EMINENT

MODE D'EMPLOI

EM4450 - Routeur sans fil

WWW.EMINENT-ONLINE.COM

EM4450 - Routeur sans fil

Avertissements et points à surveiller

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!

Sommaire

On page 17 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 Contenu du conditionnement

Les éléments suivants sont présents dans votre boîte:

- EM4450, routeur sans fil.
- Adaptateur réseau.
- Câble de réseau UTP.
- CD-rom avec le programme d'installation et les manuels.
- Le manuel d'utilisation

3.0 Fonctions et caractéristiques

Le EM4450 est idéal pour créer vous-même en un tour de main votre réseau sans fil sécurisé. Le EM4450 est une station de base sans fil permettant de pourvoir toute votre maison d'un réseau sans fil. Les performances de ce routeur sont de haut niveau ce qui vous permet de construire un réseau sans fil stable et souple. Profitez de votre réseau et laissez le EM4450 faire le travail!

- Point d'accès 54Mbps intégré pour établir un réseau sans fil.
- Routeur intégré pour le partage aisé de la connexion internet.
- Switch intégré à 4 portes pour établir un réseau avec fil.
- Pare-feu intégré pour la protection de vos données.

4.0 Installer le routeur

1. Eteignez votre ordinateur.
2. Connectez le EM4450 au moyen de l'adaptateur réseau fourni à une prise de courant.
3. Connectez le câble de réseau UTP livré à la porte "WAN" du EM4450.
4. Connectez l'autre côté du câble réseau UTP livré à la porte "LAN" de votre modem-câble.
5. Connectez un câble de réseau UTP à une des quatre portes "LAN" de votre EM4450.
6. Connectez l'autre côté de ce câble réseau UTP à l'adaptateur de réseau de votre ordinateur.

Conseil: Avant d'entamer l'installation du EM4450, vous devez contrôler s'il est connecté correctement au réseau électrique. Vous pouvez le faire en vérifiant que le témoin indiqué par le pictogramme universel de stand-by est allumé.
Contrôlez également que votre câble de réseau soit bien connecté à votre EM4450 et à votre ordinateur. Pour le contrôler, vous démarrez votre ordinateur et vous contrôlez si le témoin qui correspond à la porte LAN à laquelle vous avez connecté votre câble de réseau brûle.

5.0 Installer le EM4450 à l'aide du CD-rom.

Vous installez votre EM4450 comme routeur sans fil si vous disposez d'un modem-câble ou ADSL. La manière la plus facile d'installer le EM4450 est d'utiliser le programme d'installation, comme décrit dans le chapitre ci-dessous. Si vous ne désirez pas utiliser le programme d'installation du CD-rom, vous pouvez également installer le routeur manuellement. Voir le chapitre 5.2.

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

Conseil: lorsque le CD-rom d'installation ne démarre pas automatiquement, vous pouvez également le faire démarrer manuellement. Suivez les étapes ci-dessous:
1. *Cliquez sur "Start".*
2. *Cliquez sur "Exécuter".*

3. Tapez x:\wizard\wizard.exe ("x" étant la lettre de votre lecteur de CD-rom ou de dvd).
4. Cliquez sur "OK".

6.0 Installer le routeur manuellement

Nous allons décrire à présent les différentes méthodes pour installer votre EM4450. Si votre fournisseur d'accès utilise une certaine méthode d'installation, il vous suffit de suivre les étapes qui sont indiquées. Vous serez rapidement en-ligne.

Exemples de fournisseurs qui utilisent DHCP comme méthode de connexion: @Home, Zeelandnet, Casema Wanadoo et UPC Chello.

6.1 Se brancher sur le EM4450

Pour l'installation manuelle du routeur, il est important que votre navigateur internet et votre réseau soient bien configurés. Les réglages sont automatiquement bons, à moins que vous n'ayez changé quelque chose auparavant.

Conseil: voir le "Advanced Manual" sur le CD-rom si vous n'êtes pas certain que votre navigateur et votre réseau ont été réglés correctement.

Vous établissez une connexion manuelle avec le EM4450 en suivant 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" comme nom d'utilisateur.
6. Tapez "admin" comme mot de passe.
7. Cliquez sur "Ok".
8. L'écran d'ouverture apparaît.

Attention! Afin de pouvoir configurer rapidement votre routeur pour la connexion avec l'internet spécifique à votre provider, vous devez d'abord savoir quelle méthode de connexion est utilisée par votre fournisseur d'accès ("DHCP", "PPPoE", "StaticIP" ou "PPTP"). Vous trouvez ces données dans l'information que vous avez reçue de votre fournisseur d'accès.

6.2 Configuration pour une connexion DHCP

1. Cliquez à gauche dans le menu sur "Network'".
2. Cliquez à gauche dans le menu sur "WAN".
3. Sélectionnez "Dynamic IP".

4. Tapez dans le champ "Hostname", le hostname que vous avez reçu de votre fournisseur d'accès. Par exemple: hostname: CC1234567-a. (uniquement pour une connexion internet @Home).
5. Cliquez à gauche dans le menu sur "MAC Clone". (Uniquement d'application si votre fournisseur utilise l'enregistrement de l'adresse Mac.)
6. Cliquez sur le bouton "Clone MAC Adress"
7. Cliquez sur "Save".
8. Fermez votre navigateur internet.
9. Votre connexion internet sera opérationnelle dans 5 minutes.

Conseil! Si vous utilisez un fournisseur par câble tel que @home, voyez d'abord au chapitre 11, si vous n'avez pas pu réaliser une connexion opérationnelle dans les 5 minutes.

6.3 Configuration pour une connexion internet Static IP

1. Cliquez à gauche dans le menu sur "Network".
2. Cliquez à gauche dans le menu sur "WAN".
3. Sélectionnez "Static IP".
4. Tapez dans le champ "Static IP Address" l'adresse IP que vous avez reçue de votre fournisseur d'accès.
5. Tapez dans le champ "Static Subnet Mask" le subnet mask que vous avez reçu de votre fournisseur d'accès.
6. Tapez dans le champ " Default Gateway" l'adresse gateway que vous avez reçue de votre fournisseur d'accès.
7. Tapez dans le champ "Primary DNS" l'adresse DNS primaire que vous avez reçue de votre fournisseur d'accès.
8. Tapez dans le champ "Secondary DNS" l'adresse DNS secondaire que vous avez reçue de votre fournisseur d'accès. Si vous n'avez pas reçu d'adresse DNS secondaire, vous laissez ce champ vide.
9. Cliquez sur "Save".
10. Fermer votre navigateur internet.
11. Votre connexion internet sera opérationnelle dans 5 minutes.

6.4 Configuration pour une connexion internet PPPoE

1. Cliquez à gauche dans le menu sur "Network".
2. Cliquez à gauche dans le menu sur "WAN".
3. Sélectionnez "PPPoE".
4. Tapez dans le champ "User Name" le nom d'utilisateur que vous avez reçu de votre fournisseur d'accès.
5. Tapez dans le champ "Password" le mot de passe que vous avez reçu de votre fournisseur d'accès.
6. Cliquez sur "Save".
7. Fermer votre navigateur internet.

8. Votre connexion internet sera opérationnelle dans 5 minutes.

6.5 Configuration pour une connexion internet PPtP

1. Cliquez à gauche dans le menu sur "Network".
2. Cliquez à gauche dans le menu sur "WAN".
3. Sélectionnez "PPtP".
4. Tapez dans le champ "User Name" le nom d'utilisateur que vous avez reçu de votre fournisseur d'accès.
5. Tapez dans le champ "Password" le mot de passe que vous avez reçu de votre fournisseur d'accès.
6. Tapez dans le champ "Server IP Address" l'adresse gateway de votre modem ADSL.
   (Pour les modems Speedtouch Home, elle est par défaut 10.0.0.138).
7. Tapez dans le champ " IP Address" l'adresse IP de votre modem ADSL.
   (Pour les modems Speedtouch Home , elle est par défaut 10.0.0.150).
8. Tapez dans le champ "My Subnet Mask" le subnetmask de votre modem ADSL.
   (Pour les modems Speedtouch Home, elle est par défaut 255.255.255.0).
9. Tapez dans le champ "Gateway" l'adresse gateway de votre modem ADSL.
   (Pour les modems Speedtouch Home, elle est par défaut 10.0.0.138).
10. Cliquez sur "Save".
11. Fermer votre navigateur internet.
12. Votre connexion internet sera opérationnelle dans 5 minutes.

7.0 Installer la protection 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. La protection d'un réseau sans fil la plus puissante est WPA (WiFi Protected Access).

La manière la plus facile de protéger votre réseau sans fil est à l'aide du programme d'installation, tel que décrit ci-dessous. Si lors de l'installation du EM4450 vous ne voulez pas faire usage du programme d'installation sur le CD-rom fourni, vous pouvez également régler la protection manuellement. Voir le chapitre 8 à cet effet.

1. Allumez votre ordinateur.
2. Placez le CD-rom dans le lecteur de CD-rom.
3. Le programme d'installation démarre.
4. Sélectionnez la langue désirée et cliquez sur "Next".
5. Sélectionner "Installer la protection sans fil" et cliquez sur "Suivant".
6. Suivez les étapes à l'écran jusqu'à ce que l'installation soit achevée. Vous disposez à présent d'un réseau sans fil protégé.

Attention! La protection WPA est soutenue à partir de Windows 2000. Ce type de protection ne peut donc pas être utilisé sous Windows 98 et ME! Si vous ne possédez pas Windows Vista, XP ou Windows 2000, utilisez une protection WEP.

8.0 Installation manuelle de la protection dans le routeur

A part l'installation à l'aide du CD-rom, vous pouvez également installer la protection manuellement. Dans le chapitre suivant, nous vous expliquons comment faire. Eminent conseille le cryptage WPA parce que c'est actuellement la meilleure méthode de protection.

8.1 Installation manuelle de la protection WPA via le routeur

1. Allumez votre ordinateur.
2. Ouvrez votre navigateur internet (Par exemple Internet Explorer, Netscape ou Firefox).
3. Videz la barre d'adresse et tapez-y ensuite: http://192.168.1.1
4. Appuyez sur la touche enter ou cliquez sur "Allez vers".
5. Tapez "admin" comme nom d'utilisateur.
6. Tapez "admin" comme mot de passe.
7. Cliquez sur "Ok".
8. L'écran d'ouverture apparaît.
9. Cliquez à gauche dans le menu sur "Wireless".
10. Cliquez à gauche dans le menu sur "Wireless Settings".
11. Cochez "Enable Wireless Security".
12. Sélectionnez auprès de "Security Type" le type de sécurité désiré, dans ce cas WPA-PSK/WPA2-PSK
13. Auprès de "Security Option", vous choisissez WPA-PSK.
14. Auprès de "Encryption", vous choisissez TKIP.
15. Allez maintenant vers "PSK Passphrase". Sur cet écran, vous pouvez remplir le code de sécurité souhaité. A cet effet, vous pouvez utiliser n'importe quels chiffres et lettres. Tenez cependant compte du fait qu'une sécurité WPA doit contenir au minimum 8 caractères et au maximum 63. Notez éventuellement ce code.
16. Cliquez sur "Save".
17. Cliquez sur "Ok", et à nouveau sur "OK". Le routeur enregistrera maintenant les paramètres.

8.2 Installation manuelle de la protection WEP via le routeur

1. Allumez votre ordinateur.
2. Ouvrez votre navigateur internet (Par exemple Internet Explorer, Netscape ou Firefox).
3. Videz la barre d'adresse et tapez-y ensuite : http://192.168.1.1
4. Appuyez sur la touche enter ou cliquez sur "Allez vers".
5. Tapez "admin" comme nom d'utilisateur.
6. Tapez "admin" comme mot de passe.
7. Cliquez sur "Ok".
8. L'écran d'ouverture apparaît.
9. Cliquez à gauche dans le menu sur "Wireless".
10. Cliquez à gauche dans le menu sur "Wireless Settings".
11. Cochez "Enable Wireless Security".
12. Sélectionnez auprès de "Security Type" le type de sécurité désiré, dans ce cas WEP.
13. Sélectionnez à présent le type de Clef: vous pouvez choisir 64 bit ou 128 bit.
14. Pour une protection de 64bit, remplissez un mot de passe d'exactement 10 caractères. Cela peut être des chiffres ou des lettres. Si vous choisissez des lettres, vous pouvez utiliser les lettres de A à F. Si vous utilisez une protection 128bit, votre code doit contenir exactement 26 caractères. Cela peut également être des chiffres et des lettres. Si vous choisissez des lettres, vous pouvez utiliser les lettres de A à F.
15. Vous aurez besoin plus tard du code que vous venez d'introduire. Si nécessaire, inscrivez ce code.
16. Cliquez sur "Save".
17. Cliquez sur "Ok", et à nouveau sur "OK". Le routeur enregistrera maintenant les paramètres.

Attention! Eminent conseille d'installer la protection lorsque vous avez câblé votre routeur à votre ordinateur.

Notez ici le type de protection que vous avez installé, le nom de réseau et le mot de passe:

☐ *WPA* ☐ *WEP*

Nom de réseau: _____

Mot de passe: _____

8.3 Installation manuelle de la protection WPA/WPA2 avec Radius via le routeur

Le EM4450 dispose également de la possibilité d'installer une protection WPA/WPA2 via ce qu'on appelle un Radius Server. Il s'agit d'un type de protection qui n'est utilisé que dans un environnement d'entreprise avec un propre serveur Radius.

9.0 Installer le réseau sans fil sur l'ordinateur.

Maintenant que le routeur est protégé, l'ordinateur même doit être réglé de telle façon qu'il reconnaisse et puisse se connecter au réseau sans fil protégé
Windows XP et Windows Vista sont actuellement les systèmes de gestion les plus utilisés. Nous allons vous expliquer comment réaliser une connexion sans fil avec ces systèmes.

Conseil: Après que le routeur ait été installé avec une protection WEP ou WPA, vous pouvez retirer le câble réseau de l'ordinateur avant de commencer à l'étape 9.1.

9.1 Installer un réseau sans fil sous Windows XP.

Pour établir la connexion sans fil sous Windows XP, vous devez effectuer les étapes suivantes:

1. Démarrez votre ordinateur.
2. Cliquez sur "Start".
3. Allez vers "l'écran de configuration".
4. Sur l'écran de configuration, sélectionnez "Connexions réseau".
5. Si tout va bien, vous voyez à présent la carte ou l'adaptateur sans fil. Cliquez dessus avec le bouton droit de la souris.
6. Choisissez à présent "Afficher les réseaux sans fil disponibles ". Une liste des réseaux sans fil présents est affichée.
7. Sur la liste des réseaux sans fil disponibles, vous sélectionnez votre propre réseau.
8. Lorsque vous choisissez "Réaliser une connexion", votre ordinateur donnera un avertissement que ce réseau est protégé et qu'une clef de réseau est nécessaire.
9. Remplissez la clef de protection et choisissez "Réaliser la connexion".
10. Si votre clef a été introduite correctement, Windows indiquera après un certain temps que votre réseau est connecté. Vous êtes en-ligne.

9.2 Installer un réseau sans fil sous Windows Vista.

Pour établir la connexion sans fil sous Windows Vista, vous devez effectuer les étapes suivantes:

1. Cliquez sur "start"

2. Cliquez sur "l'écran de configuration "
3. Choisissez "Réseau et Internet".
4. Allez vers le "Centre de réseaux".
5. Au côté gauche du menu qui apparaît, vous choisissez "Gestion des réseaux sans fil"
6. Sur cette fenêtre, vous choisissez "Ajouter"
7. A l'écran suivant, vous choisissez "Ajouter un réseau sans fil à portée de cet ordinateur".
8. Dans la nouvelle fenêtre, vous choisissez votre propre réseau.
9. Cliquez à présent sur "Réaliser la connexion"
10. Votre ordinateur affichera le message suivant: “Donnez une clef pour la protection réseau ou le mot de passe pour le réseau”.
    Remplissez la clef de protection.
11. Choisissez "Réaliser la connexion". Si votre clef a été introduite correctement, Windows indiquera après un certain temps que votre réseau est connecté. Vous êtes en-ligne.

10.0 Contrôle de la connexion internet

Le EM4450 dispose d'un pare-feu avancé. Il vous donne le contrôle presque total de la connexion internet. Le pare-feu vous permet de faire des réglages par lesquels vous interdisez à des ordinateurs d'aller sur internet durant un certain temps. Vous pouvez également bloquer des sites internet. Cela peut être temporairement, en permanence, durant certaines heures, par exemple, les heures de bureau.

10.1 Installer le pare-feu

Pour régler les paramètres dans le pare-feu, nous allons d'abord le rendre actif. Suivez les étapes ci-dessous:

1. Ouvrez votre navigateur internet (Par exemple Internet Explorer, Netscape ou Firefox).
2. Videz la barre d'adresse et tapez-y ensuite : http://192.168.1.1
3. Appuyez sur la touche enter ou cliquez sur "Allez vers".
4. Tapez "admin" comme nom d'utilisateur. Tapez "admin" comme mot de passe.
5. Cliquez sur "OK".
6. L'écran d'ouverture apparaît.
7. Cliquez à gauche dans le menu sous "Advanced Settings" sur "Security".
8. Cochez "Enable Firewall" dans le champ qui s'est ouvert.
9. Cliquez sur "Save".
10. Le pare-feu est actif.

10.2 Interdire l'accès à internet via des adresses IP

Le pare-feu vous permet d'interdire l'accès à internet à un ordinateur à l'aide de l'adresse IP. Pour utiliser cette option, l'option "IP-Adress Filtering" doit être active. Pour activer cette option, suivez les mêmes étapes qu'au chapitre 10.1. Cependant, à l'étape 8, vous cochez "Enable IP-Adress Filtering". Suivez ensuite les étapes 9 et 10.

1. Cliquez à gauche de l'écran sous "Advanced Settings" sur l'option "IP Adress Filtering".
2. A l'écran suivant, vous cliquez sur "Add New".
3. Vous pouvez remplir les données à l'écran qui apparaît à présent.
4. Cliquez dans le champ "Effective time".

Dans ce champ, vous pouvez introduire les heures durant lesquelles l'ordinateur ne peut pas être en-ligne. Si vous désirez que l'ordinateur ne puisse pas être en ligne de 10 heures du matin à 8 heures du soir, vous remplissez "1000" dans la première case de "Effective time". Dans la seconde case, vous remplissez 2000.

5. Auprès de "Lan IP Adress", vous remplissez l'adresse IP de l'ordinateur auquel vous désirez interdire l'accès durant les heures indiquées, par exemple "192.168.1.5".
6. Auprès de "Action" , vous choisissez "Deny"
7. Cliquez à présent sur "Save".
8. Durant les heures indiquées, l'accès à l'internet sera à présent impossible pour l'ordinateur avec l'adresse IP que vous avez introduite.

Conseil: Au chapitre 11, il est expliqué comment vous pouvez obtenir l'adresse IP d'un ordinateur.

10.3 Interdire l'accès à internet avec "Domain Filtering".

Avec le EM4450, il est possible d'interdire certains domaines ou sites internet. Si par exemple, vous désirez que vos enfants ne puissent pas ouvrir certains sites, vous pouvez le régler. Pour activer cette option, vous suivez les mêmes étapes qu'au chapitre 10.1. Cependant, à l'étape 8, vous cochez "Enable Domain Filtering". Suivez ensuite les étapes 9 et 10.

1. Cliquez à gauche de l'écran sur "Domain Filtering"
2. Cliquez sur "Add New"
3. Cliquez dans le champ "Effective time".

Dans ce champ, vous pouvez introduire les heures durant lesquelles l'ordinateur ne peut pas être en-ligne. Si vous désirez que l'ordinateur ne puisse pas être en ligne de 10 heures du matin à 8 heures du soir, vous remplissez "1000" dans la première case de "Effective time". Dans la seconde case, vous remplissez 2000.

1. Auprès de "Domain Name", vous pouvez indiquer les domaines ou sites internet qui ne peuvent pas être visités durant les heures indiquées. Si vous désirez par exemple que personne ne puisse aller sur <www.google.be> durant les heures indiquées, vous remplissez le nom de ce site auprès de "Domain Name".
2. Dans le champ "Status", "Enabled" doit être actif.
3. Cliquez à présent sur "Save".
4. Durant les heures indiquées, l'accès aux domaines ou aux sites internet indiqués n'est plus autorisé.

10.4 Interdire l'accès à internet via "MAC Address Filtering"

En plus des méthodes ci-dessus, il existe encore une manière pour bloquer l'accès à internet. Cette méthode est d'ailleurs la plus efficace. Elle interdit l'accès total à l'internet et vous ne devez pas indiquer d'heures. Pour activer cette option, suivez les mêmes étapes qu'au chapitre 10.1. Cependant, à l'étape 8, vous cochez "Enable Mac-address filtering". Suivez ensuite les étapes 9 et 10.

1. Cliquez à gauche de l'écran sur "MAC Filtering"
2. A l'écran suivant, vous cliquez sur "Add New"
3. Auprès de " MAC Address", vous remplissez l'adresse Mac désirée.
4. Auprès de "Description", vous pouvez donner une description. Vous pouvez par exemple remplir le nom de celui qui ne peut plus aller sur internet.
5. Dans le champ "Status", "Enabled" doit être actif.
6. Cliquez à présent sur "Save".
7. Dorénavant, l'accès à internet est entièrement bloqué pour l'adresse Mac indiquée.

Conseil: Au chapitre 11, il est expliqué comment vous pouvez obtenir l'adresse Mac d'un ordinateur.

11.0 Questions fréquentes

Q: Je reçois le message " L'adresse IP de la carte réseau est erronée". Que faire?
R: Ce message apparaît à l'écran lorsque l'ordinateur n'a pas reçu d'adresse IP correcte du routeur. Contrôlez si tous les câbles sont bien accouplés, redémarrez le EM4450 si nécessaire et essayez à nouveau. Il est préférable de régler le routeur lorsqu'il est relié par câble (donc pas sans fil). Lorsque la connexion avec câble est établie, vous pouvez installer la connexion sans câble comme indiqué dans ce manuel.

Q: J'ai installé le routeur. Tout va bien, sauf l'accès à l'internet. Mon fournisseur d'accès est Chello.
R: Veillez à ce que l'adresse Mac correcte ait été sélectionnée durant l'installation. Ce message apparaît lorsqu'une adresse Mac erronée est sélectionnée.

Q: J'ai installé le routeur. Tout va bien, sauf l'accès à l'internet. Mon fournisseur d'accès est Chello/@Home/Casema ou un autre fournisseur d'accès DHCP.
R: Dans certains cas, il est possible que le modem ne puisse pas donner d'accès internet au routeur. Vous pouvez suivre les étapes suivantes pour malgré tout réaliser la connexion:

1. Eteignez le routeur et le modem.
2. Attendez environ 10 minutes.
3. Allumez le modem, attendez qu'il ait entièrement démarré, allumez le routeur et laissez-le également entièrement démarrer.
4. La connexion devrait fonctionner à présent.

Q: J'ai essayé la solution précédente, mais cela ne fonctionne toujours pas. Que dois-je faire?
R: Il existe encore une autre méthode:

1. Branchez-vous à la page du routeur via http://192.168.1.1
2. Nom d'utilisateur: admin, Mot de passe: admin
3. Vous êtes à présent branché à l'écran principal du EM4050.
4. Dévissez maintenant le câble coax de votre modem.
5. Sur la page du routeur, vous cliquez sous "WAN" sur "Renew"
6. Une adresse IP de votre modem apparaît à présent à l'écran. C'est généralement l'adresse suivante: 192.168.100.x
7. Revissez le câble coax à votre modem et attendez jusqu'à ce que le témoin Online/Internet brûle à nouveau.
8. Cliquez à présent dans l'écran du routeur sur "Renew".
9. Si tout va bien, l'adresse IP qui est fournie par votre fournisseur d'accès apparaît maintenant à l'écran. Dans ce cas, votre connexion internet est opérationnelle.

Q: Je désire connaître mon adresse IP. Comment dois-je faire?
R: Pour connaître votre adresse IP, suivez les étapes ci-dessous.

Etapes pour Windows XP/2000 et Windows Vista:

1. Cliquez sur "Start".
2. Allez vers "Exécuter".
3. Remplissez ici: "cmd"
4. Appuyez sur la touche Enter ou cliquez sur "OK"
5. Remplissez: ipconfig".
6. Appuyez à nouveau sur la touche Enter.
7. Vous voyez à présent l'adresse IP.

Etapes pour Windows98/ME:

a. Cliquez sur "Start".
b. Allez vers "Exécuter".
c. Remplissez ici "winipcfg".
d. Appuyez sur la touche Enter ou cliquez sur "OK".
e. Vous voyez à présent l'adresse IP ou l'adresse personnelle automatique.

Q: Je désire connaître l'adresse Mac de ma carte réseau. Comment dois-je faire?
R: Pour connaître l'adresse Mac de votre carte réseau, suivez les étapes ci-dessous:

Etapes pour Windows XP/2000 et Windows Vista:

1. Cliquez sur "Start".
2. Allez vers "Exécuter ".
3. Remplissez ici: "cmd"
4. Appuyez sur la touche Enter ou cliquez sur "OK"
5. Remplissez: ipconfig /all".
6. Appuyez à nouveau sur la touche Enter.
7. Vous voyez à présent "l'adresse physique". C'est l'adresse Mac de votre carte de réseau.

Etapes pour Windows98/ME:

1. Cliquez sur "Start".
2. Allez vers "Exécuter".
3. Remplissez ici "winipcfg".
4. Appuyez sur la touche Enter ou cliquez sur "OK".
5. Vous voyez à présent "l'adapteradres" ou l'adresse Mac de votre carte de réseau.

Q: Comment faire le reset de mon EM4450?
R: Vous faites un reset de votre EM4450 en sortant d'abord la fiche de courant de votre routeur. Ensuite, vous appuyez avec une trombone sur le bouton "reset". Remettez ensuite la fiche de courant dans le EM4450, en continuant à pousser sur le bouton "reset" avec la trombone. Sur le routeur, le témoin "Sys" va s'allumer. Attendez qu'il se mette à clignoter et retirez ensuite la trombone du bouton "reset". Le EM4450 est à présent réinstallé avec les paramètres d'usine.

12.0 Service et support

Ce manuel a été rédigé soigneusement par les experts techniques de Eminent.
Si, malgré tout, vous rencontrez des problèmes lors de l'installation ou de l'utilisation de ce produit Eminent en question, vous pouvez envoyer un email à support@eminent-online.com (*English only*).

Vous pouvez également téléphoner au numéro du service d’assistance Eminent. Tél: 0900-70090. (45ct 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

EM4450 | 06-2008