EMINENT

MODE D'EMPLOI

EM4218 - wSURF Routeur modem ADSL2/2+

WWW.EMINENT-ONLINE.COM

EM4218 - wSURF Routeur modem ADSL2/2+

Avertissements

Suite aux réglementations européennes, un produit sans fil peut être sujet à des limitations dans certains états membres européens. Il est également possible que l'usage de ce produit soit totalement interdit dans certains états membres de l'Europe. L'ouverture du produit et/ou des produits peut entraîner de graves lésions! Faites toujours faire vos réparations par le personnel qualifié d'Eminent!

Table des matières

On page 13 you will find the Eminent Advanced Manual for networking settings and information about home networking. (English only)

1.0 Conditions de garantie

Une période de garantie de cinq ans est accordée pour tous les produits Eminent, sauf indication contraire au moment de l'achat. Lors de l'achat d'un produit Eminent en seconde main, la période de garantie est maintenue compte tenu de la date d'achat par le premier propriétaire.

Le règlement de garantie Eminent est d'application sur tous les produits et les éléments Eminent qui sont indissociablement liés au produit concerné. Les alimentations, les piles, les batteries, les antennes et tous les autres produits qui ne sont pas intégrés ni directement liés au produit principal ou les produits dont il peut être raisonnablement accepté qu'ils connaissent une usure différente de celle du produit principal ne tombent pas sous le règlement de garantie Eminent. La garantie est annulée en cas d'utilisation erronée ou illicite, d'influences externes et/ou en cas d'ouverture du boîtier du produit concerné par des parties autres qu'Eminent.

2.0 Introduction

Félicitation pour l'achat de ce produit Eminent de haute qualité! Ce produit a été amplement testé par les experts techniques d'Eminent. Si, malgré tous nos soins, ce produit présentait un quelconque défaut, vous pouvez faire appel durant cinq ans à la garantie Eminent. Conservez donc soigneusement ce manuel ensemble avec la preuve d'achat.

Enregistrez votre achat maintenant sur www.eminent-online.com et recevez les mises à jour du produit!

2.1 Fonctions et caractéristiques

Le EM4218 d'Eminent est un routeur modem ADSL2/2+ sans fil qui vous offre une connexion internet stable sans fil. Ce routeur intégré vous permet de partager cette connexion internet avec tous les ordinateurs que vous avez à la maison, tant sans fil qu'avec câble.

2.2 Contenu du conditionnement

Les éléments suivants sont présents dans votre boîte:

- Le EM4218, routeur modem ADSL2/2+ sans fil.
- Adaptateur réseau.
- Le câble de téléphone modulaire
- Câble de réseau UTP.
- CD-rom avec wizard d'installation et les manuels.
- Le manuel d'utilisation.

2.3 Explication des lampes témoins

PWR	*S'allume lorsque le EM4218 est allumé.*
WL/ACT	*S'allume pour avertir que le point d'accès sans fil est actif.*
LAN1,2,3 en 4	*Ces lampes témoins brûlent en permanence lorsqu'un ordinateur est connecté à une des portes et elles clignotent lorsqu'il y a du trafic de données sur un des câbles réseau.*
ADSL	*Se met à clignoter environ 30 secondes après avoir allumé votre EM4218 et continue à brûler lorsque le signal ADSL a été trouvé (uniquement si vous avez connecté un câble de téléphone sur lequel un signal ADSL est présent).*
PPP	*Lorsqu'une connexion PPPoE ou PPPoA a été installée, ce témoin brûlera dès que la connexion fonctionne correctement.*

3.0 Installation à l'aide du wizard

La manière la plus facile d'installer l'EM4218 est d'utiliser le wizard d'installation comme décrit dans ce chapitre. Si lors de l'installation de votre EM4218, vous ne désirez pas utiliser le wizard du CD-rom fourni, vous pouvez continuer au chapitre 4.

1. Allumez votre ordinateur.
2. Placez le CD-rom dans le lecteur de CD-rom ou de DVD de votre ordinateur.
3. Le programme s'ouvre automatiquement.
4. Suivez les étapes à l'écran jusqu'à ce que l'installation soit achevée. Vous disposez maintenant d'une connexion internet en service.

4.0 Installation manuelle

Pour l'installation manuelle du EM4218, il est important que votre navigateur internet et votre réseau soient correctement configurés. Les réglages sont automatiquement bons, à moins que vous n'ayez changé quelque chose auparavant. Consultez le manuel sur le CD-rom si vous avez des doutes quant à la configuration de votre navigateur internet et de votre réseau.

4.1 La connexion du EM4218

1. Eteignez votre ordinateur.
2. Connectez le EM4218 à une prise de courant à l'aide de l'adaptateur de réseau électrique fourni.
3. Connectez le câble de téléphone à la porte ADSL du EM 4218.
4. Connectez l'autre côté de ce câble au splitter ADSL (non livré).
5. Connectez un câble de réseau UTP à une des quatre portes "LAN" de votre EM4218.

6. Connectez l'autre côté de ce câble réseau UTP à l'adaptateur réseau de votre ordinateur.

Est-ce que mon EM4218 est correctement connecté au réseau électrique? Contrôlez-le en vérifiant si la lampe témoin "PWR" brûle.

Est-ce que ma connexion réseau est correcte? Allumez votre ordinateur et contrôlez si la lampe témoin qui correspond avec la porte "LAN" à laquelle vous avez connecté votre câble réseau UTP brûle. Le témoin de l'adaptateur de réseau électrique de votre ordinateur doit également brûler.

4.2 Configurer le EM4218 pour la connexion avec internet

Pour configurer le EM4218 pour la connexion avec l'internet, vous devez d'abord réaliser une connexion avec le EM4218.
Pour réaliser la connexion avec le EM4218, suivez la procédure ci-dessous.

1. Allumez votre ordinateur.
2. Ouvrez votre navigateur internet (Par exemple Internet Explorer, Netscape ou Firefox).
3. Tapez "http://192.168.1.1" dans la barre d'adresse.
4. Appuyez sur la touche "enter" ou cliquez sur "Allez vers".
5. Tapez "admin" dans le champ "User Name" (Attention, ce champ est sensible aux majuscules).
6. Tapez "admin" dans le champ "Password" (Attention, ce champ est sensible aux majuscules).
7. Cliquez sur "Log in".
8. L'écran d'accueil apparaît.

Conseil! Pour éviter que des personnes non compétentes aient accès à votre EM4218, il est nécessaire de changer le mot de passe.

1. *Cliquez sur "Tools".*
2. *Cliquez sur "Password".*
3. *Tapez "admin" dans le champ "Username".*
4. *Tapez le mot de passe actuel dans le champ "Old Password".*
5. *Tapez le nouveau mot de passe dans le champ "New Password".*
6. *Tapez encore une fois le nouveau mot de passe dans le champ "Confirmed Password".*
7. *Cliquez sur le bouton "Submit".*
8. *Cliquez ensuite sur "Ok".*

Notez ici le nouveau mot de passe afin de pouvoir modifier les paramètres à l'avenir:

Nom d'utilisateur: admin
Mot de passe: _____

4.3 Configuration pour un fournisseur d'accès PPP (KPN, Planet, XS4All etc.)

1. Cliquez sur "Setup Wizard".
2. Sélectionnez votre pays auprès de "Country" (Par exemple "Belgique").
3. Sélectionnez votre fournisseur internet auprès de "ISP" (Par exemple "ADSL KPN").
4. Cliquez sur "Next".
5. Tapez votre nom d'utilisateur ADSL auprès de "Username".
6. Tapez votre mot de passe auprès de "Input Password".
7. Tapez à nouveau votre mot de passe auprès de "Confirm Password".
8. Cliquez sur "Save" pour enregistrer les paramètres et redémarrer le dSURF.

4.4 Configuration pour un fournisseur d'accès DHCP (Tele2, BabyXL, BBned)

1. Cliquez sur "Setup Wizard".
2. Sélectionnez votre pays auprès de "Country" (Par exemple "Belgique").
3. Sélectionnez votre fournisseur internet auprès de "ISP" (Par exemple "BabyXL").
4. Sélectionnez "DHCP (Get IP dynamically from ISP)" auprès de "Connection Type".
5. Cliquez sur "Next".
6. Cliquez sur "Save" pour enregistrer les paramètres et redémarrer le dSURF.

4.5 Configuration pour les autres fournisseurs d'accès

Si vous ne trouvez pas votre fournisseur d'accès sur la liste du Wizard, vous pouvez demander les données de réglage exactes à votre fournisseur d'accès. Pour introduire les données, suivez la procédure ci-dessous:

1. Cliquez sur "Advanced".
2. Cliquez sur "WAN".
3. Remplissez les données que vous avez reçues de votre fournisseur d'accès.
4. Cliquez sur "Add".
5. Cliquez sur "Save" (en haut à droite).
6. Cliquez sur "Ok" pour redémarrer le dSURF.

5.0 Protection du réseau sans fil

Etant donné que des personnes non autorisées peuvent également recevoir le signal d'un réseau sans fil, nous vous conseillons de protéger votre réseau. Il existe plusieurs méthodes pour protéger votre réseau. Pour appliquer une certaine méthode dans un réseau, il est nécessaire que tous les appareils de ce réseau sans fil supportent cette méthode. Nous vous recommandons d'installer la protection d'un réseau sans fil la plus puissante : WPA2 (WiFi Protected Access).

1. Ouvrez votre navigateur internet (Par exemple Internet Explorer, Netscape ou Firefox).
2. Tapez "http://192.168.1.1" dans la barre d'adresse.
3. Appuyez sur "enter" ou cliquez sur "Allez vers".
4. Tapez "admin" dans le champ "User Name". (Attention, ce champ est sensible aux majuscules.)
5. Tapez votre mot de passe dans le champ "Password". (Attention, ce champ est sensible aux majuscules.) Le mot de passe est "admin" si vous ne l'avez pas changé.
6. Cliquez sur "Advanced".
7. Cliquez sur "Wireless".
8. Cliquez sur "Security".
9. Pour la protection WPA2 poursuivez avec le paragraphe 5.1 (recommandé) ou pour la protection WEP poursuivez au paragraphe 5.2.

La protection WPA2 est soutenue à partir de Windows XP. Ce type de protection ne peut donc pas être utilisé avec des anciennes versions de Windows, à moins que le logiciel de votre adaptateur de réseau sans fil soutienne WPA2. Si vous ne possédez pas Windows Vista, Windows XP ou le logiciel exact, poursuivez avec le paragraphe 5.2.

5.1 Protection WPA2 (recommandée)

1. Choisissez "WPA2 (AES)" auprès de "Encryption".
2. Choisissez "Personal (Pre-Shared Key)" auprès de "WPA Authentication Mode".
3. Choisissez "Passphrase" auprès de "Pre-Shared Key Format".
4. Tapez un mot de passe à côté de "Pre-Shared Key". Par exemple "votrenom01". N'utilisez pas de signes de ponctuation et veillez à ce que votre mot de passe compte au moins 8 caractères!
5. Notez le mot de passe choisi*.
6. Cliquez sur "Submit".
7. Cliquez sur "Save" (en haut à droite) pour enregistrer les paramètres.

5.2 Protection WEP

1. Choisissez "WEP" auprès de "Encryption".
2. Cliquez sur le bouton "Set WEP Key".
3. Un nouvel écran apparaît.
4. Choisissez 64 ou 128 bit auprès de "Key Length".
5. Choisissez "ASCII" ou "Hex" auprès de "Key Format".
6. Choisissez "Key 1" auprès de "Default Tx Key".
7. Tapez un mot de passe à côté de "Encryption Key 1". N'utilisez pas de signes de ponctuation et veillez à ce que votre mot de passe compte exactement 5, 10, 13 ou 26 selon les paramètres déjà choisis.
8. Notez le mot de passe choisi *.
9. Cliquez sur "Submit".
10. Cliquez sur "Save" (Notez le nom de réseau et le mot de passe choisi).

La liaison est interrompue lorsque la protection (WPA2, WEP) est installée sur le EM4218 et que ce n'est pas le cas dans l'adaptateur de réseau sans fil. Lorsque la protection est également installée dans l'adaptateur de réseau sans fil, la liaison est restaurée.

** Notez ici le type de protection que vous avez installé et le mot de passe:*
☐ *WPA2* ☐ *WEP*

Mot de passe: _____

6.0 Contrôle de la connexion internet

Si en plus du WPA2 ou WEP, vous désirez installer une protection supplémentaire sur votre réseau sans fil, installez le MAC Address Control sur votre EM4218. Une adresse MAC est un code unique dont tout apareil en réseau est équipé. Le MAC Address Control vous permet de donner accès à votre réseau à certains appareils de réseau. L'accès est refusé à tout autre utilisateur. Si vous indiquez donc uniquement votre propre adresse MAC, personne d'autre ne peut réaliser une connexion avec votre réseau.

L'adresse MAC se trouve souvent sur un autocollant sur le produit de réseau. Vous la trouverez également en suivant les étapes ci-dessous.

1. *Cliquez sur "Start".*
2. *Cliquez sur "Exécuter".*
3. *Tapez "CMD".*
4. *Appuyez sur "Enter".*
5. *Tapez "ipconfig /all".*
6. *Appuyez sur "Enter".*
7. *Vous trouverez l'adresse MAC auprès de "Adresse physique".*

Conseil! Le Firewall est installé par défaut pour votre propre sécurité. Nous vous conseillons cependant d'utiliser toujours un scanner de virus et de le mettre régulièrement à jour.

6.1 Contrôle de l'adresse MAC, bloquer des utilisateurs

1. Ouvrez votre navigateur internet (Par exemple Internet Explorer, Netscape ou Firefox).
2. Tapez "http://192.168.1.1" dans la barre d'adresse.
3. Appuyez sur la touche "enter" ou cliquez sur "Allez vers".
4. Tapez "admin" dans le champ "User Name". (Attention, ce champ est sensible aux majuscules.)
5. Tapez votre mot de passe dans le champ "Password". (Attention, ce champ est sensible aux majuscules.) Le mot de passe est "admin" si vous ne l'avez pas changé.
6. L'écran d'ouverture apparaît.
7. Cliquez sur "Advanced".
8. Cliquez sur "Wireless".
9. Cliquez sur l'intercalaire "Access Control".

10. Sélectionnez "Allow Listed".
11. Remplissez l'adresse MAC du produit de réseau qui peut avoir accès à votre réseau.
12. Cliquez sur "Submit".
13. Répétez l'étape 11 et 12 si vous désirez donner accès à votre réseau à d'autres appareils de réseau.
14. Cliquez sur "Save" (en haut à droite) pour enregistrer les paramètres.
15. Vous avez déterminé ainsi quels sont les appareils de réseau qui ont exclusivement accès à votre réseau.

7.0 WDS, augmenter la portée du réseau

La fonction WDS convient surtout pour augmenter la portée d'un réseau sans fil et pour permettre la connexion de tout votre réseau à internet. A l'aide de WDS, vous pouvez augmenter la portée en installant plusieurs routeurs sans fil qui fonctionnent comme "repeater" et qui augmentent ainsi via WDS la portée sans fil. Cette configuration ne nécessite qu'une seule connexion internet.
Tous les routeurs connectés via WDS ont accès à internet, il ne faut donc pas installer de câble entre les portes LAN ou WAN des routeurs. Via WDS, vous pouvez partager une connexion internet sans fil avec d'autres routeurs ou access points sans fil qui soutiennent WDS.

7.1 Installer la fonction WDS sur l'EM4218

Suivez les instructions ci-dessous pour utiliser le WDS. Dans cet exemple, deux routeurs sans fil sont utilisés, le EM4218 est connecté à internet. Un (autre) routeur sans fil amplifie le signal.

1. Allumez votre ordinateur.
2. Ouvrez votre navigateur internet (Par exemple Internet Explorer, Netscape ou Firefox).
3. Tapez "http://192.168.1.1" dans la barre d'adresse.
4. Appuyez sur "Enter" ou cliquez sur "Allez vers".
5. Tapez "admin" dans le champ "User Name" (Attention, ce champ est sensible aux majuscules).
6. Tapez "admin" dans le champ "Password" (Attention, ce champ est sensible aux majuscules).
7. Cliquez sur "Log in".
8. L'écran d'accueil apparaît.
9. Cliquez sur "Advanced".
10. Cliquez sur "Wireless".
11. Cliquez sur "Setting".
12. Réglez le "Mode" sur "WDS".
13. Cliquez sur "Submit".
14. Cliquez sur "Ok".

15. Cliquez dans le menu supérieur sur "WDS".
16. Cochez "Enable WDS".
17. Remplissez auprès de "Add WDS AP" l'adresse WLAN MAC (BSSID) de l'autre routeur sans fil. Cette adresse MAC se trouve probablement sur le fond du routeur concerné.
18. Si vous ne trouvez pas cette adresse MAC, vous pouvez faire chercher les réseaux sans fil par le EM4218 via le bouton "Show AP". Notez le BSSID du routeur à connecter, ensuite refermez l'écran "Show Ap".
19. Cliquez sur "Submit" lorsque vous avez tout rempli.
20. Si vous désirez encore ajouter des routeur à votre réseau WDS, vous répétez les étapes 17 et 18 pour chaque routeur.
21. Cliquez en haut sur "Save".
22. Cliquez sur "Ok".

Pour créer une connexion WDS, vous devrez remplir l'adresse MAC du EM 4218 sur l'appareil réceptionnant, pour plus d'information, nous vous renvoyons à la documentation de l'appareil concerné.

Si vous utilisez une protection sur votre réseau sans fil, vous devrez également l'installer sur les autres appareils sans fil. En mode WDS, seul WEP est soutenu comme type de protection. Voir chapitre 5.2 pour l'installation de la protection WEP.

7.2 A quoi dois-je faire attention lors de l'installation du WDS?

- Tous les routeurs qui sont connectés par WDS doivent se trouver dans la même série IP (Par exemple 192.168.1.1 pour le routeur A et 192.168.1.200 pour le routeur B). Il est possible que vous deviez donner une adresse IP fixe à l'appareil réceptionnant.
- La protection WEP doit être identique sur les deux routeurs.
- Les canaux des connexions sans fil doivent être identiques.
- Les noms (SSID) des connexions sans fil ne doivent pas être identiques.
- Il n'est pas conseillé d'utiliser le MAC Address Control en combinaison avec WDS.
- Le(s) serveur(s) DHCP sur le deuxième (ou troisième ou quatrième) routeur doi(ven)t être éteint(s).

Attention! WPA2 ne peut pas être utilisé pour protéger la connexion.

8.0 Questions & réponses

Q. Je reçois le message "L'adresse IP de la carte réseau est incorrecte". Que faire?

R. Ce message apparaît lorsque l'ordinateur n'a pas reçu l'adresse IP exacte du routeur. Contrôlez si tous les câbles sont bien connectés, faites un reste du EM

4218 et essayez à nouveau. Il est préférable de régler le routeur avec câble (donc pas lorsqu'il est sans fil). Lorsque la connexion avec câble fonctionne correctement, vous pouvez installer la connexion sans câble comme indiqué dans ce manuel.

Q. Comment faire un reset du modem vers les paramètres d'usine?

R. Suivez les étapes ci-dessous pour faire le reset du EM4218:

1. Allumez le modem et attendez qu'il ait démarré.
2. Appuyez durant environ 20 secondes avec un trombone à papier dans le petit trou à côté du bouton pour l'allumer à l'arrière.
3. Le reset du modem est fait.

Q. Mon signal sans fil est faible ou instable. Quelle peut être la cause?

R. Posez le modem à un autre endroit et regardez si le signal est meilleur. Placez le modem de préférence dans un espace ouvert. L'armoire du compteur est par exemple un mauvais endroit pour placer un appareil sans fil.

R. Vous pouvez changer le canal du model pour voir si cela fournit un meilleur signal. Suivez les instructions ci-dessous:

1. Ouvrez votre navigateur internet (Par exemple Internet Explorer, Netscape ou Firefox).
2. Tapez "http://192.168.1.1" dans la barre d'adresse.
3. Appuyez sur "enter" ou cliquez sur "Allez vers".
4. Tapez "admin" dans le champ "User Name". (Attention, ce champ est sensible aux majuscules.)
5. Tapez votre mot de passe dans le champ "Password". (Attention, ce champ est sensible aux majuscules.) Le mot de passe est "admin" si vous ne l'avez pas changé.
6. Cliquez sur "Advanced".
7. Cliquez sur "Wireless"
8. Choisissez un autre canal auprès de "Channel", par exemple 3.
9. Cliquez sur "Submit".
10. Cliquez en haut sur "Save".
11. Cliquez sur "Ok".

9.0 Service et support

Ce manuel a été rédigé soigneusement par les experts techniques de Eminent. Si toutefois vous avez des problèmes lors de l'installation ou de l'utilisation de votre produit Eminent, veuillez dans ce cas remplir le formulaire support sur le site web: www.eminent-online.com/support.

Vous pouvez également téléphoner au numéro du service d'assistance Eminent. Tél: 0900-70090. (50ct par minute, frais d'utilisation de votre téléphone portable non compris.)

Eminent Advanced Manual

Table of contents

Why an Eminent advanced manual?

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

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

Your tips and suggestions in the Eminent Advanced Manual?

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

Service and support

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

Networking settings for Windows 98 and Windows ME)

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

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

Networking settings (Windows 2000 and Windows XP)

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

Configuring Internet Explorer 5 and 5.5

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

Configuring Internet Explorer 6

1. Start Internet Explorer.
2. Click ‘Stop’.
3. When asked to establish a connection, press ‘Cancel’.
4. Click ‘Extra’.
5. Click ‘Internet options’.
6. Click the ‘Connections’ tab.
7. Click the ‘LAN settings’ tab.
8. Uncheck ‘Find Explorer settings automatically’.
9. Uncheck ‘Use configuration script’.
10. Uncheck ‘Use proxy-server’.
11. Click ‘Ok’.
12. Remove dial-up connections by pressing ‘Delete’.
13. Click ‘Settings’ to start the ‘New connection’ Wizard.
14. Click ‘Next’.
15. Select ‘Connect to the Internet’.
16. Click ‘Next’.
17. Select ‘I want to connect to the Internet manually’.

18. Click ‘Next’.
19. Select ‘Permanent broadband connection’.
20. Click ‘Next’.
21. Click ‘Complete’.
22. Close all Windows that are currently open.
23. Restart your PC

DHCP, Automatic allocation of ip-addresses

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

Translating ip-adresses and domain names

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

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

Using a single ip-address for your entire network

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

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

Security for your computer and your network

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

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

Making a computer available for Internet users in your network

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

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

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

Simplifying network management

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

Blocking websites with explicit content

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

Checking data traffic at package level

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

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

Blocking a complete domain

A ‘Domain Filter’ will enable you to block an entire domain. A domain is a location on the Internet such as a website. A Domain Filter is therefore very similar to a ‘URL Filter’, apart from the fact that a Domain Filter blocks the entire domain. If, for example, you wish to protect your children from explicit content on a certain website, as well as blocking the website by way of catchwords (see: ‘Parental Control’), you can block the entire website. You can do this using the Domain Filter.

Carrying out actions based on date or time

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

A safe remote connection

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

Remote network management

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

Allocating or blocking network access

A MAC address is a unique code which each network product has. This code can often be found on a sticker on the product. You can also find the MAC address by clicking on ‘Start’, ‘Execute’. Type ‘CMD’ and press ‘Enter’. Then type ‘ipconfig /all’ and press ‘Enter’ again. The MAC address is shown under ‘Physical Address’. A MAC address consists of six pairs each of two hexadecimal characters. For example, 00-0C-6E-85-03-82. MAC Address Control enables you to set up rules for MAC addresses and therefore to deny for example, certain network products access to your

network. When you use a wireless network, you can meanwhile use MAC Address Control to configure for example, your wireless network adapter to be able to connect to your network without the neighbouring network adapter being able to do so. MAC Address Control is a possibility, as well as WEP or WPA of providing extra security for your wireless network.

Making your wireless network secure

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

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

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

Expanding the range of your wireless network

WDS (Wireless Distribution System) or ‘Bridging’ is an option with which you can easily expand the range of your wireless network should the range of your wireless network remain limited. Appliances linked via WDS can share your Internet connection. You therefore do not need to interlink appliances sharing WDS by way of a physical connection (such as a cable). Appliances supporting WDS or Bridging

recognize one another automatically in most cases. You can use a so-called ‘Range Extender’ if you wish to expand your network using WDS or Bridging. This is an appliance largely similar to an ‘Access Point’. The advantage of using a Range Extender rather than a second router – if the second router bridging is supported – is that a Range Extender is considerably cheaper.

Index

Déclaration de Conformité

Pour vous assurer d'un produit fiable conforme aux directives établies par la Commission Européenne, vous pouvez demander une copie de la Déclaration de Conformité relative à votre produit en envoyant un email à : info@eminent-online.com. Vous pouvez aussi envoyer une lettre à :

Eminent Computer Supplies
Postbus 276
6160 AG GELEEN
Pays-Bas

Veuillez mentionner clairement dans ce cas 'Déclaration de Conformité' et le numéro d'article du produit pour lequel vous demandez la Déclaration de Conformité.

EMINENT

WWW.EMINENT-ONLINE.COM

EM4218 | 03-2009