On page 8 you will find the Eminent Advanced Manual for networking settings and information about home networking.

MANUALE

EM8012/EM8013 - adattatore(i) xLINE di rete per prese domestiche

WWW.EMINENT-ONLINE.COM

EM8012/EM8013 - adattatore(i) xLINE di rete per prese domestiche

Avvertenze

L'apertura del prodotto e/o dei prodotti potrebbe causare seri infortuni! Per l'assistenza rivolgetevi esclusivamente a personale qualificato Eminent!

Indice

1.0 Condizioni di garanzia 2
2.0 Introduzione 3
2.1 Funzioni e specifiche 3
2.2 Contenuto della confezione 3
2.3 Prima di iniziare 3
3.0 Come collegare un adattatore xLINE ad un computer 4
3.1 Come collegare un adattatore xLINE Pro ad un modem o ad un router 4
3.2 Come installare il software di sicurezza xLINE 4
3.3 Come rendere sicura la vostra rete domestica xLINE 5
3.4 Aggiungere un nuovo adattatore xLINE alla vostra rete protetta 6
4.0 Domande frequenti 7
5.0 Manutenzione e supporto 7

On page 9 you will find the Eminent Advanced Manual for networking settings and information about home networking. (English only)

1.0 Condizioni di garanzia

La garanzia di 5 anni Eminent si applica a tutti i prodotti Eminent a meno che non diversamente disposto all'atto dell'acquisto. Nel caso un prodotto Eminent sia acquistato di seconda mano il periodo di garanzia parte dal momento dell'acquisto da parte del primo acquirente. La garanzia Eminent si applica a tutti i prodotti Eminent ed alle parti indissolubilmente connesse a e/o montate sul prodotto principale. Gli adattatori di alimentazione, le batterie, le antenne e tutti gli altri prodotti non integrati o non direttamente connessi al prodotto principale e/o i prodotti per i quali, senza ragionevole dubbio, si possa presupporre un discostamento dai normali schemi di usura del prodotto principale non sono coperti dalla garanzia Eminent. I prodotti Eminent non sono coperti da garanzia quando vengono esposti ad uso improprio/scorretto o ad influenze esterne. La garanzia Eminent ugualmente decade qualora i prodotti vengano aperti o ne venga tentata la riparazione da personale non autorizzato da Eminent.

2.0 Introduzione

Congratulazioni per aver acquistato questo prodotto Eminent ad alta qualità! Questo prodotto è stato sottoposto da parte degli esperti Eminent ad un'ampia gamma di test. Va ricordato, qualora si riscontrassero problemi di natura tecnica, che il prodotto Eminent è coperto da una garanzia Eminent della durata di 5 anni. Vi preghiamo, pertanto, di conservare il presente manuale e la ricevuta d'acquisto in un luogo sicuro.

Registrate subito questo prodotto su www.eminent-online.com e riceverete gli aggiornamenti del prodotto!

2.1 Funzioni e specifiche

Non sarebbe fantastico poter disporre di una rete di computer a casa? Ideale, ma spesso difficile da realizzare. Bisognerebbe collegare molti cavi e bucare laddove si preferirebbe evitarlo. Eminent Vi offre una soluzione differente: potrete creare una rete informatica vostra utilizzando l'unica rete già predisposta nella vostra abitazione. Una rete che utilizzate da anni e non vi ha mai deluso. La rete elettrica! Per collegare un solo computer ad Internet potrete utilizzare il kit di base xLINE. Volete collegare un altro computer? Utilizzate semplicemente il kit di estensione xLINE!

2.2 Contenuto della confezione

Prima di iniziare la procedura di installazione vi preghiamo di verificare che tutte le componenti menzionate di seguito siano presenti.

Il kit di estensione Eminent EM8012 xLINE dovrebbe contenere le seguenti parti:

- 1x EM8012 adattatore xLINE per prese domestiche.
- 1x cavo di rete UTP.
- Manuale utente.
- CD-Rom contenente il software di installazione.

Il kit base Eminent EM8013 xLINE dovrebbe contenere le seguenti parti:

- 2x EM8012 adattatori xLINE per prese domestiche.
- 2x cavi di rete UTP.
- Manuale utente.
- CD-Rom contenente il software di installazione

2.3 Prima di iniziare

Prima di avviare la procedura di installazione dovrete verificare:

1. Di avere una connessione di rete perfettamente operativa
2. Di avere configurato le impostazioni di rete in modo corretto (consultate il manuale avanzato presente nel CD ROM).

3.0 Come collegare un adattatore xLINE ad un computer

Se volete condividere una connessione Internet esistente con più di un utente, o se volete semplicemente creare una rete domestica, per prima cosa dovrete connettere l'adattatore xLINE Pro al vostro computer. Lo potete realizzare facilmente seguendo le istruzioni riportate di seguito. Ripetete questi punti per ciascun computer che intendete connettere alla vostra rete domestica xLINE.

1. Collegare l'adattatore Eminent xLINE Pro ad una presa di corrente vicina al computer che intendete mettere in rete.
2. Collegare il cavo di rete UTP fornito nella confezione alla porta di rete sull'adattatore xLINE Pro.
3. Collegare l'altro capo del cavo UTP alla scheda di rete del vostro computer.
4. Ora l'adattatore xLINE Pro è collegato ed installato.

3.1 Come collegare un adattatore xLINE Pro ad un modem o ad un router

Se volete condividere una connessione Internet preesistente con più utenti o se volete spostare la vostra connessione internet in un altro luogo, dovrete collegare un adattatore xLINE Pro ad un modem o ad un router. Sarà sufficiente seguire le indicazioni riportate di seguito:

1. Collegare l'adattatore Eminent xLINE Pro ad una presa di corrente vicina al modem o al router che si intende collegare.
2. Collegare il cavo di rete UTP fornito nella confezione alla porta di rete dell'adattatore xLINE Pro.
3. Collegare l'altra estremità del cavo di rete UTP ad una delle porte di rete del modem o del router che si intende connettere. Queste porte solitamente vengono chiamate porte LAN.
4. L'adattatore xLINE Pro è ora collegato ed installato.

3.2 Come installare il software di sicurezza xLINE

Solitamente tutti gli adattatori xLINE collegati scambiano i dati tra di loro. In alcuni casi è consigliato, quindi, rendere più sicura la propria rete domestica xLINE criptandola. Per prima cosa dovrete installare il software di sicurezza.

1. Accendere il computer
2. Inserire il CD ROM in allegato nel lettore di CD/DVD.
3. Il software wizard partirà automaticamente.
4. Seguire le istruzioni che appariranno sullo schermo sino al termine dell'installazione.

3.3 Come rendere sicura la vostra rete domestica xLINE

Sul vostro desktop troverete un nuovo collegamento chiamato 'Powerpacket Utility'. Potete utilizzare questo collegamento per rendere sicura la vostra rete domestica xLINE.

Effettuare un doppio click sul collegamento 'Powerpacket Utility'. La schermata che appare è divisa in due parti. La parte superiore mostra l'adattatore xLINE che è collegato direttamente al vostro computer. La parte inferiore mostra gli altri adattatori presenti nella rete domestica xLINE. Qui potrete trovare gli adattatori appartenenti alla rete nominata in modo predefinito 'HomePlug'.

Per proteggere gli adattatori che non sono direttamente connessi al computer, sarà necessaria la cosiddetta chiave 'DEK' (ovvero Device ID key) che potete trovare su un'etichetta adesiva collocata sull'adattatore xLINE. Non sarà necessario, invece, proteggere l'adattatore che è direttamente connesso al vostro computer. Seguire le istruzioni di seguito riportate per proteggere gli adattatori xLINE:

1. Nel campo inferiore del 'Powerpacket utility' potete scegliere un adattatore xLINE dalla lista tra quelli che non hanno alcun valore evidenziato nella colonna 'Password'.
2. Premere 'Enter Password'.
3. Inserire la chiave 'DEK Key / Device ID', e premere 'OK'. La chiave 'DEK Key / Device ID' si trova sull'etichetta adesiva dell'adattatore xLine. Un esempio potrebbe essere 'XK8Y-GH36-BR1K-LSZA'.
4. Apparirà un messaggio che comunica che la password è corretta. Premere 'OK' per confermare.
5. Se questo messaggio non dovesse apparire, controllare la chiave 'DEK Key' o 'Device ID' che avete inserito.
6. Ripetere i punti da 1 a 5 per tutti gli adattatori xLINE, finché tutti siano elencati nella lista in basso con password evidenziata nella colonna 'Password'.
7. Premere l'etichetta 'Privacy' nel software.
8. Inserire un nome creato da voi, segreto per la rete nel campo 'Private Network Name'.
9. Premere 'Set All Devices', sulla destra rispetto al centro dello schermo.
10. Apparirà il messaggio 'Devices were all added to your network'.
11. Premere 'OK'.
12. Congratulazioni! Ora la vostra rete domestica xLINE è stata protetta. Non sarà necessario ripetere queste operazioni sugli altri computer della rete.

Suggerimento: Il campo 'Private Network Name' consente di accedere alla vostra rete domestica xLINE. Non rivelate il codice che avete creato a persone sconosciute! Se volete, potete trascrivere qui sotto il 'Private Network Name', e conservare il manuale in un luogo sicuro.

Private Network Name: _____

3.4 Aggiungere un nuovo adattatore xLINE alla vostra rete protetta

Se disponete di una rete domestica protetta xLINE, e volete aggiungere un nuovo adattatore xLine, dovrete impostare la cosiddetta 'Private Network Name' su questo nuovo adattatore. Questo può essere realizzato in due modi.

Opzione 1: La nuova apparecchiatura xLINE è connessa ad un computer.

1. Installare il software sul nuovo computer come descritto nel paragrafo 3.2.
2. Effettuare un doppio click sul collegamento 'Powerpacket Utility' del vostro desktop per aprire il software.
3. Premere l'etichetta 'Privacy'.
4. Inserire il nome segreto della rete nel campo 'Private Network Name'.
5. Premere 'Set Local Device', che si trova a destra rispetto al centro dello schermo.
6. Il 'Powerpacket Utility' indicherà che il nome della rete è stato impostato.
7. Premere 'OK'.
8. Ora potrete andare a controllare se è presente una connessione con gli altri adattatori nella rete domestica xLINE.
9. Premere l'etichetta 'Main'.
10. Tutti gli adattatori xLINE della vostra rete domestica saranno visibili e connessi.

Opzione 2: Il nuovo xLINE è collegato ad un altro dispositivo, come ad esempio una consolle per giochi.

1. Usate il computer sul quale è già stato installato il software, oppure installate il software come spiegato nel capitolo 3.2
2. Premere 'Add' nella parte a destra in basso dello schermo.
3. Non dovete scrivere nulla nel campo 'Device Name'.
4. Inserite la chiave 'DEK key / Device ID' dell'apparato xLINE nel campo 'Password'.
5. Premere 'OK'. Il nuovo apparato xLINE è stato aggiunto.
6. Premere l'etichetta 'Privacy'.
7. Vistare il 'Private Network Name'. Inserite nuovamente il nome se necessario.
8. Premere 'Set All Devices', situato a destra del centro dello schermo.
9. Apparirà il messaggio 'Devices were all added to your network'.
10. Premere l'etichetta 'Main'.
11. Tutti gli adattatori xLINE presenti nella rete domestica saranno visibili e connessi.

Avete appena aggiunto il vostro nuovo adattatore xLINE alla vostra rete xLINE, e l'avete messo in sicurezza.

4.0 Domande frequenti

D. La mia rete è lenta ed instabile, quale potrebbe esserne la causa?

R 1. Controllate che tutti gli adattatori siano connessi direttamente alle prese. Non usate prolunghe o prese multiple perché queste potrebbero influenzare significativamente, in modo negativo, la qualità della rete. In particolare sconsigliamo l'uso di prese multiple o prese che sia dotate di protezione contro le sovratensioni.

R 2. Il segnale dipende anche dall'età della rete elettrica nella vostra casa. Può influire anche il tipo di contatore che si sta usando; ad esempio se dotato di filtri interni.

R 3. Se la vostra casa o il vostro ufficio ricevono la corrente da un sistema tri-fase , la ricezione tra le tre fasi differenti potrebbe risultare debole. Nella maggior parte dei casi, comunque, la comunicazione tra le 3 non dovrebbe essere eccessivamente influenzata dalla debolezza del segnale. Una rete di alimentazione tri-fase si può facilmente riconoscere dalla presenza di tre interruttori principali nell'armadio dei contatori.

D. I miei adattatori xLINE non comunicano tra di loro?

R. Controllate le impostazioni della vostra rete (consultate il manuale avanzato presente nel CD ROM). Ci sono probabilità che questi non siano correttamente configurati. La vostra rete necessita, per funzionare correttamente, di un protocollo TCP/IP che sia configurato come 'Ottenere automaticamente un indirizzo IP.

D. La mia rete domestica xLINE è visibile dai miei vicini?

R. Normalmente il segnale dell'adattatore xLINE viene filtrato dai filtri e contatori nel quadro corrente e perciò dovrebbe essere troppo debole per essere ricevuto dai vostri vicini. Vi raccomandiamo, comunque, di mettere in sicurezza la vostra rete xLINE criptandola.

D. Posso amplificare il segnale xLINE? Devo raggiungere distanze elevate o devo accoppiare fasi diverse.

R. Si, il segnale xLINE può essere amplificato. Questo si può fare usando due differenti nomi di rete (ad esempio A e B) in due diverse posizioni dopo di che connettete un adattatore xLINE dalla posizione A ad un adattatore xLINE dalla posizione B, usando un cavo di rete.

5.0 Manutenzione e supporto

Questo manuale è stato scritto da esperti tecnici della Eminent. Se si riscontrano dei problemi nell'installazione o nell'utilizzo del prodotto, vi preghiamo di rinvolgervi al Supporto Eminent, compilando il modulo presente sul sito www.eminent-online.com/support.

Eminent Advanced Manual

Table of contents

Table of contents 8
Why an Eminent advanced manual? 9
Your tips and suggestions in the Eminent Advanced Manual? 9
Service and support 9
Networking settings for Windows 98 and Windows ME 9
Networking settings for Windows 2000 and Windows XP 10
Networking settings for Windows Vista 11
Configuring Internet Explorer 5 and 5.5 11
Configuring Internet Explorer 6 12
Configuring Internet Explorer 7 12
DHCP, Automatic allocation of IP addresses 13
Translating IP addresses and domain names 13
Using a single IP address for your entire network 13
Security for your computer and your network 14
Making a computer available for Internet users in your network 14
Simplifying network management 15
Blocking websites with explicit content 15
Checking data traffic at package level 15
Blocking a complete domain 16
Carrying out actions based on date or time 16
A safe remote connection 16
Remote network management 16
Allocating or blocking network access 16
Making your wireless network secure 17
Expanding the range of your wireless network 17
Index 19

Why an Eminent advanced manual?

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

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

Your tips and suggestions in the Eminent Advanced Manual?

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

Service and support

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

Networking settings for Windows 98 and Windows ME

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

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

Networking settings for Windows 2000 and Windows XP

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

Networking settings for Windows Vista

1. Click on the Windows Vista logo (start button).
2. Choose ‘Configuration screen’.
3. Choose ‘Show network status and –tasks’.
4. Choose ‘Control network connections’.
5. Right-click on ‘LAN-connection’.
6. Choose ‘Connect.
7. If windows asks for your permission: choose ‘Continue’
8. Windows Vista now connects your LAN-connection.
9. Right-click on ‘LAN-connection’.
10. Choose ‘Properties’.
11. If windows asks for your permission: choose ‘Continue’.
12. Select ‘Internet Protocol version 4 (TCP/IPv4)’.
13. Click on ‘Properties’.
14. Choose ‘Obtain IP Address automatically.’
15. Choose ‘Obtain DNS Server address automatically’.
16. Click ‘OK’.
17. Click ‘Close’.
18. Windows Vista will now set-up your connection.

Configuring Internet Explorer 5 and 5.5

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

22. Restart your PC.

Configuring Internet Explorer 6

1. Start Internet Explorer.
2. Click ‘Stop’.
3. When asked to establish a connection, press ‘Cancel’.
4. Click ‘Extra’.
5. Click ‘Internet options’.
6. Click the ‘Connections’ tab.
7. Click the ‘LAN settings’ tab.
8. Uncheck ‘Find Explorer settings automatically’.
9. Uncheck ‘Use configuration script’.
10. Uncheck ‘Use proxy-server’.
11. Click ‘Ok’.
12. Remove dial-up connections by pressing ‘Delete’.
13. Click ‘Settings’ to start the ‘New connection’ Wizard.
14. Click ‘Next’.
15. Select ‘Connect to the Internet’.
16. Click ‘Next’.
17. Select ‘I want to connect to the Internet manually’.
18. Click ‘Next’.
19. Select ‘Permanent broadband connection’.
20. Click ‘Next’.
21. Click ‘Complete’.
22. Close all Windows that are currently open.
23. Restart your PC.

Configuring Internet Explorer 7

1. Start internet Explorer.
2. Click ‘Stop’.
3. When asked to establish a connection, press ‘Cancel’.
4. Click ‘Extra’.
5. Click ‘Internet options’.
6. Click the ‘Connections’ tab.
7. Click the ‘LAN settings’ tab.
8. Uncheck ‘Find Explorer settings automatically’.
9. Uncheck ‘Use configuration script’.
10. Uncheck ‘Use proxy-server’
11. Click ‘Ok’.
12. Remove dial-up connections by clicking ‘Delete’.
13. Click on ‘Settings’ (at the top).
14. Choose your type of connection.

15. Windows Vista will now set-up your connection.

DHCP, Automatic allocation of IP addresses

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

Translating IP addresses and domain names

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

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

Using a single IP address for your entire network

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

NAT enables you to share a single public IP address with several computers in your network. NAT ensures the computers in your network can use the Internet without any problems but users on the Internet will not have access to the computers in your

network. You will understand that NAT also offers a certain level of security partly due to the fact that private IP addresses are not visible on the Internet.
Fortunately, most routers currently use NAT.

Security for your computer and your network

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

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

Making a computer available for Internet users in your network

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

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

Port Triggering or Special Apps is based on the same principle as Virtual Server. Port Triggering also enables you to make a computer within your network set up for example as an FTP- or webserver, accessible from the Internet. The ports you

allocate always remain open when you use Virtual Server. With Port Triggering however, the respective ports will only be opened if requested by the respective application.

Simplifying network management

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

Blocking websites with explicit content

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

Checking data traffic at package level

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

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

Blocking a complete domain

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

Carrying out actions based on date or time

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

A safe remote connection

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

Remote network management

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

Allocating or blocking network access

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

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

Making your wireless network secure

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

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

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

Expanding the range of your wireless network

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

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

Index

Access blocks 16
Access Point ..... *Zie* Range Extender
Administrator 16
Application.....15
ASCII.....17
Block 15
Bridging..... *Zie* WDS
Business network 16
Data traffic.....16
DDNS
  Dynamic DNS..... *Zie* DNS
DHCP
  Dynamic Host Configuration
    Protocol 13
DMZ
  DeMilitarized Zone 14
DNS
  Domain Name System.....13
Domain.....16
Domain Filter.....16
Domain name.....13
Dynamic 13
Dynamic DNS.....13
Explicit content 15
Firewall.....9
Firewall software solution 14
Gatekeeper 15
Hardware 14
Hexadecimal 16
Key.....17
Key words
  Catchwords 15
MAC address 16
Name resolution 13
NAT
  Network Address Translation.....13
Online games 14
Operating system 15
Package filter
  Packet inspection 15
Packet inspection 15
Parental Control 16
Plug & Play.....15
Policies.....15. *Zie* Rules
Pool.....13
Port Triggering.....14
Ports.....14
Pre Shared Key (PSK).....17
Private IP addresses 13
Programming language 15
Public IP address 13
Range 17
Range Extender 18
Rules.....15
Schedule Rule.....15
SNMP
  Simple Network Management
    Protocol 16
Tunnel 16
UPnP
  Universal Plug and Play.....15
URL Blocking 15
Virtual Server 16
Viruses 14
VPN
  Virtual Private Networking 16
WDS
  Wireless Distribution System 17
WEP encryption.....17
Wi-Fi Protected Access .....*Zie* WPA
WPA.....17
WPA2.....17

Dichiarazione di Conformità

Per garantire la vostra incolumità ed in conformità con le direttive e con le leggi sui prodotti emanate dalla Commissione Europea potete ottenere una copia della Dichiarazione di Conformità riguardante il prodotto da voi acquistato inviando un messaggio e-mail al seguente indirizzo: info@eminent-online.com. In alternativa potete richiederla tramite lettera indirizzata a:

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

Vogliate specificare 'Dichiarazione di Conformità' ed il codice del prodotto del quale volete la Dichiarazione di Conformità.

EMINENT

WWW.EMINENT-ONLINE.COM

Trademarks: all brand names are trademarks and/or registered trademarks of their respective holders.
The information contained in this document has been created with the utmost care. No legal rights can be derived from these contents. Eminent cannot be held responsible, nor liable for the information contained in this document.

Eminent is a member of the Intronics Group

EM8012-EM8013 R3 | 12-2008