EMINENT

MANUALE

EM4218 - wSURF Modem Wireless ADSL2/2+

WWW.EMINENT-ONLINE.COM

EM4218 - wSURF Modem Wireless ADSL2/2+

Avvisi e punti importanti cui prestare attenzione

In virtù delle leggi, delle direttive e dei regolamenti emanati dal Parlamento Europeo, questo apparecchio potrebbe essere soggetto alle limitazioni relative al suo utilizzo adottate da alcuni stati membri. In alcuni stati membri dell'Unione Europea, si potrebbe proibire l'utilizzo di questo prodotto. Altre informazioni su questo soggetto si trovano nella Dichiarazione di Conformità, riportata nell'ultima pagina di questo documento.

Indice

On page 12 you will find the Eminent Advanced Manual for networking settings and information about home networking. (English only)

1.0 Condizioni di garanzia

La garanzia Eminent si applica a tutti i prodotti Eminent a meno che non sia diversamente stabilito prima o al momento dell'acquisto. Quando si acquista n prodotto Eminent di seconda mano, il periodo di garanzia è calcolato dalla data d'acquisto del primo acquirente/proprietario. La garanzia Eminent si applica a tutti i prodotti Eminent e ai componenti inestricabilmente collegati e/o montati sul prodotto principale. Adattatori, batterie, antenne e tutti gli altri prodotti non inseriti o direttamente collegati al prodotto principale e/o prodotti la cui usura si possa presumere, senza ragionevoli dubbi, di grado diverso rispetto al prodotto principale, non sono coperti da garanzia Eminent. I prodotti non sono coperti dalla garanzia Eminent, quando se ne fa un uso scorretto/improprio, se sono esposti a influenze esterne e /o quando sono aperti da soggetti diversi da personale autorizzato Eminent.

2.0 Introduzione

Congratulazioni per l'acquisto di questo prodotto Eminent di qualità superiore! Questo prodotto è stato sottoposto ad analisi approfondite da parte dei tecnici Eminent. Se si dovessero riscontrare problemi di qualsiasi sorta con questo prodotto, si è coperti da una garanzia Eminent quinquennale. Si prega di conservare questo manuale e lo scontrino di acquisto.

Registrare subito il prodotto sul sito www.eminent-online.com per ricevere aggiornamenti sul prodotto!

2.1 Funzioni e caratteristiche

EM4218 è un modem wireless ADSL2/2+ che offre una connessione ad Internet wireless e stabile. Il router integrato consente di condividere questa connessione ad Internet con altri computer, usando un cavo di rete o una connessione wireless.

2.2 Contenuto della confezione

La confezione contiene i seguenti elementi:

- Modem router Wireless ADSL2/2+ EM4218.
- Adattatore di corrente.
- Cavo telefonico modulare.
- Cavo di rete UTP.
- CD-ROM con procedura guidata d'installazione e manuali.
- Manuale.

2.3 Spiegazione dei LED

PWR	*Si accende quando il modem EM4218 è acceso.*
WL/ACT	*Si accenderà quando il punto d'accesso wireless è attivo.*
LAN1, 2, 3 e 4	*Sarà acceso costantemente quando un computer è collegato ad una delle porte e lampeggerà quando i dati sono inviati o ricevuti usando uno dei cavi di rete.*
ADSL	*Inizierà a lampeggiare 30 secondi dopo avere acceso il modem EM4218 e sarà accesso costantemente quando il segnale ADSL è stato rilevato (sono se collegato ad un cavo telefonico con un segnale ADSL attivo).*
PPP	*Se è stata configurata una connessione PPPoE o PPPoA, questo LED sarà acceso quando la connessione funzione correttamente.*

3.0 Uso della procedura guidata d'installazione

Il modo più facile di installare il modem EM4218 è di usare la procedura guidata, come spiegato in questo capitolo. Se non si vuole usare la procedura guidata (che si trova nel CD-ROM fornito in dotazione) continuare con il Capitolo 4.

1. Accendere il computer.
2. Inserire il CD-ROM nell'unità CD-ROM o DVD del computer.
3. Il software si eseguirà automaticamente.
4. Attenersi alle istruzioni su schermo fino al completamento dell'installazione. La connessione ad Internet adesso è disponibile.

4.0 Installazione manuale

Quando si installa manualmente il modem EM4218, è importante che il browser Internet e la rete siano configurati in modo corretto. Le impostazioni saranno corrette automaticamente, salvo siano state modificate in precedenza. Consultare il manuale, che si trova nel CD-ROM, se si hanno dei dubbi sulle impostazioni del browser Internet o della rete.

4.1 Collegamento del modem EM4218

1. Spegnere computer.
2. Collegare il modem EM4218 alla presa di corrente usando il cavo d'alimentazione fornito in dotazione.
3. Collegare il cavo telefonico alla porta 'ADLS' del modem EM4218.
4. Collegare l'altra estremità del cavo telefonico al ripartitore ADSL (non fornito in dotazione).
5. Collegare un cavo di rete UTP ad una delle quattro 'LAN' del modem EM4218.
6. Collegare l'altra estremità del cavo di rete UTP alla scheda di rete del computer.

Il modem EM4218 è collegato in modo appropriato alla corrente elettrica? Verificare controllando se il LED 'PWR' è acceso.

La connessione di rete è appropriata? Accendere il computer e verificare se il LED – corrispondente alla porta LAN a cui è collegato il cavo di rete UTP – è acceso. Anche sulla scheda di rete del computer dovrebbe essere acceso un LED.

4.2 Configurazione del modem EM4218 per una connessione ad Internet

Prima configurare il modem EM4218 per la connessione ad Internet, EM4218 deve essere collegato. Il modem EM4218 può essere collegato usando le seguenti procedure:

1. Accendere il computer.
2. Aprire il browser Internet (ad esempio: Internet Explorer, Netscape o Firefox).
3. Nella barra dell'indirizzo, inserire 'http://192.168.1.1'.
4. Premere Enter o fare clic su 'Go to' (Vai a).
5. Inserire 'admin' nel campo 'User Name' (Nome utente) (Nota! Questo campo è sensibile alle maiuscole/minuscole).
6. Inserire 'admin' nel campo 'Password' (Nota! Questo campo è sensibile alla maiuscole/minuscole).
7. Fare clic su 'Log in' (Accedi).
8. È visualizzata la pagina d'apertura.

Suggerimento! Si raccomanda di modificare la password per impedire accessi nona autorizzati al modem EM4218.

1. *Fare clic su 'Tools' (Strumenti).*
2. *Fare clic su 'Password'.*
3. *Scegliere 'admin' nel campo 'Username' (Nome utente).*
4. *Inserire la password corrente nel campo 'Old Password' (Vecchia password).*
5. *Inserire una nuova password nel campo 'New Password' (Nuova password).*
6. *Inserire di nuovo la password nel campo 'Confirmed Password' (Conferma password).*
7. *Fare clic su 'Submit' (Invia).*
8. *Fare clic su 'OK'.*

Scrivere la nuova password per poter modificare le impostazioni in futuro:

Nome utente: *admin*
Password: _____

4.3 Configurazione per provider PPP

1. Fare clic su 'Setup Wizard' (Impostazione guidata).

2. Selezionare il paese di residenza nel campo ‘Country’ (Paese) (ad esempio: Olanda).
3. Selezionare il provider Internet nel campo ‘ISP’.
4. Fare clic su “Next” (Avanti).
5. Inserire il nome utente ADSL nel campo ‘Username’ (Nome utente).
6. Inserire la password nel campo ‘Input Password’ (Inserire la password).
7. Inserire di nuovo la password nel campo ‘Confirmed Password’ (Conferma password).
8. Fare clic su ‘Save’ (Salva) per salvare le impostazioni e riavviare il modem EM4218.

4.4 Configurazione per provider DHCP

1. fare clic su ‘Setup Wizard’ (Impostazione guidata).
2. Selezionare il paese di residenza nel campo ‘Country’ (Paese) (ad esempio: Olanda).
3. Selezionare il provider Internet nel campo ‘ISP’.
4. Selezionare ‘DHCP (Get IP dynamically from ISP)’ (DHCP (Ottieni IP dinamico dall'ISP)) nel campo ‘Connection Type’ (Tipo di connessione).
5. Fare clic su “Next” (Avanti).
6. Fare clic su ‘Save’ (Salva) per salvare le impostazioni e riavviare il modem EM4218.

4.5 Configurazione per altri provider

Se non si riesce a trovare il proprio provider nell’elenco, rivolgersi al provider per ottenere le impostazioni corrette. Attenersi alla procedura che segue per inserire queste impostazioni nel modem EM4218:

1. Fare clic su ‘Advanced’ (Avanzate).
2. Fare clic su ‘WAN’.
3. Inserire le impostazioni fornite dal provider.
4. Fare clic su ‘Add’ (Aggiungi).
5. Fare clic su ‘Save’ (Salva) (nell’angolo in alto a destra).
6. Fare clic su "OK" per riavviare il modem EM4218.

5.0 Proteggere la rete wireless

Per evitare che ospiti indesiderati usino la rete, si raccomanda di proteggere la rete wireless. La rete può essere protetta usando vari metodi. Per applicare un metodo alla rete, è necessario che tutti i dispositivi wireless supportino questo metodo. Si raccomanda di impostare la protezione più alta: WPA2 (WiFi Protected Access).

1. Aprire il browser Internet (ad esempio: Internet Explorer, Netscape o Firefox).
2. Nella barra dell‘indirizzo, inserire ‘http://192.168.1.1’.
3. Premere Enter o fare clic su ‘Go to’ (Vai a).

4. Inserire ‘admin’ nel campo ‘User Name’ (Nome utente) (Nota! Questo campo è sensibile alla maiuscole/minuscole).
5. Inserire ‘admin’ nel campo ‘Password’ (Nota! Questo campo è sensibile alla maiuscole/minuscole).
6. Fare clic su ‘Advanced’ (Avanzate).
7. Fare clic su ‘Wireless’.
8. Fare clic su ‘Security’ (Protezione).
9. Andare alla sezione 5.1 per la protezione WPA2 (raccomandata), andare alla sezione 5.2 per la protezione WEP.

La protezione WPA2 è supportata da Windows XP e dalle versioni più recenti di Windows. Se la versione di Windows in uso è meno recente, continuare con la sezione 5.2.

5.1 Protezione WPA2 (raccomandata)

1. Selezionare ‘WPA2 (AES)’ nel campo ‘Encryption’ (Codifica).
2. Selezionare ‘Personal (Pre-Shared Key)’ (Personale (Chiave pre-condivisa)) nel campo ‘WPA Authentication Mode’ (Modalità d’autenticazione WPA).
3. Selezionare ‘Passphrase’ nel campo ‘Pre-Shared Key Format’ (Formato chiave pre-condivisa).
4. Inserire una password nel campo ‘Pre-Shared Key’ (Chiave pre-condivisa). Ad esempio ‘iltuonome01’. Non usare periferiche ed accertarsi che la password sia composta da almeno 8 caratteri!
5. Annotare la password scelta *.
6. Fare clic su ‘Submit’ (Invia).
7. Fare clic su ‘Save’ (Salva) (nell’angolo in alto a destra) per salvare le impostazioni.

5.2 Protezione WEP

1. Selezionare ‘WEP’ nel campo ‘Encryption’ (Codifica).
2. Fare clic su ‘Set WEP Key’ (Imposta chiave WEP).
3. Apparirà una nuova schermata.
4. Selezionare 64 o 128 bit nel campo ‘Key Length’ (Lunghezza chiave).
5. Selezionare ‘ASCII’ o ‘Hex’ nel campo ‘Key Format’ (Formato chiave).
6. Selezionare ‘Key 1’ (Chiave 1) nel campo ‘Default Tx Key’ (Chiave predefinita di trasmissione).
7. Inserire una password nel campo ‘Encryption Key 1’ (Chiave di codifica 1). Non usare periferiche ed assicurarsi che la password sia composta esattamente da 5, 10, 13 o 26 caratteri, in base alle impostazioni delle altre chiavi.
8. Annotare la password scelta *.
9. Fare clic su ‘Submit’ (Invia).
10. Fare clic su ‘Save’ (Salva) (nell’angolo in alto a destra) per salvare le impostazioni.

Quando la protezione (WPA2 o WEP) è abitata sul modem EM4218 e no sulla scheda di rete, la connessione cade. Appena le impostazioni di protezione cono configurate nella scheda di rete, la connessione è riparata.

** Annotare il metodo di protezione usato e la password:*
☐ WPA2 ☐ WEP

Password: _____

6.0 Controllo della connessione Internet

Se si vuole espandere la protezione della rete wireless, impostare la funzione MAC Address Control (Controllo indirizzo MAC) sul modem EM4218. Questo indirizzo MAC è un codice unico abbinato a ciascun dispositivo di rete. La funzione MAC Address Control (Controllo indirizzo MAC) abilita a consentire la connessione alla rete a prodotti di rete specifici. A tutti gli altri utenti sarà negato l'accesso. Se si aggiunge solo il proprio indirizzo MAC, nessun altro può collegarsi alla rete.

Spesso l'indirizzo MAC si trova su un'etichetta adesiva apposta sul dispositivo di rete. Si trova anche attenendosi alle fasi che seguono:

1. *Fare clic su 'Start'.*
2. *Fare clic su 'Run' (Esegui).*
3. *Scrivere 'CMD'.*
4. *Premere Enter (Invio).*
5. *Scrivere 'ipconfig /all'.*
6. *Premere Enter (Invio).*
7. *'Physical Address' (Indirizzo fisico) è l'indirizzo MAC.*

Suggerimento! Per garantire la protezione il Firewall è attivato per impostazione predefinita. Si raccomanda anche di installare un programma antivirus e di aggiornarlo regolarmente.

6.1 MAC Address Control (Controllo indirizzo MAC), blocco utenti

1. Aprire il browser Internet (ad esempio: Internet Explorer, Netscape o Firefox).
2. Nella barra dell'indirizzo, inserire 'http://192.168.1.1'.
3. Premere Enter o fare clic su 'Go to' (Vai a).
4. Inserire 'admin' nel campo 'User Name' (Nome utente) (Nota! Questo campo è sensibile alla maiuscole/minuscole).
5. Inserire 'admin' nel campo 'Password' (Nota! Questo campo è sensibile alla maiuscole/minuscole).
6. Fare clic su 'Advanced' (Avanzate).
7. Fare clic su 'Wireless'.

8. Fare clic sulla scheda ‘Access Control’ (Controllo accesso).
9. Selezionare ‘Allow Listed’ (Elenco autorizzati).
10. Inserire l’indirizzo MAC del dispositivo di rete al quale si vuole consentire l’accesso alla rete.
11. Fare clic su ‘Submit’ (Invia).
12. Ripetere le fasi 11 e 12 se si vuole consentire ad altri dispositivi di rete di accedere alla rete.
13. Fare clic su ‘Save’ (Salva) (nell’angolo in alto a destra) per salvare le impostazioni.
14. Adesso sono stati specificati i dispositivi di rete a cui è consentito di accedere alla rete.

7.0 WDS, espandere la portata della rete

La funzione WDS è utile per aumentare la portata della rete wireless e consentire a tutta la rete di collegarsi ad Internet. Usando il sistema WDS si può estendere la portata della rete installando vari router che, tramite il sistema WDS, funzionano come ripetitori estendendo così la portata wireless. Questa configurazione richiede una sola connessione ad Internet. Tutti i router collegati al sistema WDS hanno accesso ad Internet, quindi non è necessario collegare le porte LAN o WAN dei router usando cavi. Il sistema WDS consente di condividere senza fili una connessione ad Internet con altri router o punti d’accesso wireless che supporranno la funzione WDS.

7.1 Attivazione della funzione WDS sul modem EM4218

Ci sono delle istruzioni per usare il sistema WDS. In questo esempio saranno usati due router wireless, ed il modem EM4218 è collegato ad Internet. L’altro router wireless ripete il segnale wireless.

1. Accendere il computer.
2. Aprire il browser Internet (ad esempio: Internet Explorer, Netscape o Firefox).
3. Nella barra dell‘indirizzo, inserire ‘http://192.168.1.1’.
4. Premere Enter o fare clic su ‘Go to’ (Vai a).
5. Inserire ‘admin’ nel campo ‘User Name’ (Nome utente) (Nota! Questo campo è sensibile alla maiuscole/minuscole).
6. Inserire ‘admin’ nel campo ‘Password’ (Nota! Questo campo è sensibile alla maiuscole/minuscole).
7. Fare clic su ‘Log in’ (Accedi).
8. Il router visualizzerà una schermata di benvenuto.
9. Fare clic su ‘Advanced’ (Avanzate).
10. Fare clic su ‘Wireless’.
11. Fare clic su ‘Setting’ (Impostazioni).
12. Impostare ‘Mode’ (Modalità) su ‘WDS’.
13. Fare clic su ‘Submit’ (Invia).
14. Fare clic su "OK".
15. Fare clic su ‘WDS’ in alto sul menu.

16. Fare clic su ‘Enable WDS’ (Abilita WDS).
17. Inserire l’indirizzo MAC WLAN (BSSID) dell’altro router nel campo ‘Add WDS AP’ (Aggiungi punto d'accesso WDS). Questo indirizzo MAC si trova sulla parte inferiore del router.
18. Se non si riesce a trovare l’indirizzo, fare clic sul tasto ‘Show AP’ (Mostra punto d’accesso). Annotare il codice BSSID del router che si vuole collegare usando il sistema WDS e chiudere la schermata ‘Show AP’ (Mostra punto d’accesso).
19. Fare clic su ‘Submit’ (Invia).
20. Se si vogliono aggiungere altri router alla rete WDS, ripetere le fasi 17 e 18 per ciascun router.
21. Fare clic su ‘Save’ (Salva).
22. Fare clic su "OK".

Per stabilire una connessione WDS è necessario inserire l’indirizzo MAC del modem EM4218 nel dispositivo ricevente. Fare riferimento al Manuale d’uso del dispositivo ricevente per altre informazioni.

Se la rete wireless è protetta, sarà anche necessario configurare la protezione dell’altro dispositivo wireless. In modalità WDS può essere usata solo la protezione WEP. Fare riferimento al capitolo 5.2 per informazioni sulla protezione WEP.

7.2 Cose da ricordare quando si usa il sistema WDS

- Tutti i router della rete WDS devono trovarsi nello stesso intervallo IP (ad esempio: 192.168.1.1 per il router A e 192.168.1.200 per il router B). A volte è necessario impostare un indirizzo IP fisso sul dispositivo ricevente.
- La protezione WEP deve essere identica su entrambi i dispositivi.
- I canali della comunicazione wireless devono essere identici.
- I nomi (SSID) delle connessioni wireless non devono essere identici.
- Si sconsiglia di usare la funzione MAC Address Control (Controllo indirizzo MAC) insieme alla funzione WDS.
- I server DHCP de secondo (o terzo, o quarto) router devono essere disabilitati.

Attenzione! Quando si protegge la connessione non può essere usata la protezione WPA2.

8.0 FAQ (Domande frequenti)

Q. Ricevo il messaggio ‘The IP address of the network adapter is incorrect’ (L’indirizzo IP della scheda di rete non è corretto). Che cosa possono fare?

A. Questo messaggio appare quando il computer non riceve un indirizzo IP corretto dal router. Assicurarsi che tutti i cavi siano collegati in modo corretto. Se necessario, ripristinare il modem EM4218 e riprovare. Si raccomanda di configurare il router usando una connessione cablata (non wireless). Quando la connessione cablata funziona in modo appropriato, si può impostare la connessione wireless come spiegato in questo manuale.

Q. Come si fa per ripristinare il modem EM4218?

A. Ripristinare il modem attenendo alle fasi che seguono:
   1. Accendere il modem ed attendere che si avvii.
   2. Tenere premuto per circa venti secondi il tasto di ripristino a fianco del tasto d'accensione/spegnimento, usando un fermaglio.
   3. È stato eseguito il ripristino del modem.

Q. Il segnale wireless è debole o instabile. Quale può essere la causa?

A. Spostare il modem in un'altra posizione per vedere se la potenza del segnale aumenta. Se possibile collocare il modem in uno spazio aperto. Il quadro elettrico, ad esempio, non è un buon luogo dove installare un modem wireless.

A. Provare a cambiare il canale del modem per vedere se la potenza del segnale aumenta. Seguire le istruzioni riportate sotto:
   1. Aprire il browser Internet (ad esempio: Internet Explorer, Netscape o Firefox).
   2. Nella barra dell'indirizzo, inserire 'http://192.168.1.1'.
   3. Premere Enter o fare clic su 'Go to' (Vai a).
   4. Inserire 'admin' nel campo 'User Name' (Nome utente) (Nota! Questo campo è sensibile alla maiuscole/minuscole).
   5. Inserire 'admin' nel campo 'Password' (Nota! Questo campo è sensibile alla maiuscole/minuscole).
   6. Fare clic su 'Advanced' (Avanzate).
   7. Fare clic su 'Wireless'.
   8. Impostare 'Channel' (Canale) su un altro numero, ad esempio 3.
   9. Fare clic su 'Submit' (Invia).
   10. Fare clic su 'Save' (Salva).
   11. Fare clic su "OK".

9.0 Manutenzione e assistenza

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

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

Dichiarazione di Conformità

Per assicurarsi della sicurezza e della conformità del prodotto con le direttive e leggi create dalla commissione della comunità europea può ottenere una copia della dichiarazione di conformità del Suo prodotto inviando una mail a: info@eminent-online.com. Può contattarci anche via posta a:

Eminent Computer Supplies
Postbus 276
6160 AG GELEEN
The Netherlands

Si prega di indicare chiaramente 'Dichiarazione di Conformità' e il codice dell'articolo del quale vuole ottenere una copia della dichiarazione di conformità.

EMINENT

WWW.EMINENT-ONLINE.COM

CE

Eminent is a member of the Intronics Group