwijder eventuele inbelverbindingen met de knop 'Verwijderen'.
13. Klik op 'Instellingen' (helemaal bovenaan) om de 'Wizard Nieuwe verbinding' te starten.
14. Klik op 'Volgende'.
15. Selecteer 'Verbinding met het internet maken'.
16. Klik op 'Volgende'.
17. Selecteer 'Ik wil handmatig een verbinding instellen'.
18. Klik op 'Volgende'.
19. Selecteer 'Verbinding maken via een permanente breedband verbinding'.
20. Klik op 'Volgende'.
21. Klik op 'Voltooien'.
22. Sluit alle vensters en herstart uw computer.

## Het instellen van Internet Explorer 7

1. Start Internet Explorer.
2. Klik op 'Stop' of wacht tot er wordt aangegeven dat de pagina niet kan worden gevonden.
3. Als wordt gevraagd om verbinding te maken kunt u dit annuleren.
4. Klik op 'Extra'.

5. Klik op 'internet-opties'.
6. Klik op het tabblad 'Verbindingen'.
7. Klik op 'LAN-instellingen'.
8. Schakel het vinkje bij 'Instellingen automatisch detecteren' aan.
9. Schakel het vinkje bij 'Automatisch configuratie script gebruiken' uit.
10. Schakel het vinkje bij 'Proxy server gebruiken' uit.
11. Klik op 'Ok'.
12. Verwijder eventuele inbelverbindingen met de knop 'Verwijderen'.
13. Klik op 'Instellen' (helemaal bovenaan).
14. Kies uw gewenste soort verbinding.
15. Windows Vista stelt nu uw verbinding in.

## DHCP, het automatisch toekennen van IP adressen

Voor de ontwikkeling van DHCP (Dynamic Host Configuration Protocol) werden TCP/IP instellingen met de hand geconfigureerd op iedere TCP/IP cliënt (zoals bijvoorbeeld uw computer). Dit kan een lastig karwei zijn wanneer het een groot netwerk betreft of als er regelmatig iets moet worden veranderd in het netwerk. Om het altijd opnieuw te moeten instellen van een IP-adres te vermijden werd DHCP ontwikkeld. Met DHCP worden IP-adressen automatisch toegekend wanneer nodig, en vrijgegeven als ze niet langer nodig zijn. Een DHCP server heeft een reeks ('pool') van geldige adressen die hij kan toekennen aan de cliënt. Wanneer een cliënt bijvoorbeeld opstart zal deze een bericht versturen met het verzoek voor een IP-adres. Een DHCP server (er kunnen er meerdere zijn in een netwerk) antwoordt door IP-adres en configuratiegegevens terug te sturen. De cliënt zal een bevestiging van ontvangst versturen waarna de cliënt kan deelnemen aan het netwerk.

## Het vertalen van IP-adressen en domeinnamen

IP-adressen zijn verre van gebruiksvriendelijk. Domeinnamen daarentegen zijn eenvoudiger te onthouden en te gebruiken. Het proces waarin een domeinnaam wordt vertaald in een voor een machine (zoals uw computer) begrijpelijk adres wordt 'nameresolution' genoemd. Het voornoemde proces wordt uitgevoerd door een 'Domain Name System' server. Dankzij DNS gebruikt u domeinnamen in plaats van IP-adressen als u een website bezoekt of een e-mailbericht verstuurd. Een aan DNS verwante optie is Dynamic DNS of DDNS. Wanneer uw provider werkt met dynamische IP-adressen ('dynamisch' betekent in deze dat de IP-adressen frequent wijzigen) en wilt u toch uw IP-adres aan een domeinnaam koppelen dan doet u dit middels DDNS. Immers; wanneer uw provider uw IP-adres verandert dan wijzigt ook het IP-adres waarnaar uw domeinnaam verwijst. Om Dynamic DNS te kunnen

gebruiken dient u zich te registreren bij een Dynamic DNS provider zoals 'www.dyndns.org' en 'www.no-ip.com'.

## Een enkel publiek IP-adres gebruiken voor uw gehele netwerk

Network Address Translation (NAT) is een internetstandaard waarmee een lokaal netwerk gebruik kan maken van privé IP-adressen. Privé IP-adressen zijn adressen die worden gebruikt binnen het eigen netwerk. Privé IP-adressen worden niet op het internet herkend, noch gebruikt. Een IP-adres dat op internet wordt gebruikt wordt ook wel een publiek IP-adres genoemd.

NAT stelt u in staat een enkel publiek IP-adres te delen met meerdere computers in uw netwerk. NAT zorgt ervoor dat de computers in uw netwerk zonder problemen gebruik kunnen maken van het internet. Gebruikers op het internet echter, hebben geen toegang tot de computers in uw netwerk. U begrijpt dat NAT, mede dankzij het feit dat de privé IP-adressen niet zichtbaar zijn op het internet, tevens een bepaalde mate van beveiliging biedt. Gelukkig maken de meeste routers tegenwoordig gebruik van NAT.

## Beveiliging voor uw computer en uw netwerk

Een firewall kan bestaan uit zowel een software- of een hardwarematige oplossing en plaatst als het ware een muur tussen het interne netwerk en de buitenwereld.

Firewalls controleren in de regel zowel inkomend als uitgaand dataverkeer. Firewalls kunnen worden ingesteld om bepaalde informatie vanaf het internet tegen te houden of door te laten. Ook kunnen firewalls worden ingesteld om aanvragen van binnenuit tegen te houden of door te laten. Om een firewall in te stellen worden 'regels', 'rules' of 'policies' gebruikt. Deze geven aan wat een firewall moet tegenhouden of juist moet doorlaten en vormen dus het eigenlijke filter.

De meeste routers zijn voorzien van diverse firewall-functies. Het grote voordeel van een firewall in een router (hardwarematige oplossing) is dat een aanval van buitenaf al wordt afgeslagen voordat uw netwerk wordt bereikt. Wilt u gebruik maken van een softwarematige firewall dan kunt u bijvoorbeeld de in Windows XP Service Pack 2 ingebouwde firewall gebruiken, betere alternatieven zijn het gratis beschikbare ZoneAlarm en de commerciële pakketten Norman, Norton, Panda en McAfee. Deze commerciële pakketten bieden desgewenst ook bescherming tegen virussen.

## Een computer binnen uw netwerk beschikbaar stellen voor internetgebruikers

De DMZ of DeMilitarized Zone vormt de zone tussen de buitenwereld – het internet – en het veilige, interne netwerk. De computer die in de DMZ geplaatst wordt, is bereikbaar vanaf het internet. Dit in tegenstelling tot de computers die zich buiten de DMZ bevinden en dus veilig zijn. De DMZ wordt dan ook vaak gebruikt voor servers die websites hosten. Websites moeten immers toegankelijk zijn vanaf het internet. Ook wanneer men veelvuldig online games speelt plaatst men een computer vaak in een DMZ. Het verdient echter aanbeveling om, wanneer u een computer in de DMZ plaatst, toch een softwarematige firewall (zoals bijvoorbeeld het gratis beschikbare ZoneAlarm) te installeren. Dit omdat de firewall alle poorten van de router opent voor een computer binnen de DMZ. Er is dus geen enkele restrictie op dataverkeer, terwijl dit in sommige situaties toch wenselijk is.

Net als de DMZ functie stelt ook Virtual Server u in staat een computer binnen uw netwerk, ingericht als bijvoorbeeld FTP- of webserver, toegankelijk te maken vanaf het internet. U kunt, wanneer u gebruik maakt van een Virtual Server, poorten opgeven die in de firewall moeten worden geopend. Dit is tevens het belangrijkste verschil met de DMZ: wanneer u een computer in de DMZ plaatst worden alle poorten voor de betreffende computer geopend. Gebruikt u Virtual Server dan kunt u enkel de poorten die voor het gebruik van de betreffende computer van belang zijn openen.

Port Triggering oftewel Special Apps is gebaseerd op hetzelfde principe als Virtual Server. Ook Port Triggering stelt u in staat een computer binnen uw netwerk, ingericht als bijvoorbeeld FTP- of webserver, toegankelijk te maken vanaf het internet. Wanneer u gebruik maakt van Virtual Server, dan blijven de door u toegewezen poorten te allen tijde geopend. Bij Port Triggering echter, worden de betreffende poorten alleen geopend als de betreffende applicatie daarom vraagt.

## Het vereenvoudigen van netwerkbeheer

UPnP 'Universal Plug and Play': de naam doet vermoeden dat UPnP erg lijkt op het bekende – en beruchte – 'Plug & Play'. Niets is minder waar. UPnP is een heel andere techniek. De insteek is dat UPnP apparaten in staat moeten zijn via TCP/IP met elkaar te communiceren ongeacht het besturingssysteem, de programmeertaal en de hardware. UPnP dient het leven van de gebruiker aanzienlijk makkelijker te maken. Naast de producten van een beperkt aantal andere fabrikanten, ondersteunen de meeste netwerkproducten van Eminent UPnP. Meer informatie over UPnP vindt u op de navolgende website: [www.upnp.org](http://www.upnp.org).



## Websites met expliciete inhoud blokkeren

Parental Control stelt u in staat een of meerdere computers binnen uw netwerk de toegang tot het internet te ontfangen. Parental Control bestaat veelal uit meerdere functies zoals bijvoorbeeld 'URL Blocking'. Deze functie blokkeert websites middels zogenaamde 'Key Words' of steekwoorden. Websites met expliciete inhoud worden zo geblokkeerd. Vaak wordt 'URL Blocking' gecombineerd met tijd en/of datum blokkades. Dergelijke blokkades stellen u in staat internettoegang per tijdseenheid toe te laten of juist tegen te houden. Om uw eigen schema van blokkades op te stellen maakt u gebruik van 'rules', 'regels' of 'polities' (zie ook 'Schedule Rule'). Deze 'regels' beschrijven precies wanneer en waarop een bepaalde actie, in dit geval een blokkade, moet worden toegepast.

## Dataverkeer op pakketniveau controleren

Het pakketfilter (of 'Packet Inspection') is een programma dat datapakketten controleert terwijl ze passeren. Dit intelligente pakketfilter controleert de passerende datastroom of bedrijfsspecifieke definities zoals het IP- of gebruikersadres, tijd en datum, functie en tal van andere definities. Het pakketfilter is het best voor te stellen als een portier. De portier screent de voorbijgangers: "wie bent u en wat is uw bestemming?" De voorbijgangers die de portier als onveilig of onbetrouwbaar beschouwd worden tegengehouden.

In de meeste apparatuur hoeft u het pakketfilter niet te configureren. U hoeft de optie slechts in te schakelen. Het gebruik van deze optie wordt dan ook beslist aangeraden.

## Een compleet domein blokkeren

Een domeinfilter of 'Domain Filter' stelt u in staat een compleet domein te blokkeren. Een domein is een locatie op Internet zoals een website. Een 'Domain Filter' vertoont dus grote gelijkenis met een 'URL Filter', ware het niet dat een 'Domain Filter' het gehele domein blokkeert. Wanneer u bijvoorbeeld uw kinderen wilt beschermen voor expliciete inhoud op een bepaalde website dan kunt u naast het blokkeren van de website middels steekwoorden (zie: 'Parental Control') ook de gehele website blokkeren. Dit doet u middels het 'Domain Filter'.

## Acties uitvoeren op basis van tijd of datum

Met de optie 'Schedule Rule' configureert u wanneer een bepaalde optie actief mag zijn. Stelt u zich voor dat u uw 'Virtual Server' op gezette tijden toegankelijk wilt maken. Dan gebruikt u 'Schedule Rule' om in te stellen wanneer internetgebruikers uw Virtual Server mogen benaderen. Buiten de ingestelde periode is het vervolgens internetgebruikers niet toegestaan verbinding te maken met uw Virtual Server.

'Schedule Rule' is een handige optie om bepaalde toegangsblokkades te automatiseren.

## Een veilige verbinding op afstand

VPN (Virtual Private Networking) stelt u in staat een beveiligde verbinding te creëren, zodat u bijvoorbeeld thuis gebruik kunt maken van uw bedrijfsnetwerk. Een VPN verbinding is in feite niets meer dan een sterk beveiligde tunnel die, gebruikmakend van het internet, verbinding maakt met een andere computer of netwerk. Wanneer data verstuurd via een VPN wordt ontvangen door derden dan nog is de data onbruikbaar dankzij geavanceerde encryptietechnieken.

## Het op afstand beheren van een netwerk

Simple Network Management Protocol (SNMP) is een beheersfunctie die u in staat stelt informatie uit de router te verzamelen. Voornoemde informatie bestaat uit informatie over het aantal op de router aangesloten computers, hun IP- en MAC-adressen en de hoeveelheid dataverkeer die op het moment van de informatieaanvraag wordt verwerkt. SNMP stelt de systeembeheerder in staat de router op afstand te beheren. Dit gebeurt veelal met speciale applicaties die het SNMP protocol ondersteunen.

## Netwerktogang toewijzen of blokkeren

Een MAC adres is een unieke code waarmee ieder netwerkproduct is uitgerust. Vaak is deze code terug te vinden op een sticker op het product. U kunt het MAC adres ook vinden door op 'Start', 'Uitvoeren' te klikken. Type 'CMD' en druk op enter. Type vervolgens 'ipconfig /all' en druk weer op enter. Bij 'Fysiek Adres' vindt u het MAC adres. Een MAC adres bestaat uit zes paren van ieder twee hexadecimale karakters. Bijvoorbeeld 00-0C-6E-85-03-82. MAC Address Control stelt u in staat om regels op te stellen voor MAC adressen en dus om bepaalde netwerkproducten bijvoorbeeld de toegang tot uw netwerk te ontfeggen. Wanneer u gebruik maakt van een draadloos netwerk kunt u middels MAC adres controle bijvoorbeeld instellen dat uw draadloze netwerkadapter wel verbinding mag maken met uw netwerk, maar de draadloze netwerkadapter van uw buurman niet. MAC Address Control is een mogelijkheid om uw draadloze netwerk naast WEP of WPA van een extra vorm van beveiliging te voorzien.

## Uw draadloze netwerk beveiligen

WEP encryptie is een vorm van beveiliging die het draadloze signaal van uw draadloze router of modem versleutelt zodat de gegevens niet zonder meer door derden kunnen worden onderschept.

Het beveiligingsniveau wordt uitgedrukt in bits. 64-Bit WEP encryptie is het laagste beveiligingsniveau om via 128-Bit uit te komen bij het hoogste beveiligingsniveau dat WEP encryptie te bieden heeft: 256-Bit. Om WEP encryptie in te stellen dient u een hexadecimale tekenreeks of ASCII tekenreeks in te voeren. Hexadecimale tekens bestaan uit de karakters 'A' tot en met 'F' en '0' tot en met '9'. ASCII karakters omvatten alle karakters, inclusief symbolen. Wanneer u de juiste mate van beveiliging hebt gekozen en de sleutel heeft ingevoerd, dan dient u exact dezelfde sleutel ook in te voeren in alle draadloze apparaten binnen hetzelfde netwerk. Hou er rekening mee dat – wanneer u de sleutel in het eerste apparaat activeert – de verbinding met het netwerk wordt verbroken. U herstelt de verbinding door systematisch alle draadloze netwerkproducten van dezelfde sleutel te voorzien.

WPA is een vorm van beveiliging die het draadloze signaal van uw draadloze router of modem versleutelt zodat de gegevens niet zonder meer door derden kunnen worden onderschept. WPA staat voor 'Wi-Fi Protected Access' en is een zeer sterke verbetering van draadloze beveiliging. WPA maakt gebruik van een 'Pre Shared Key (PSK)'. Dit is een sleutel die van tevoren in alle op het draadloze netwerk aangesloten apparaten moet worden ingesteld. Deze WPA sleutel mag niet langer zijn dan 63 (willekeurige) karakters en niet korter dan 8 (willekeurige) karakters. De beste vorm van draadloze beveiliging wordt momenteel echter gevormd door WPA2. Voornoemde standaard wordt slechts door een paar fabrikanten – waaronder Eminent – ondersteund en is daarom moeilijk te combineren met draadloze netwerkproducten van andere merken.

Wanneer u gebruik wilt maken van WPA of misschien zelfs WPA2, verzeker uzelf er dan van dat alle in uw draadloze netwerk opgenomen apparaten deze vormen van beveiliging ondersteuning. Het combineren van verschillende typen beveiliging in een draadloos netwerk is niet mogelijk en resulteren in het verlies van verbinding.

## Het bereik van uw draadloze netwerk uitbreiden

WDS (Wireless Distribution System) or 'Bridging' is een optie waarmee u het bereik van uw draadloze netwerk eenvoudig kunt uitbreiden, mocht de reikwijdte van uw draadloze netwerk beperkt blijken. Via WDS gekoppelde apparaten zijn in staat uw internetverbinding te delen. U hoeft apparaten die WDS ondersteunen dus niet middels een fysieke verbinding (zoals een kabel) onderling te koppelen. In de meeste gevallen herkennen apparaten die WDS of bridging ondersteunen elkaar automatisch. Wanneer u uw netwerk middels WDS of bridging uit wilt breiden maakt u gebruik van een zogenaamde 'Range Extender'. Dit is een apparaat dat grotendeels identiek is aan een 'Access Point'. Het voordeel van het gebruik van een range extender boven een tweede draadloze router – wanneer de tweede router bridging ondersteunt – is dan een range extender aanzienlijk goedkoper is.

# Index

Access point.....	<i>Zie</i> Range extender	Parental Control .....	17
Applicatie .....	16	Plug & Play.....	16
ASCII.....	19	Policies.....	<i>Zie</i> Regels
Bedrijfsnetwerk.....	18	Pool.....	14
Bereik.....	19	Poorten .....	16
Besturingssysteem .....	16	Port Triggering.....	16
Blokkade .....	17	Portier .....	17
Bridging.....	<i>Zie</i> WDS	Pre Shared Key (PSK).....	19
Datastroom.....	17	Privé IP-adressen.....	15
DDNS		Programmeertaal.....	16
Dynamic DNS.....	<i>Zie</i> DNS	Publiek IP-adres .....	15
DHCP		Range extender.....	19
Dynamic Host Configuration		Regels.....	15
Protocol .....	14	Rules.....	<i>Zie</i> Regels
DMZ		Schedule Rule.....	17
DeMilitarized Zone .....	16	sleutel.....	19
DNS		SNMP	
Domain Name System.....	14	Simple Network Management	
Domain Filter.....	17	Protocol .....	18
Domein.....	17	Softwarematige firewall .....	15
Domeinfilter.....	<i>Zie</i> Domain Filter	Steekwoorden .....	<i>Zie</i> Key words
Domeinnaam		Systeembeheerder .....	18
Domeinnamen.....	14	Toegangsblokkades .....	18
Dynamisch .....	14	Tunnel .....	18
Expliciete inhoud.....	17	UPnP	
Firewall.....	15	Universal Plug and Play.....	16
Fysiek adres.....	<i>Zie</i> MAC adres	URL Blocking .....	17
Hardware .....	16	Virtual Server .....	16
Hexadecimale		Virussen .....	15
Hexadecimaal.....	19	VPN	
Key words .....	17	Virtual Private Networking .....	18
MAC Adres.....	18	WDS	
Name resolution .....	14	Wireless Distribution System .....	19
NAT		WEP Encryptie .....	18
Network Address Translation.....	15	Wi-Fi Protected Access .....	<i>Zie</i> WPA
Online games .....	16	WPA.....	19
Packet Inspection .....	17	WPA2.....	19
Pakketfilter .....	<i>Zie</i> Packet Inspection		

# Verklaring van Overeenstemming

Om u te verzekeren van een veilig product conform de richtlijnen opgesteld door de Europese Commissie kunt u een kopie van de Verklaring van Overeenstemming met betrekking tot uw product opvragen door een emailbericht te sturen naar: [info@eminent-online.com](mailto:info@eminent-online.com). U kunt ook een brief sturen naar:

Eminent Computer Supplies  
Postbus 276  
6160 AG Geleen  
Nederland

Vermeld bij uw aanvraag duidelijk 'Verklaring van Overeenstemming' en het artikelnummer van het product waarvan u de Verklaring van Overeenstemming opvraagt.



Trademarks: all brand names are trademarks and/or registered trademarks of their respective holders.

The information contained in this document has been created with the utmost care. No legal rights can be derived from these contents. Eminent cannot be held responsible, nor liable for the information contained in this document.



Eminent is a member of the Intronic Group