EMINENT

MANUAL

EM4450 - Trådlös Router

WWW.EMINENT-ONLINE.COM

EM4450 - Trådlös Router

Varningar och uppmärksammanden

På grund av gällande EU-direktiv och regleringar så kan denna produkts egenskaper vara begränsade i vissa medlemsländer. Den kan även vara förbjuden att använda i vissa medlemsländer. Mer information om detta kan återfinnas under rubriken Försäkran av Överensstämmelse på dokumentets sista sida.

Innehållsförteckning

1.0 Garantibestämmelser 2
2.0 Introduktion 3
2.1 Förpackade delar 3
3.0 Funktioner och egenskaper 3
4.0 Att ansluta din EM4450 4
5.0 Använda sig av den medföljande installationsguiden för att installera EM4450 4
6.0 Manuell installation av din trådlösa router 4
6.1 Logga in på EM4450 5
6.2 Konfiguration för en uppkoppling via DHCP 5
6.3 Konfiguration av en internetuppkoppling som använder sig av Statiskt IP-nummer 6
6.4 Konfiguration av en internetuppkoppling som använder sig av PPPoE 6
6.5 Konfiguration av en internetuppkoppling som använder sig av PPTP 6
7.0 Skydda ditt trådlösa nätverk 7
8.0 Skydda ditt nätverk manuellt 7
8.1 Att ställa in WPA-skydd manuellt 7
8.2 Att ställa in WEP-skydd manuellt 8
9.0 Konfigurera det trådlösa nätverket på din dator 9
10.0 Övervaka din internetuppkoppling 10
10.1 Aktivera brandväggen 10
10.2 Neka internetåtkomst genom att använda sig av IP-adresser 10
10.3 Neka internetåtkomst genom att använda sig av ‘Domain Filtering’ 11
10.4 Neka internetåtkomst genom att använda sig av ‘MAC Address Filtering’ 11
11.0 Vanliga frågor 12
12.0 Service och support 14

On page 15 you will find the Eminent Advanced Manual for networking settings and information about home networking. (English only)

1.0 Garantibestämmelser

Den femåriga garantin på Eminents produkter återfinns på alla Eminents produkter om inte annat har framgått före eller under köpet. Vid köp av begagnade Eminentprodukter så räknas den femåriga garantin från det datum den första ägaren gjorde köpet. Garantin täcker alla Eminentprodukter, dess komponenter och dess fasta såväl som påmonterade delar. Batteriemulatorer, batterier, antenner och övriga komponenter som inte är direkt kopplade till Eminents huvudprodukt som utan godtagbar härledning till Eminents huvudprodukt uppvisar skador täcks inte av Eminents garanti. Produkter som har blivit utsatta för en inkorrekt eller felaktig användning och/eller har blivit öppnade av annan part än Eminent täcks inte av Eminents garanti.

2.0 Introduktion

Låt oss gratulera dig till ditt köp av denna hög-kvalitativa Eminentprodukt! Denna produkt har genomgått grundlig testning av Eminents tekniska experter. Skulle du mot förmodan stöta på problem med denna produkt så är du täckt av vår femåriga Eminentgaranti. Vänligen spara denna manual och ditt kvitto på en säker plats.

Registrera ditt inköp idag på www.eminent-online.com för att få produktuppdateringar!

2.1 Förpackade delar

Följande delar måste återfinnas I förpackningen:

- EM4450, trådlös router
- Batteriemulator
- UTP-nätverkskabel
- CD-skiva med installationsguide och manual.
- Denna användarhandbok.

3.0 Funktioner och egenskaper

Eminent EM4450 låter dig skapa ditt egna skyddade trådlösa nätverk inom bara ett par minuter. EM4450 är en trådlös basstation som är skapad för att förse ditt hem med en trådlös uppkopppling som du kan komma åt i varje skrymsle av ditt hem. EM4450 presterar på en hög nivå och det kommer leda till ett flexibelt och stabilt nätverk. Njut av ditt trådlösa nätverk och låt EM4450 stå för allt arbete!

- Inbyggd 54Mbps accesspunkt för upprättande av ett trådlöst nätverk.
- Inbyggd router för att utan vidare ansträngning dela med dig av din internetuppkoppling.
- Inbyggd 4-portars switch för upprättande av ett trådburet nätverk.

- Inbyggd brandvägg för att skydda din information.

4.0 Att ansluta din EM4450

1. Stäng av din dator.
2. Anslut EM4450 till elförsörjning genom att använda dig av den medföljande batteriemulatorn.
3. Anslut den medföljande nätverkssladden till WAN-porten på din EM4450.
4. Anslut den andra änden av nätverkssladden till LAN-porten på ditt modem.
5. Anslut en nätverkssladd i en LAN-port på din EM4450
6. Med den andra änden på sladden ansluter du din dators nätverkskort till EM4450.

Tips: Innan du fortsätter installationen av EM4450 så måste du försäkra dig om att routern får en korrekt elförsörjning. Du kan verifiera att så är fallet genom att titta om lampan märkt med stand-by-ikonen lyser.
Försäkra dig även om att du har anslutit din dator och din router med nätverssladdar på ett korrekt sätt. För att kontrollera detta så tittar du om lampan som tillhör den LAN-port du har anslutit datorn till på routern lyser.

5.0 Använda sig av den medföljande installationsguiden för att installera EM4450

EM4450 måste konfigureras som en trådlös router om den är ansluten till ett ADSL- eller Kabel-modem. Lättaste sättet att konfigurera detta är med den medföljande installationsguiden som ni finner på skivan. Om du inte vill använda dig av installationsguiden kan du även konfigurera routern manuellt. Se kapitel 5.2

1. Starta din dator.
2. Stoppa in den medföljande CD-skivan i din dators DVD-läsare eller CD-läsare.
3. Installationsguiden kommer att startas automatiskt.
4. Följ instruktionerna som visas på din skärm till det att installationen är slutförd. Du har nu en fungerande internetanslutning.

Tips: Om inte installationsguiden startas automatiskt när du stoppar in CD-skivan så kan du starta denna manuellt genom att gå till 'Start', 'Kör...' och skriva in 'x:\wizard\wizard.exe' ('x' är den bokstav som din CD-läsare har som enhetsbeteckning) och trycka enter.

6.0 Manuell installation av din trådlösa router

Vi kommer nu att gå genom de olika konfigurationer man kan använda sig av. Vilken metod du använder dig av beror på vilken internetleverantör du har, du behöver bara följa en instruktion för en säker och snabb anslutning!

6.1 Logga in på EM4450

Kontrollera så att din webbläsare och ditt nätverk är konfigurerade på rätt sätt när du ska konfigurera manuellt. Du kan utgå från att dessa inställningar är korrekta om det inte är så att du har ändrat i inställningarna själv någon gång.

Tips! Är du inte säker på inställningarna så kan du titta på den avancerade manualen på CD-skivan.

Du kan manuellt ansluta dig till EM4450 genom att använda dig av följande procedur:

1. Starta din dator.
2. Starta din webbläsare (t.ex. Internet Explorer, Netscape, Safari eller Firefox).
3. Skriv in 'http://192.168.1.1' i adressfältet.
4. Tryck Enter eller 'Gå till'.
5. Skriv in 'admin' i fältet Användarnamn.
6. Skriv in 'admin' i fältet Lösenord.
7. Klicka på 'OK'.
8. Du ska nu se välkomstskärmen på din wLINK.

Observera! Först måste du avgöra vilken metod du ska använda dig av vid din internetanslutning ('DHCP', 'PPPoE', 'StaticIP' eller 'PPTP') som din internetleverantör använder sig av. Du ska ha fått denna information av din internetleverantör

6.2 Konfiguration för en uppkoppling via DHCP

1. Klicka på 'Network' i den vänstra menyn.
2. Klicka på 'WAN' i den vänstra menyn.
3. Välj 'Dynamic IP'.
4. Om din internetleverantör har uppgett ett visst värdnamn skriver du in det I fältet 'Hostname'.
5. Klicka på 'MAC Clone' I den vänstra menyn. (Detta behövs endast om din internetleverantör använder sig av registrering via MAC-adresser.)
6. Klicka på knappen 'Clone MAC'.
7. Klicka på 'Save'.
8. Stäng din webbläsare.
9. Inom fem minuter ska du ha en fungerande internetuppkoppling.

Observera! Om du har en internetleverantör som använder sig av uppkoppling via kabel och inte får en fungerande uppkoppling inom fem minuter ska du gå vidare till kapitel 11.

6.3 Konfiguration av en internetuppkoppling som använder sig av Statiskt IP-nummer

1. Klicka på ‘Network’ i den vänstra menyn.
2. Klicka på ‘WAN’ i den vänstra menyn.
3. Välj ‘Static IP’.
4. Ange den IP-adress som du har fått av din internetleverantör i fältet ’IP address’.
5. Ange den subnetmask som din internetleverantör har angett i fältet ’Subnet Mask’.
6. Ange den gateway som din internetleverantör har angett i fältet ’Gateway’.
7. Ange adressen till den primära DNSen som din internetleverantör angett i fältet ’Primary DNS’.
8. Ange adressen till den sekundära DNSen som din internetleverantör angett i fältet ’Secundary DNS’. Om du inte har fått något adress till en sekundär DNS så lämnar du fältet tomt.
9. Klicka på ‘Save’.
10. Stäng din webbläsare.
11. Inom fem minuter ska du ha en fungerande internetuppkoppling.

6.4 Konfiguration av en internetuppkoppling som använder sig av PPPoE

1. Klicka på ‘Network’ i den vänstra menyn.
2. Klicka på ‘WAN’ i den vänstra menyn.
3. Välj ‘PPPoE’.
4. Ange det användarnamn du har fått av din internetleverantör i fältet ‘User Name’.
5. Ange det lösenord du har fått av din internetleverantör i fältet ‘Password’.
6. Klicka på ‘Save’.
7. Stäng din webbläsare.
8. Inom fem minuter ska du ha en fungerande internetuppkoppling.

6.5 Konfiguration av en internetuppkoppling som använder sig av PPTP

1. Klicka på ‘Network’ i den vänstra menyn.
2. Klicka på ‘WAN’ i den vänstra menyn.
3. Välj ‘PPtP’.
4. Ange det användarnamn du har fått av din internetleverantör i fältet ‘User Name’.
5. Ange det lösenord du har fått av din internetleverantör i fältet ‘Password’.
6. Ange den gateway-adress till ditt ADSL-modem i textfältet ‘Server IP Address/Name’.
7. Ange IP-adressen till ditt modem i fältet ’IP Address’.
8. Ange den subnetmask ditt ADSL-modem använder sig av i textfältet ’Subnet Mask’ field.

9. Ange gateway-adressen för ditt ADSL-modem i textfältet 'Gateway'.
10. Klicka på 'Save'.
11. Stäng din webbläsare.
12. Inom fem minuter ska du ha en fungerande internetuppkoppling.

7.0 Skydda ditt trådlösa nätverk

För att undvika att oinbjudna gäster använder sig av ditt trådlösa nätverk så rekommenderar vi starkt att du skyddar ditt trådlösa nätverk. Det finns ett antal olika sätt att skydda ditt trådlösa nätverk på. När du har valt en metod är det mycket viktigt att samtliga produkter i ditt nätverk har stöd för denna teknik. Det säkraste sättet för tillfället är WPA (WiFi Protected Access).

Det lättaste sättet att skydda ditt nätverk är att använda dig av installationsguiden på CD-skivan, instruktioner för hur du går tillväga med denna metod återfinns nedan. Om du inte vill använda dig av den medföljande CD-skivan så kan du manuellt konfigurera ett skydd för ditt nätverk genom att använda dig av routerns hemsida, hur du går tillväga finner du i kapitel 6.

1. Starta din dator.
2. Stoppa in den medföljande CD-skivan i din dators DVD- eller CD-läsare.
3. Installationsguiden kommer att startas automatiskt.
4. Välj ditt språk.
5. Välj 'Konfigurera skydd för trådlöst nätverk' och väl 'Nästa'.
6. Följ instruktionerna som visas på din skärm till det att installationen är färdig. Du har nu en fungerande internetanslutning.

Notera! WPA-skydd stöds av Windows 2000 och XP. Denna säkerhetsmetod går inte att använda med Windows 98 eller ME, om det inte är så att mjukvaran till ditt trådlösa nätverkskort stödjer WPA. Använd WEP om möjligheten att använda WPA inte finns.

8.0 Skydda ditt nätverk manuellt

Om du inte använder dig av den medföljande CD-skivan för installation av skydd för ditt nätverk så kan du göra detta manuellt. Detta kapitel förklarar hur du går tillväga med denna installation. Eminent föreslår och rekommenderar att du använder dig av säkerhetstekniken WPA då den är säkrast och ger ditt nätverk bäst skydd.

8.1 Att ställa in WPA-skydd manuellt

1. Starta din dator.
2. Starta din webbläsare (t.ex. Internet Explorer, Netscape, Safari eller Firefox).
3. Skriv in 'http://192.168.1.1' i adressfältet.
4. Tryck Enter eller 'Gå till'.
5. Skriv in 'admin' i textfältet 'Username'.

6. Skriv in admin som lösenord i textfältet ’Password’.
7. Klicka på ‘Wireless’ I den vänstra menyn.
8. Klicka på ‘Wireless Settings’ I den vänstra menyn.
9. Klicka för ‘Enable Wireless Security’.
10. Välj önskad säkerhetsmetod intill ‘Security Type’, i detta fall WPA-PSK/WPA2-PSK.
11. Välj WPA-PSK intill fältet ‘Security Option’.
12. Välj TKIP intill fältet ‘Encryption’.
13. Gå till ‘PSK Pass phrase’. Här kan du ange en säkerhetskod(lösenord). Du kan använda dig av både siffror och bokstäver. Du vill antagligen skriva ned koden.
14. Klicka på ‘Save’.
15. Klicka på ‘OK’, sedan på ‘OK’ igen. Din router kommer nu att spara dessa inställningar.

8.2 Att ställa in WEP-skydd manuellt

1. Starta din dator.
2. Starta din webbläsare (t.ex. Internet Explorer, Netscape, Safari eller Firefox).
3. Skriv in ‘http://192.168.1.1’ i adressfältet.
4. Tryck Enter eller ‘Gå till’.
5. Skriv in ’admin’ i textfältet ’Username’.
6. Skriv in admin som lösenord i textfältet ’Password’.
7. Klicka på ‘Wireless’ I den vänstra menyn.
8. Klicka på ‘Wireless Settings’ I den vänstra menyn.
9. Klicka för ‘Enable Wireless Security’.
10. Välj önskad säkerhetsmetod intill ‘Security Type’, i detta fall WEP.
11. Välj önskad lösenordstyp: Du kan välja mellan 64bitars eller 128bitars. Om du väljer att använda dig av 64bitar så anger du ett lösenord (kod) på exakt tio (10) tecken. Om du vill använda dig av bokstäver så kan du endast använda dig av A-F. Om du vill använda dig av 128bitar så anger du ett lösenord (kod) på exakt 26 tecken.
12. Du kommer att ha användning för detta lösenord (kod) senare så skriv ned den.
13. Klicka på ‘Save’.
14. Klicka på ‘OK’, och ‘OK’ igen. Din router kommer nu att spara dina inställningar.

Notera! Eminent rekommenderar att du har din dator ansluten till EM4450 med en nätverkskabel vid säkerhetsinställningar.

Här kan du skriva ned säkerhetsmetod, nätverksnamn och lösenord:
☐ *WPA* ☐ *WEP*

Nätverksnamn: _____
Lösenord: _____

9.0 Konfigurera det trådlösa nätverket på din dator

Nu när din router är skyddad så behöver du konfigurera din dator så den blir aktiverad för att känna igen och ansluta sig till ditt skyddade nätverk.
Windows XP och Vista är de för tillfället mest använda operativsystemen. Vi kommer därför att förklara hur du ansluter dig till ditt trådlösa nätverk med dessa operativsystem.

Tips: Efter det att din router har konfigurerats för WEP- eller WPA-skydd kan du ta bort nötverkskabeln innan du fortsätter till steg 9.1.

9.1 Konfigurera ett trådlöst nätverk vid användning av Windows XP

För att kunna skapa en trådlös uppkoppling vid användning av Windows XP måste du följa dessa instruktioner:

1. Starta din dator.
2. Klicka på ‘Start’.
3. Gå till ‘Kontrollpanelen.
4. Välj ’Nätverksanslutningar.
5. Du ska nu kunna se anslutningen till det trådlösa nätverket. Högerklicka på denna anslutning.
6. Välj ‘Visa tillgängliga trådlösa nätverk’. En lista med de tillgängliga nätverken kommer nu att visas.
7. Välj ditt egna nätverk på listan genom att klicka på det.
8. När du klickar på ’Anslut’ så kommer din dator att varna dig för att nätverket är skyddat och kräver ett lösenord.
9. Mata in ditt lösenord och klicka på ‘Anslut’.
10. Om du angett rätt lösenord så kommer Windows att inom en kort stund att informera dig om att du är ansluten till nätverket. Du är nu online.

9.2 Konfigurera ett trådlöst nätverk vid användning av Windows Vista

För att kunna skapa en trådlös uppkoppling vid användning av Windows Vista måste du följa dessa instruktioner:

1. Klicka på ‘Start’.
2. Gå till ‘Kontrollpanelen’.
3. Välj ’Network and Internet Connections’.
4. Gå till ‘Nätverks- och Delningscenter’.
5. Välj ‘Hantera trådlösa nätverk’ i den vänstra delen av menyn.

6. Här måste du klicka på ‘Lägg till’.
7. I nästa fönster väljer du ‘Add a network that is in range of this computer’.
8. In this window you can select your own network.
9. Click ‘Connect’.
10. Din dator kommer att visa följande meddelande: ‘Ange nätverkssäkerhetsnyckeln eller lösenfrasen för ….. ’. Ange lösenordet.
11. Klicka på ‘Anslut’. If the key has been entered correctly, your computer will be connected and you will be online.

10.0 Övervaka din internetuppkoppling

EM4450 är utrustad med en avancerad brandvägg. Detta tillåter dig att ha en nästan komplett övervakning av din internetanslutning. Brandväggen tillåter dig att neka en dator åtkomst till internet. Du kan även blockera specifika hemsidor. Detta kan göras temporärt, permanent eller för en specifik tid, t.ex. kontorstid.

10.1 Aktivera brandväggen

För att kunna konfigurera brandväggen måste vi först aktivera den, följ dessa instruktioner:

1. Starta din dator.
2. Starta din webbläsare (t.ex. Internet Explorer, Netscape, Safari eller Firefox).
3. Skriv in ‘http://192.168.1.1’ i adressfältet.
4. Tryck Enter eller ‘Gå till’.
5. Skriv in ’admin’ i textfältet ’Username’.
6. Skriv in admin som lösenord i textfältet ’Password’.
7. Klicka på ’OK’.
8. Klicka på ‘Security’ under ‘Advanced Settings’ i den vänstra delen av din skärm.
9. Klicka för ‘Enable Firewall’.
10. Klicka på ‘Save’.
11. Brandväggen är nu aktiverad.

10.2 Neka internetåtkomst genom att använda sig av IP-adresser

Brandväggen låter dig neka en dator internetåtkomst genom att använda sig av dess IP-adress. För att använda dig av denna funktion måste du aktivera ’IP address filtering’. För att aktivera denna funktion så följer du instruktionerna i kapitel 10.1. I steg åtta så klickar du för ’Enable IP address filtering’ följt av steg nio och tio.

1. Klicka på ‘IP Address Filtering’ under ‘Advanced Settings’ i den vänstra delen av skärmen.
2. Klicka på ‘Add New’ i nästa fönster.
3. Ange nödvändig information i detta fönster.

4. Klicka på ’Effective time’.

I detta fält ange inom vilken tidsram som internetåtkomsten ska nekas. Om du vill att internetåtkomsten ska vara blockerad från 10.00 till 20.00 anger du 1000 i fältet ’Effective time’ samt 2000 i det andra fältet.

5. Ange IP-adressen till den dator som du vill neka åtkomst till internet i fältet ‘LAN IP Address’. T.ex. ‘192.168.1.5’.
6. Välj ‘Deny’ intill ‘Action’.
7. Klicka på ‘Save’.
8. Det är nu omöjligt för denna dator med detta specifika IP-nummer att ansluta sig till internet under den tid du angav.

Tips: Kapitel 11 tar upp hur man får tag i en dators IP-adress.

10.3 Neka internetåtkomst genom att använda sig av ‘Domain Filtering’.

EM4450 tillåter dig att neka åtkomst till vissa domäner eller hemsidor. Om du inte vill att din son eller dotter ska komma åt vissa hemsidor kan du konfigurera detta filter. För att använda dig av detta filter använder du sig helt enkelt av samma guide som i kapitel 10.1. Med den enda skillnaden att du denna gång klickar för ’Enable Domain Filtering’ i steg åtta som återföljs av steg åtta och nio.

1. Klicka ‘Domain Filtering’ i det vänstra fönstret.
2. Klicka på ‘Add New’
3. Klicka på ’Effective time’.

I detta fält ange inom vilken tidsram som internetåtkomsten ska nekas. Om du vill att internetåtkomsten ska vara blockerad från 10.00 till 20.00 anger du 1000 i fältet ’Effective time’ samt 2000 i det andra fältet.

4. Ange den domän eller webbplats som du vill neka åtkomst till under denna tidsram. T.ex. om du vill neka åtkomst till www.google.se så anger du denna adress i fältet ’Domain Name’.
5. Klicka för ‘Enabled’ i fältet ‘Status’.
6. Klicka på ‘Save’.
7. Det är nu omöjligt att nå denna domän eller webbplats under den angivna tidsramen.

10.4 Neka internetåtkomst genom att använda sig av ‘MAC Address Filtering’

Utöver de tidigare förklarade metoderna för att neka åtkomst till internet finns det ännu ett sätt att neka internetåtkomst. Detta sätt är även det mest effektiva. Internetåtkomst

är totalt blockerad och du behöver inte ange en tidsram. För att använda dig av detta filter använder du sig helt enkelt av samma guide som i kapitel 10.1. Med den enda skillnaden att du denna gång klickar för 'Enable Mac-address filtering' i steg åtta som återföljs av steg nio och tio.

1. Klicka på' MAC Filtering' i den vänstra rutan.
2. Klicka på 'Add New'
3. Ange den specifika MAC-adress i fältet 'MAC Address'.
4. Du kan ange en kort förklaring i fältet 'Description'.
5. Klicka för 'Enabled' i fältet 'Status'.
6. Klicka på 'Save'.
7. Det är nu omöjligt att för den dator med denna MAC-adress att ansluta sig till internet.

Tips: Kapitel 11 tar upp hur man får tag i en dators MAC-adress.

11.0 Vanliga frågor

F: Jag får meddelandet 'The IP address of the network adapter is incorrect'. Vad kan jag göra?
S: Detta meddelande fås när din dator inte fick en korrekt IP-adress av din router. Kontrollera så att alla kablar är korrekt anslutna, om nödvändigt så starta om din router och försök igen. Det är rekommenderat att du konfigurerar din router med en kabelburen anslutning (inte trådlös). När det trådburna nätverket fungerar korrekt kan du konfigurera den trådlösa anslutningen som det förklaras i denna manual.

F: Jag har konfigurerat routern. Allting verkar fungera, men jag kan inte få någon anslutning till internet. Min internetleverantör använder sig av DHCP.
S: Ibland så ger inte modemet routern någon internetanslutning. Följ dessa instruktioner för att få igång internetuppkopplingen:

1. Stäng av både router och modem.
2. Vänta i 10 minuter.
3. Starta modemet, vänta tills det har startat helt, sätt sedan igång din router och låt den starta upp helt.
4. Internetanslutningen bör nu fungera korrekt.

F: Jag testade lösningen ovan, men internetanslutningen fungerar fortfarande inte. Vad ska jag göra?
S: Det finns en annan metod:

1. Logga in på routerns hemsida på http://192.168.1.1
2. Username: admin, Password: admin
3. Du är nu inloggad på huvudsidan till EM4450.
4. Ta loss koaxialkabeln från ditt modem.
5. Klicka på 'Renew' under 'WAN' på routerns hemsida.

6. En IP-adress till ditt modem kommer att visas. Ofta är denna adress något liknande: 192.168.100.x
7. Sätt tillbaka koaxialkabeln till ditt modem och vänta tills det att Online/Internet lampan lyser.
8. Klicka på 'Renew' I routerns hemsida.
9. En IP-adress, som du har fått av din internetleverantör borde nu visas. Om den visas så är du online.

F: Jag vill veta min IP-adress, hur tar jag reda på den?
S: För att få tag i din IP-adress följer du dessa instruktioner:

Instruktioner för Windows XP/2000 och Windows Vista:
1. Klicka på 'Start'.
2. Klicka på 'Kör…'.
3. Skriv in 'cmd'.
4. Tryck på 'Enter' eller klicka på 'OK'Skriv in 'ipconfig'.
5. Tryck på 'Enter'.
6. Du kommer nu att se din IP-adress.

Instruktioner för Windows98/ME:
1. Klicka på 'Start'.
2. Gå till 'Kör…'.
3. Skriv in 'winipcfg'.
4. Tryck på 'Enter' eller klicka på 'OK'.
5. Du kommer nu att se din IP-adress.

F: jag vill veta MAC-adressen på min dators nätverkskort, hur får jag tag i denna information?
S: För att få tag i ditt nätverkskorts MAC-adress följer du dessa instruktioner:

Instruktioner för Windows XP/2000 och Windows Vista:
1. Klicka på 'Start'.
2. Gå till 'Kör…'.
3. Skriv in 'cmd'
4. Tryck på 'Enter' eller klicka på 'OK'
5. Skriv in 'ipconfig /all'.
6. Tryck på 'Enter'.
7. Du kommer nu att se den fysiska adressen. Detta är MAC-adressen till din dators nätverkskort.

Instruktioner för Windows98/ME:
1. Klicka på 'Start'.
2. Gå till 'Kör…'.
3. Skriv in 'winipcfg'
4. Tryck på 'Enter' eller klicka på 'OK'

5. Du kommer nu att se den fysiska adressen. Detta är MAC-adressen till din dators nätverkskort.

F: Hur nollställer jag EM4450?
S: Du kan nollställa EM4450 genom att först dra ur elsladden och sedan genom att använda dig av ett gem trycka in reset-knappen. Återanslut sedan elsladden medans du har reset-knappen nedtryckt. Lampan 'sys' kommer nu att lysa, vänta tills det att den börjar blinka och släpp då upp knappen. EM4450 har nu nollställts och har sina standardinställningar.

12.0 Service och support

Denna användarmanual har noggrant utformats av Eminents tekniska experter. Om du stöter på problem under installationen så kan gärna kontakta oss på support@eminent-online.com.

Eminent Advanced Manual

Table of contents

Table of contents 15
Why an Eminent advanced manual? 16
Your tips and suggestions in the Eminent Advanced Manual? 16
Service and support 16
Networking settings for Windows 98 and Windows ME) 16
Networking settings (Windows 2000 and Windows XP) 17
Configuring Internet Explorer 5 and 5.5 18
Configuring Internet Explorer 6 18
DHCP, Automatic allocation of ip-addresses 19
Translating ip-adresses and domain names 19
Using a single ip-address for your entire network 19
Security for your computer and your network 20
Making a computer available for Internet users in your network 20
Simplifying network management 21
Blocking websites with explicit content 21
Checking data traffic at package level 21
Blocking a complete domain 22
Carrying out actions based on date or time 22
A safe remote connection 22
Remote network management 22
Allocating or blocking network access 22
Making your wireless network secure 23
Expanding the range of your wireless network 23
Index 25

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

Access blocks 22
Access Point *See* Range Extender
Administrator 22
Application 21
ASCII 23
Block 21
Bridging *See* WDS
Business network 22
Data traffic 22
DDNS
  Dynamic DNS *See* DNS
DHCP
  Dynamic Host Configuration Protocol 19
DMZ
  DeMilitarized Zone 20
DNS
  Domain Name System 19
Domain 22
Domain Filter 22
Domain name 19
Dynamic 19
Dynamic DNS 19
Explicit content 21
Firewall 16
Firewall software solution 20
Gatekeeper 21
Hardware 20
Hexadecimal 22
Key 23
Key words
  Catchwords 21
MAC address 22
Name resolution 19
NAT
  Network Address Translation 19
Online games 20
Operating system 21
Package filter
  Packet inspection 21
Packet inspection 21
Parental Control 22
Plug & Play 21
Policies 21. *See* Rules
Pool 19
Port Triggering 21
Ports 20
Pre Shared Key (PSK) 23
Private IP addresses 19
Programming language 21
Public IP address 19
Range 23
Range Extender 24
Rules 21
Schedule Rule 21
SNMP
  Simple Network Management Protocol 22
Tunnel 22
UPnP
  Universal Plug and Play 21
URL Blocking 21
Virtual Server 22
Viruses 20
VPN
  Virtual Private Networking 22
WDS
  Wireless Distribution System 23
WEP encryption 23
Wi-Fi Protected Access *See* WPA
WPA 23
WPA2 23

Försäkran av Överensstämmelse

För din säkerhets skull och för att uppfylla gällande direktiv skapade av EU-kommissionen kan du få en kopia av Försäkran av Överensstämmelse gällande denna produkt genom att skicka ett e-brev till: info@eminent-online.com. Du kan även skicka ett brev till:

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

Var vänlig märk brevet tydligt med 'Försäkran av Överensstämmelse' samt artikelnumret på produkten det gäller.

EMINENT

WWW.EMINENT-ONLINE.COM

EM4450 | 06-2008