*Eminent Advanced Manual voor netwerkinstellingen en uitgebreide informatie over thuisnetwerken vanaf pagina 12.*

HANDLEIDING

# EM4219 - wSURF ISDN Draadloos ADSL2/2+ Modem

WWW.EMINENT-ONLINE.COM

# EM4219 - wSURF ISDN Draadloos ADSL2/2+ Modem

## Waarschuwingen en aandachtspunten

Als gevolg van Europese regelgeving kan een draadloos product in sommige Europese lidstaten onderwerp zijn van beperkingen. Ook kan het gebruik van dit product in sommige Europese lidstaten in het geheel verboden zijn. Het openen van het product en/of de producten kan leiden tot ernstige verwondingen! Laat een reparatie altijd uitvoeren door gekwalificeerd personeel van Eminent!

## Inhoudsopgave



*Eminent Advanced Manual voor netwerkinstellingen en uitgebreide informatie over thuisnetwerken vanaf pagina 12.*

# 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 en ontvang product updates!*

## *2.1 Functies en kenmerken*

De Eminent wSURF is een draadloos ADSL2/2+ ISDN modemrouter dat je een stabiele, draadloze internetverbinding biedt. Door de routerfunctie kun je deze internetverbinding vervolgens delen met alle computers in je huis, zowel draadloos als bekabeld.

## *2.2 Inhoud van de verpakking*

De volgende onderdelen zijn aanwezig in het pakket:

- EM4219, wSURF Draadloze ADSL2/2+ ISDN modemrouter.
- Lichtnetadapter.
- Modulaire telefoon kabel.
- UTP netwerkkabel.
- Cd-rom met installatiewizard en handleidingen.
- Gebruikershandleiding.

## *2.3 Uitleg van de lampjes*

| | |
|---|---|
| *PWR* | *Gaat branden als de wSURF aan staat.* |
| *WL/ACT* | *Gaat branden ten teken dat het draadloze access point actief is.* |
| *LAN1,2,3 en 4* | *Deze lampjes branden constant als op één van de poorten een computer aangesloten is en gaan knipperen als er dataverkeer is over een van de netwerkkabels.* |
| *ADSL* | *Gaat ongeveer 30 seconden na het inschakelen van de wSURF knipperen en zal blijven branden als het ADSL signaal gevonden is (alleen als je een telefoonkabel hebt aangesloten waarop een ADSL signaal aanwezig is).* |
| *PPP* | *Als er een PPPoE of PPPoA verbinding is ingesteld, zal dit lampje gaan branden zodra de verbinding correct werkt.* |

# 3.0 Installatie met behulp van de wizard

De makkelijkste manier om de wSURF te installeren is met behulp van de installatiewizard, zoals staat beschreven in dit hoofdstuk. Indien je bij de installatie van de wSURF geen gebruik wilt maken van de wizard op de meegeleverde cd-rom, kun je verder gaan met hoofdstuk 4.

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

# 4.0 Handmatige installatie

Voor de handmatige installatie van de wSURF is het van belang dat je internet browser en je netwerk goed zijn geconfigureerd. De instellingen staan automatisch goed, tenzij je in het verleden iets hebt veranderd. Kijk in de handleiding op de cd-rom als je twijfelt of je internet browser en je netwerk goed zijn ingesteld.

## *4.1 Het aansluiten van de wSURF*

1. Schakel je computer uit.
2. Sluit de wSURF middels de meegeleverde lichtnetadapter aan op het stopcontact.
3. Sluit de telefoonkabel aan op de ‘ADSL’-poort van de wSURF.
4. Sluit de andere kant van deze kabel aan op de ADSL splitter (niet meegeleverd).
5. Sluit een UTP netwerkkabel aan op één van de vier ‘LAN’-poorten van je wSURF.
6. Sluit de andere kant van deze UTP netwerkkabel aan op de netwerkadapter in je computer.

*Is mijn wSURF juist op het lichtnet aangesloten? Dit controleer je door te verifiëren of het 'PWR'-lampje brandt.*

*Is mijn netwerkverbinding correct aangesloten? Schakel je computer in en controleer of het lampje brandt dat correspondeert met de 'LAN'-poort waarop je de UTP netwerkkabel hebt aangesloten. Ook dient het lampje op de netwerkadapter in je computer te branden.*

## *4.2 De wSURF configureren voor verbinding met het internet*

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

1. Schakel je computer in.
2. Open je internetbrowser (Bijvoorbeeld Internet Explorer, Netscape of Firefox).
3. Typ 'http://192.168.1.1' in de adresbalk.
4. Druk op de entertoets of klik op 'Ga naar'.
5. Typ 'admin' in het veld 'User Name' (Let op! Dit veld is hoofdlettergevoelig).
6. Typ 'admin' in het veld 'Password' (Let op! Dit veld is hoofdlettergevoelig).
7. Klik op 'Log in'.
8. Het openingsscherm wordt getoond.

*Tip! Om te voorkomen dat onbevoegden toegang kunnen krijgen tot je wSURF is het nodig dat je het wachtwoord wijzigt.*

*1. Klik op 'Tools'.*
*2. Klik op daaronder op 'Password'.*
*3. Typ bij 'Username' 'admin' in.*
*4. Typ bij 'Old Password' het huidige wachtwoord in.*
*5. Typ bij 'New Password' het nieuwe wachtwoord in.*
*6. Typ bij 'Confirmed Password' nogmaals het nieuwe wachtwoord in.*
*7. Klik op de knop 'Submit'.*
*8. Klik daarna op 'Ok'.*

*Noteer hier het nieuwe wachtwoord om in de toekomst instellingen te kunnen wijzigen:*

*User Name:* *admin*
*Password:* _____

### 4.3 Configuratie voor PPP providers (KPN, Planet, XS4All etc.)

1. Klik op ‘Wizard’.
2. Selecteer je land bij ‘Country’ (Bijvoorbeeld ‘Netherlands’).
3. Selecteer je internetprovider bij ‘ISP’ (Bijvoorbeeld ‘ADSL KPN’).
4. Klik op ‘Next’.
5. Typ je ADSL-gebruikersnaam bij ‘Username’.
6. Typ je wachtwoord bij ‘Input Password’.
7. Typ je wachtwoord nogmaals bij ‘Confirm Password’.
8. Klik op ‘Save’ om de instellingen op te slaan en de wSURF te herstarten.

### 4.4 Configuratie voor DHCP providers (Tele2, BabyXL, BBned)

1. Klik op ‘Wizard’.
2. Selecteer je land bij ‘Country’ (Bijvoorbeeld ‘Netherlands).
3. Selecteer je internetprovider bij ‘ISP’ (Bijvoorbeeld ‘BabyXL’).
4. Selecteer ‘DHCP (Get IP dynamically from ISP)’ bij ‘Connection Type’.
5. Klik op ‘Next’.
6. Klik op ‘Save’ om de instellingen op te slaan en de wSURF te herstarten.

### 4.5 Configuratie voor overige providers

Vind je je provider niet in de lijst van de Wizard, dan kun je de juiste instellingsgegevens opvragen bij je provider. Om deze gegevens in te voeren, volg je de onderstaande procedure:

1. Klik op ‘Advanced’.
2. Klik op ‘WAN’.
3. Vul de gegevens in die je van je provider hebt gekregen in.
4. Klik op ‘Add’.
5. Klik op ‘Save’ (rechts bovenin).
6. Klik op ‘Ok’ om de wSURF opnieuw op te starten.

## 5.0 Het draadloze netwerk beveiligen

Omdat ook onbevoegden het signaal van een draadloos netwerk kunnen ontvangen word je aanbevolen om je netwerk te beveiligen. Er zijn verschillende beveiligingsmethoden die het netwerk kunnen beveiligen. Om een methode toe te passen in een netwerk is het noodzakelijk dat alle draadloze netwerkapparatuur deze methode ondersteunt. We raden je aan om de sterkste vorm van draadloze beveiliging in te stellen: WPA2 (WiFi Protected Access).

1. Open je internetbrowser (Bijvoorbeeld Internet Explorer, Netscape of Firefox).

2. Typ ‘http://192.168.1.1’ in de adresbalk.
3. Druk op de entertoets of klik op ‘Ga naar’.
4. Typ ‘admin’ in het veld ‘User Name’ (Let op! Dit veld is hoofdlettergevoelig).
5. Typ je wachtwoord in het veld ‘Password’ (Let op! Dit veld is hoofdlettergevoelig). Het wachtwoord is ‘admin’ als je het niet hebt veranderd.
6. Klik op ‘Advanced’.
7. Klik op ‘Wireless’.
8. Klik op ‘Security’.
9. Ga voor WPA2 beveiliging verder met paragraaf 5.1 (aanbevolen) of ga voor WEP beveiliging verder met paragraaf 5.2.

*WPA2 beveiliging wordt ondersteund vanaf Windows XP. Dit type beveiliging kan dus niet gebruikt worden onder oudere Windows versies, tenzij de software van je draadloze netwerkadapter WPA2 ondersteunt. Beschik je niet over Windows Vista, Windows XP of over de juiste software, ga dan verder met paragraaf 5.2.*

## 5.1 WPA2 beveiliging (aanbevolen)

1. Kies bij ‘Encryption’ voor ‘WPA2 (AES)’.
2. Kies bij ‘WPA Authentication Mode’ voor ‘Personal (Pre-Shared Key)’.
3. Kies bij ‘Pre-Shared Key Format’ voor ‘Passphrase’.
4. Typ bij ‘Pre-Shared Key’ een wachtwoord in. Bijvoorbeeld ‘uwnaam01’. Gebruik hierbij geen leestekens en let erop dat het wachtwoord minimaal 8 karakters lang is!
5. Noteer het gekozen wachtwoord*.
6. Klik op ‘Submit’.
7. Klik op ‘Save’ (rechts bovenin) om de instellingen op te slaan.

## 5.2 WEP beveiliging

1. Kies bij ‘Encryption’ voor ‘WEP’.
2. Klik op de knop ‘Set WEP Key’.
3. Er komt een nieuw scherm tevoorschijn.
4. Kies bij ‘Key Length’ voor 64 of 128 bit.
5. Kies bij ‘Key Format’ voor ‘ASCII’ of ‘Hex’.
6. Kies bij ‘Default Tx Key’ voor ‘Key 1’.
7. Typ bij ‘Encryption Key 1’ een wachtwoord in. Gebruik hierbij geen leestekens en let erop dat het wachtwoord precies 5, 10, 13 of 26 karakters lang is, afhankelijk van de eerder gekozen instellingen.
8. Noteer het gekozen wachtwoord*.
9. Klik op ‘Submit’.
10. Klik op ‘Save’ (rechts bovenin) om de instellingen op te slaan.

*De verbinding wordt verbroken als beveiliging (WPA2, WEP) is ingesteld in de wSURF en dit niet het geval is bij de draadloze netwerkadapter. Wanneer je de beveiliging ook in de draadloze netwerkadapter hebt ingesteld, wordt de verbinding hersteld.*

**Noteer hier het type beveiliging dat je hebt ingesteld en het wachtwoord:*
☐ *WPA2* ☐ *WEP*

*Wachtwoord: _____*

# 6.0 Controle over de internetverbinding

Wil je je draadloze netwerk naast WPA2 of WEP van extra beveiliging voorzien, stel dan MAC Address Control op je wSURF in. Een MAC adres is een unieke code waarmee ieder netwerkproduct is uitgerust. MAC Address Control stelt je in staat om bepaalde netwerkproducten toegang te geven tot je netwerk. Bij àlle andere gebruikers wordt de toegang ontzegd. Als je dus je eigen MAC adres opgeeft, kan niemand anders verbinding maken met jouw netwerk.

*Vaak is het MAC adres terug te vinden op een sticker op het netwerkproduct. Je kunt het ook vinden door onderstaande stappen te volgen.*

1. *Klik op 'Start'.*
2. *Klik op 'Uitvoeren'.*
3. *Typ 'CMD'.*
4. *Druk op de entertoets.*
5. *Typ 'ipconfig /all'.*
6. *Druk op entertoets.*
7. *Bij 'Fysiek Adres' vind je het MAC adres.*

*Tip! Voor jouw veiligheid is de Firewall standaard ingeschakeld. Wij adviseren je echter altijd een virusscanner te gebruiken en deze regelmatig te updaten.*

## *6.1 MAC Address Control, gebruikers blokkeren*

1. Open je internetbrowser (Bijvoorbeeld Internet Explorer, Netscape of Firefox).
2. Typ 'http://192.168.1.1' in de adresbalk.
3. Druk op de entertoets of klik 'Ga naar'.
4. Typ 'admin' in het veld 'User Name' (Let op! Dit veld is hoofdlettergevoelig).
5. Typ je wachtwoord in het veld 'Password' (Let op! Dit veld is hoofdlettergevoelig). Het wachtwoord is 'admin' als je het niet hebt veranderd.
6. Het openingsscherm wordt getoond.
7. Klik op 'Advanced'.
8. Klik op 'Wireless'.
9. Klik op het tabblad 'Access Control'.
10. Selecteer 'Allow Listed'.

11. Vul het MAC adres in van het netwerkproduct dat toegang mag hebben tot je netwerk.
12. Klik op ‘Submit’.
13. Herhaal stap 11 en 12 als je andere netwerkproducten toegang wilt geven tot je netwerk.
14. Klik op ‘Save’ (recht bovenin) om de instellingen op te slaan.
15. Je hebt nu ingesteld welke netwerkproducten uitsluitend toegang hebben tot je netwerk.

# 7.0 WDS, bereik van het netwerk vergroten

De functie WDS is vooral geschikt als het bereik van één draadloze router niet voldoende is om je hele locatie van draadloos internet te voorzien. Met WDS kun je het bereik vergroten door meerdere draadloze routers te installeren die via WDS als “repeater” werken en zo het draadloze bereik vergroten. In deze opstelling kun je met één internetaansluiting voldoen. Alle via WDS gekoppelde routers kunnen op het internet, er hoeft dus geen kabel tussen de LAN of WAN poorten van de routers te worden geplaatst. Via WDS kun je een internetverbinding draadloos delen met andere draadloze routers of access points die WDS ondersteunen.

## *7.1 De WDS functie inschakelen op de wSURF*

Hieronder de instructies voor het gebruik van WDS. In dit voorbeeld worden twee draadloze routers gebruikt, de wSURF is met het internet verbonden. Een (andere) draadloze router versterkt het signaal.

1. Schakel je computer in.
2. Open je internet browser (Bijvoorbeeld Internet Explorer, Netscape of Firefox).
3. Typ ‘http://192.168.1.1’ in de adresbalk.
4. Druk op de entertoets of klik op ‘Ga naar’.
5. Typ ‘admin’ in het veld ‘User Name’ (Let op! Dit veld is hoofdlettergevoelig).
6. Typ ‘admin’ in het veld ‘Password’ (Let op! Dit veld is hoofdlettergevoelig).
7. Klik op ‘Log in’.
8. Het openingsscherm wordt getoond.
9. Klik op ‘Advanced’.
10. Klik op ‘Wireless’.
11. Klik op ‘Setting’.
12. Zet ‘Mode’ op ‘WDS’.
13. Klik op ‘Submit’.
14. Klik op ‘Ok’.
15. Klik bovenin op ‘WDS’.
16. Zet een vinkje bij ‘Enable WDS’.
17. Vul bij ‘Add WDS AP’ het WLAN MAC (BSSID) adres van de andere draadloze router in. Dit MAC adres staat mogelijk op de onderkant van de betreffende router.

18. Indien het MAC adres niet te achterhalen is, kun je via de knop ‘Show AP’ de wSURF laten zoeken naar draadloze netwerken. Noteer het getoonde BSSID van de te koppelen router,daarna kun je het ‘scan’ scherm weer sluiten.
19. Klik op ‘Submit’ als je alles hebt ingevuld.
20. Als je nog meer routers aan je WDS netwerk wilt toevoegen, dan herhaal je de stappen 17 en 18 voor iedere router.
21. Klik bovenin op ‘Save’.
22. Klik op ‘Ok’.

*Om een WDS koppeling op te bouwen, zul je op het ontvangende apparaat het MAC adres van de wSURF in moeten vullen, voor meer informatie verwijzen wij je naar de documentatie van het betreffende apparaat.*

*Als je gebruik maakt van beveiliging op je draadloze netwerk, zul je dat ook moeten instellen op het andere draadloze apparaat. In WDS mode wordt alleen WEP als beveiligingstype ondersteund. Zie hoofdstuk 5.2 voor het instellen van WEP beveiliging.*

## *7.2 Waar moet ik op letten bij het instellen van WDS?*

- Alle routers die gekoppeld worden door WDS moet in dezelfde IP-reeks zitten (bijvoorbeeld 192.168.1.1 voor router A en 192.168.1.200 voor router B). De mogelijkheid bestaat dat je een ‘fixed’ of vast IP-adres moet instellen op het ontvangende apparaat.
- WEP beveiligingssleutel moet gelijk zijn op beide routers.
- De kanalen van de beide draadloze verbindingen moeten gelijk zijn.
- De namen van de draadloze verbindingen hoeven niet gelijk te zijn.
- Het is niet raadzaam MAC Address Control te gebruiken in combinatie met WDS.
- DHCP server(s) op de tweede (of derde of vierde) router moet(en) uitgeschakeld zijn.

*Let op! WPA2 kan niet worden gebruikt bij het beveiligen van de verbinding.*

# 8.0 Vraag & antwoord

*V. Ik krijg de melding ‘Het IP-adres van de netwerkkaart staat verkeerd’. Wat nu?*

A. Deze melding verschijnt in beeld wanneer de PC geen juist IP-adres heeft ontvangen van de router. Controleer of alle kabels goed aangesloten zijn, reset de wSURF en probeer het opnieuw. Bij voorkeur dien je de router bekabeld (dus niet draadloos) in te stellen. Wanneer de verbinding bekabeld tot stand is gebracht, kun je de draadloze verbinding gaan instellen zoals in de handleiding is aangegeven.

*V. Hoe reset ik het modem naar de fabrieksinstellingen?*

A. Volg onderstaande stappen om de wSURF te resetten:
   1. Zet het modem aan en wacht tot deze is opgestart.
   2. Druk gedurende 20 seconden met een paperclip in het kleine gaatje naast de powerknop op de achterkant.
   3. Het modem is gereset.

*V. Mijn draadloze signaal is zwak of onstabiel. Wat kan de oorzaak zijn?*

A. Zet het modem op een andere locatie en kijk of het signaal nu beter is. Plaats het modem bij voorkeur in een open ruimte. De meterkast is bijvoorbeeld een slechte locatie voor een draadloos product.

A. Je kunt het kanaal van het modem veranderen om te zien of dat een sterker signaal oplevert. Dit kan je op de volgende manier doen:
   1. Open je internetbrowser (Bijvoorbeeld Internet Explorer, Netscape of Firefox).
   2. Typ ‘http://192.168.1.1’ in de adresbalk.
   3. Druk op de entertoets of klik op ‘Ga naar’.
   4. Typ ‘admin’ in het veld ‘User Name’ (Let op! Dit veld is hoofdlettergevoelig).
   5. Typ je wachtwoord in het veld ‘Password’ (Let op! Dit veld is hoofdlettergevoelig). Het wachtwoord is ‘admin’ als je het niet hebt veranderd.
   6. Klik op ‘Advanced’.
   7. Klik op ‘Wireless’
   8. Kies bij ‘Channel’ een ander kanaal, bijvoorbeeld 3.
   9. Klik op ‘Submit’.
   10. Klik bovenin op ‘Save’.
   11. Klik op ‘Ok’.

# 9.0 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.

Je kunt tevens gebruik maken van het Eminent servicenummer. Bel 0900-EMINENT (0900-3646368, 45ct per minuut*) of, in geval je woonachtig bent in Vlaanderen 0900-70090 (50ct per minuut*).

*Exclusief de kosten voor het gebruik van je mobiele telefoon.

# Eminent Advanced Manual

## Inhoudsopgave

# 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. 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.

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 (netwerkkaart).
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 netwerklocaties’ 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 entertoets.
19. Type ‘ipconfig /release’.

20. Druk op de entertoets.
21. Type ‘ipconfig /renew’.
22. Druk op de entertoets.
23. Type ‘exit’.
24. Druk op de entertoets.

# 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 word: 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 word: 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 registeren 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 toegangkelijk 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, toegangkelijk 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, toegangkelijk 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’.

# Websites met expliciete inhoud blokkeren

Parental Control stelt u in staat een of meerdere computers binnen uw netwerk de toegang tot het internet te ontzeggen. 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 ‘policies’ (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 creeeren, 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.

## Netwerktoegang 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 ontzeggen. 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

# 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. 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.

EMINENT

**WWW.EMINENT-ONLINE.COM**



CE

Eminent is a member of the Intronics Group