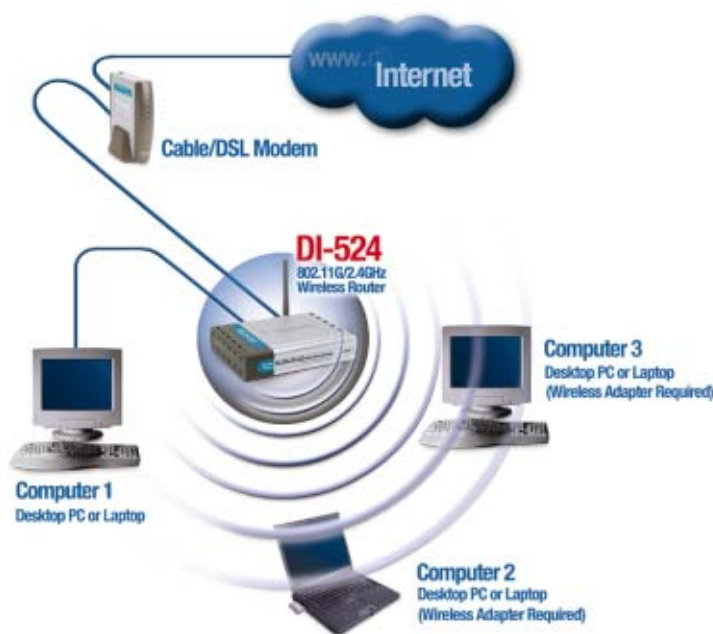




**Wireless Information
& Security Guide**
2005/06

Generell trådlös information

Ett trådlöst nätverk är troligen det enklaste och mest kostnadseffektiva alternativet när det gäller att dela en Internetanslutning mellan flera datorer och/eller medienheter. Men eftersom den trådlösa signalen är luftburen kan den, och kommer den, att påverkas av omgivningen, som t ex väggar, tak, andra trådlösa signaler och elektriska fält. Detta är något du måste ha i åtanke när du köper och installerar ett trådlöst nätverk.



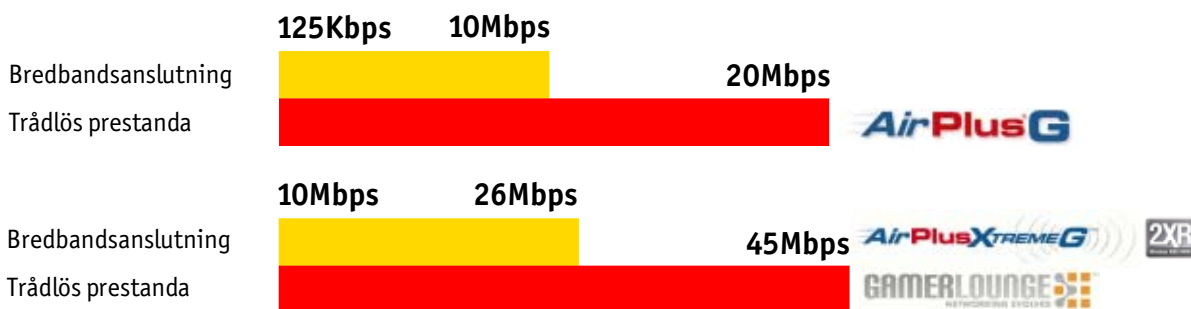
Värt att fundera på innan du investerar i ett trådlöst nätverk:

1. Vilken typ av bandbredd och prestanda behöver jag?

Det beror helt och hållet på vad du ska använda det trådlösa nätverket till. Om du bara vill dela Internet-anslutningen mellan några få användare för surfing och e-post kan du välja de billigare produkterna i [AirPlusG-serien](#), med en maximal teoretisk hastighet på 54Mbps som baseras på 11g-standard. Men om du vill skicka stora filer, spela spel, streama eller lyssna på musik eller titta på video behöver du högre prestanda. Det kan du få från [AirPlus XtremeG-serien](#) med 108Mbps-produkter liksom från sortimentet av [MIMO-produkter](#). Om du spelar mycket spel kan vi definitivt rekommendera [GamerLounge](#)-produkterna.

2. Vilken trådlös bandbredd rekommenderas till min bredbandsanslutning?

Det beror på vilken tjänst som ingår i det abonnemang du har hos din Internetleverantör (testa på www.tpctest.se). De vanligaste tjänsterna ligger på mellan 125Kbps och 26Mbps (kan vara upp till 100Mbps). Nedan kan du se vilken typ av trådlös serie vi rekommenderar för en viss bredbandsanslutning:



Som du ser ovan är den trådlösa signalens faktiska hastighet lägre än standarden anger, vilket man enklast kan förklara genom att ta en bilmotor som exempel: bilmotorn kommer att ha extremt hög prestanda om den testas utanför bilen, men när motorn sedan placeras i bilen kommer dess prestanda att påverkas av en rad faktorer som vikt, hjul, passagerare etc. Samma sak gäller för trådlösa prestanda – utan trafikbelastning har signalen den prestanda som standarden anger, men med belastning i form av datapaket minskar signalens prestanda. Detta är normalt och gäller för alla trådlösa produkter på marknaden.

3. Vilken täckning behöver jag med min trådlösa anslutning?

Eftersom signalerna går genom luften kan de påverkas av miljöfaktorer som väggar, elektriska fält och annan trådlös utrustning, t ex DECT-telefoner. Om du har en DECT-telefon som använder 2,4GHz-bandet ska du tänka på att placera basenheten så långt bort från din trådlösa utrustning som möjligt. Basenheten sänder ut en signal även när telefonen inte används. Det innebär att du aldrig kan vara säker på att få önskad täckning, men du kan göra en del åtgärder för att förbättra din täckning.

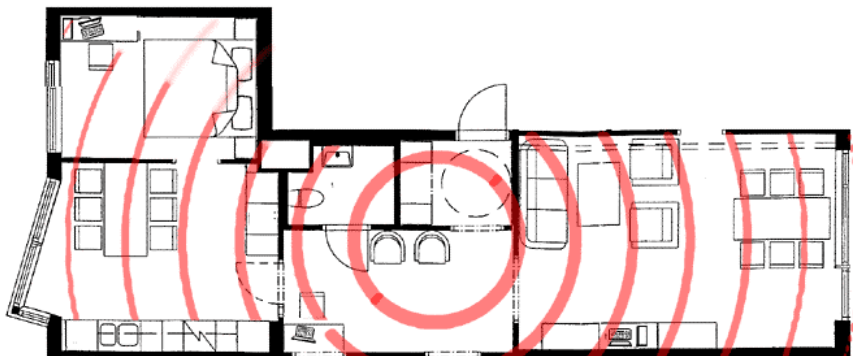
För det första ska du välja produkter vars befintliga antenn kan bytas ut mot en **antenn** med högre prestanda. Alla D-Links produkter utom de kombinerade a/b/g-produkterna (*AirPremier AG*) samt MIMO-produkterna har denna funktion. MIMO-produkterna har dock redan bättre prestanda och räckvidd tack vare MIMO-tekniken som använder sig av effektivare chipsteknik och fler antenner som byggs in från början.

För det andra ska du välja en klok placering av routern så den trådlösa räckvidden blir så optimal som möjligt:

- "Göm" inte routern i ett skåp eller bakom datorskärmen. Utseendemässigt är det kanske den bästa lösningen men du kan få kraftigt försämrad trådlös prestanda.

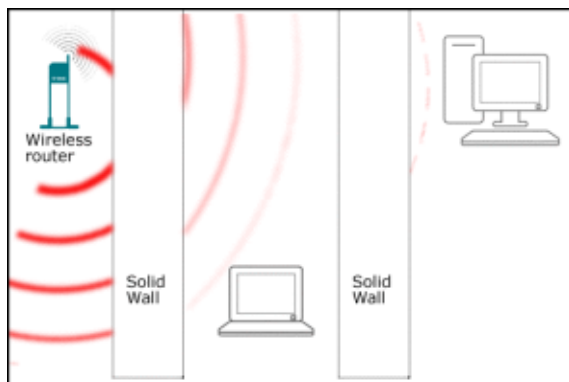


Om routern står i ett hörn av lägenheten kommer vissa områden att få dålig anslutning eller helt sakna mottagning. I detta exempel skulle datorn i vardagsrummet få en mycket svag anslutning till nätverket.



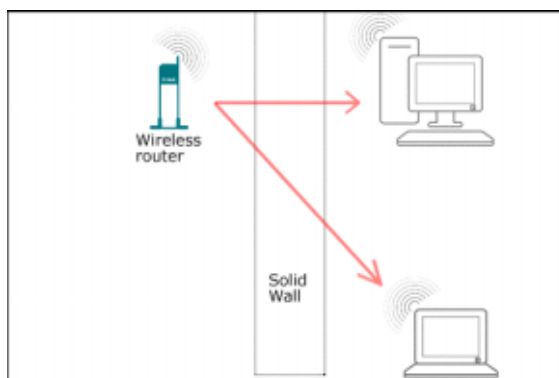
En centralt placerad router ger bättre uppkoppling. Tänk på att nätverkshastigheten minskar med avståndet till routern. Du kan t ex få 10Mbps i närheten av routern men kanske bara 5Mbps tio meter bort.

- b. Se till att ha så få väggar och tak mellan nätverksenheterna som möjligt – varje vägg eller tak kan minska nätverkets räckvidd. Placera enheterna så att antalet väggar och tak mellan dem blir så få som möjligt.



Den första datorn i detta exempel skulle ha en anslutning (om än ganska svag) till nätverket. Den andra datorn skulle troligen inte få någon mottagning alls.

- c. Tänk på att ha en rak linje mellan nätverksenheterna. Signalen färdas den kortaste och inte den enklaste vägen mellan enheterna. En vägg som är 0,5 meter tjock uppfattas vid en 45-gradersvinkel som nästan 1 meter tjock. För bättre mottagning ska du placera enheterna så att signalen färdas rakt igenom väggen eller taket (i stället för i en vinkel).



Trots att väggen är lika tjock överallt måste de trådlösa signalerna till den bärbara datorn färdas mycket längre än till den stationära datorn.

- d. Se till att ha ett avstånd (på minst 1–2 meter) mellan produkten och elektrisk apparatur eller utrustning som alstrar radiofrekvent brus.
- e. Byggmaterialet har betydelse. En massiv metalledör eller aluminiumreglar kan påverka räckvidden negativt. Försök placera accesspunkter, trådlösa routrar och datorer så att signalen går genom gipsväggar eller öppna dörrar. Material och föremål såsom glas, stål, metall, isolerade väggar, vatten (akvarier, golvvärme), speglar, dokumentskåp tegel och betong försämrar den trådlösa signalen avsevärt.

Så hög och tydlig placering som möjligt är nyckeln till framgång!

4. Vilken säkerhetsnivå behöver jag?

Grundregeln är naturligtvis att försöka ha en så hög säkerhetsnivå som möjligt och vi rekommenderar att du använder antingen WPA eller den nyare och mer kraftfulla WPA2 som krypteringsstandard i ditt trådlösa nätverk. Den äldre WEP-standarderna fungerar naturligtvis också men ger ett sämre skydd.

WEP (Wired Equivalency Protocol)

Nätverkssäkerheten är oerhört viktig, i synnerhet för applikationer eller program som innehåller värdefull information. WEP krypterar informationen i nätverket så att endast den tilltänkta mottagaren kan få tillgång till den. 64 och 128 bitars kryptering är två nivåer av WEP-säkerhet. WEP kodar din data med hjälp av en "krypteringsnyckel" innan de sänds ut på trådlös väg. Ju längre nyckeln är, desto kraftfullare blir krypteringen. Alla mottagarenheter måste känna till denna nyckel för att kunna kommunicera. Nycklarna anges som strängar med 10 eller 26 hexadecimala tecken (0-9 samt a-f). Till D-Links produkter hör en webbaserad installationsguide som vägleder dig steg för steg genom installationen av nätverkssäkerheten.

Aktivering av 128 bitars WEP-kryptering hindrar hackare från att få åtkomst till dina filer eller använda ditt höghastighetsinternet. Men eftersom säkerhetsnyckeln är statisk, eller inte ändras, är det fortfarande möjligt för en målmedveten inkräktare att ta sig in i ditt nätverk efter att ha lagt tillräckligt mycket tid och möda på detta. Därför är det klokt att ändra WEP-nyckeln ofta. Trots denna begränsning är det bättre att ha WEP än ingen säkerhet alls och WEP bör aktiveras som en miniminivå av säkerhet.

WPA (Wi-Fi Protected Access)

WPA använder sig av dynamisk nyckelkryptering, vilket innebär att nyckeln ständigt ändras och att det därför är svårare att ta sig in i det trådlösa nätverket än om man använder WEP. WPA anses som en av de högsta nivåerna av trådlös säkerhet för nätverk och är att rekommendera om din utrustning stöder denna typ av kryptering. Inom WPA finns det två versioner, dessa tillämpar olika procedurer för autentisering:

- * För privat användning i hemmet: Temporal Key Integrity Protocol (TKIP) är en typ av metod som används för att skapa dynamisk nyckelkryptering och ömsesidig autentisering. TKIP erbjuder de säkerhetsfunktioner som åtgärdar begränsningarna med WEP. Eftersom nycklarna hela tiden ändras får nätverket en mycket hög säkerhetsnivå.
- * För användning i företagsmiljö: Extensible Authentication Protocol (EAP) används för meddelandeutbyte under autentiseringsprocessen. Med hjälp av 802.1x-servertekniken autentiseras användare via en RADIUS-server (Remote Authentication Dial-In User Service). Denna lösning ger ditt nätverk säkerhet i företagsklass men kräver en RADIUS-server.

WPA2 är andra generationen av WPA. WPA2 har utvecklats för att inte påverkas av begränsningar i WPA och är bakåtkompatibel med produkter som stöder WPA. Den största skillnaden mellan den ursprungliga WPA och WPA2 är att WPA2 kräver Advanced Encryption Standard (AES) för kryptering av data medan den ursprungliga WPA arbetar med TKIP (se ovan). AES erbjuder en säkerhetsnivå som uppfyller de höga kraven hos många statliga institutioner. I likhet med ursprungliga WPA stöder WPA2 versioner för såväl hem som företag.

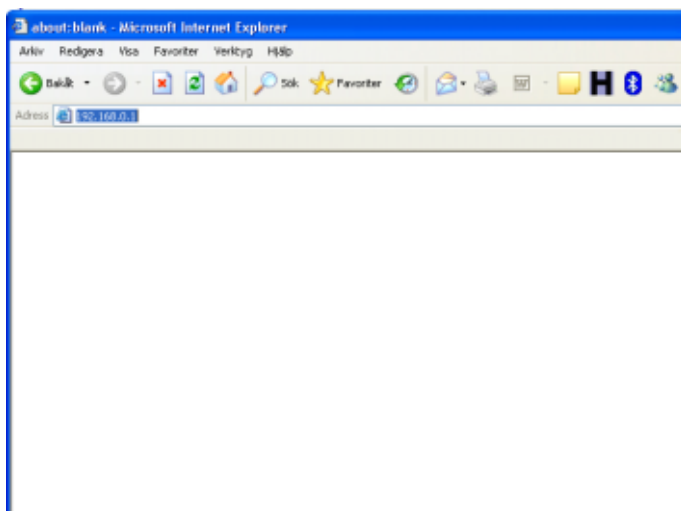
Fem enkla åtgärder för att skydda ditt trådlösa nätverk

En nätverkslösning gör livet enklare. Du kan dela Internetuppkoppling, musik, videofilmer och data med familj, vänner och kollegor, men du kanske inte vill dela din information med vem som helst. Med ett trådlöst nätverk transporteras informationen via radiovågor och inte genom fysiska ledningar, vilket betyder att alla inom räckviddsområdet kan "avlyssna" nätverket. Därför måste du skydda ditt trådlösa nätverk. Här följer fem grundläggande, standardiserade säkerhetsåtgärder som du bör vidta för att skydda ditt trådlösa nätverk:

Exemplen i denna guide baseras på D-Links DI-524 men i princip går installationen till på samma sätt för alla D-Links routrar. Du bör emellertid ändå **titta i din Snabbinstallationsguide** när det gäller detaljer som rör just din produkt.

(Obs! Alla åtgärder som beskrivs i detta dokument förutsätter att du har loggat in till routern. Detta beskrivs här i detalj.)

Logga in i din router genom att ange routerns IP-adress (standard 192.168.0.1).



En inloggningsruta visas:



Logga in genom att ange användarnamnet "admin" och ditt aktuella lösenord (tomt fält som standard).

1. Byte av standard-SSID

Din trådlösa utrustning har en standard-SSID (Service Set Identifier) som ställts in på fabriken. SSID är namnet på ditt trådlösa nätverk och kan innehålla upp till 32 tecken. Hackare känner till dessa standardvärden och kan utnyttja dem för att ta sig in i ditt nätverk. Ändra nätverkets SSID till något unikt, och se till att namnet inte relaterar till de nätverksprodukter du använder. Som en extra säkerhetsåtgärd bör du byta SSID regelbundet så att eventuella hackare som tidigare tagit reda på ditt nätverks SSID ständigt måste ta reda på ditt nya SSID. Det kommer att avskräcka från framtida försök till intrång.

Så här ändrar du standard-SSID:



Klicka på knappen "Wireless" (trådlöst) i menyn till vänster.



Ändra SSID och klicka på knappen "Apply" (verkställ).

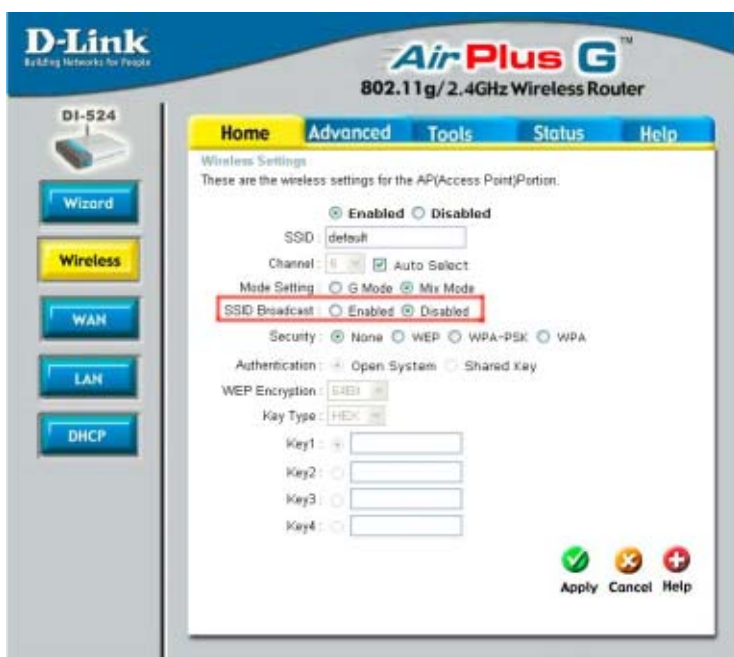
2. Inaktivering av SSID-visning

De flesta trådlösa nätverksenheter sänder som standard ut SSID så att vem som helst lätt kan få åtkomst till det trådlösa nätverket, endast med hjälp av denna information. Men hackare kan också ansluta sig, så om du inte driver en allmän surfzon är det säkrast att inaktivera SSID-visningen. Du kanske tycker att det är mer praktiskt att din SSID sänds ut så att du kan klicka på den för att komma in i ditt nätverk, men det går att konfigurera enheterna i nätverket så att de automatiskt ansluts till ett SSID utan att SSID visas publikt från din router.

Så här inaktiverar du SSID-visningen:



Klicka på knappen "Wireless" (trådlöst) i menyn till vänster.



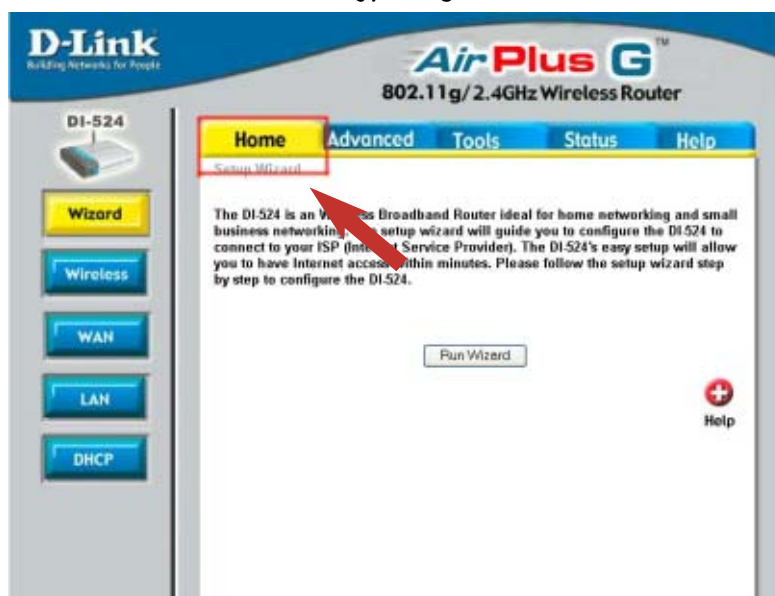
Markera "SSID Broadcast" (SSID-visning) som "Disabled" (inaktiverad) och klicka på knappen "Apply" (verkställ).

3. Krypteringsaktivering

Krypteringen ger ett skydd för data som överförs via ett trådlöst nätverk. Wired Equivalency Protocol (WEP) och Wi-Fi Protected Access (WPA) erbjuder olika säkerhetsnivåer för trådlös kommunikation. WEP är just nu den vanligaste krypteringsnivån och den stöds av fler enheter än WPA.

WPA anses vara säkrare än WEP eftersom den tillämpar dynamisk nyckelkryptering. För att skydda informationen när den sänds via radiovågor bör du aktivera den högsta krypteringsnivå som din nätverksutrustning stöder.

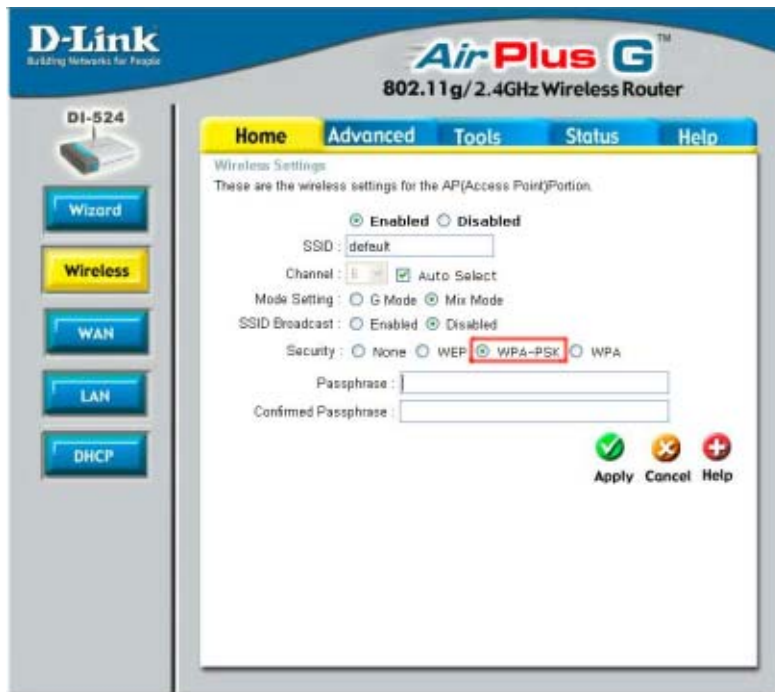
Så här aktiverar du WPA-PSK krypteringen:



Klicka på knappen "Home" (hem) i menyn högst upp.



Klicka på knappen "Wireless" (trådlöst) i menyn till vänster.



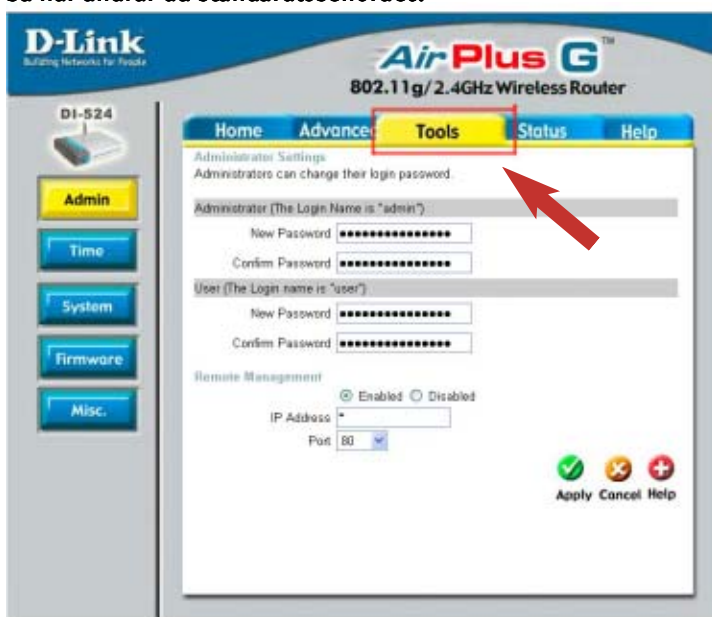
Under "Security" (säkerhet) ska du klicka i alternativknappen "WPA-PSK".
Skriv in ett lösenord (Passphrase) som innehåller minst 8 tecken.
Giltiga tecken är a–z och 0–9. Du kan blanda små och stora bokstäver.
Bekräfta lösenordet (Confirmed Passphrase).

Klicka på knappen "Apply" (verkställ) för att spara inställningarna.

4. Ändring av standardlösenord

När du ska ändra inställningar för trådlösa produkter som accesspunkter och routrar måste du uppge ett lösenord. Dessa enheter har ett standardlösenord som ställts in på fabriken. (D-Links standardlösenord är "admin".) Hackare känner till detta standardlösenord och kommer att testa det för att försöka få åtkomst till din trådlösa utrustning och ändra dina nätverksinställningar. För att förhindra detta måste du ge enheten ett personligt lösenord som är svårt att komma på.

Så här ändrar du standardlösenordet:



Klicka på knappen "Tools" (verktyg) i menyn högst upp.



Ändra båda lösenorden.

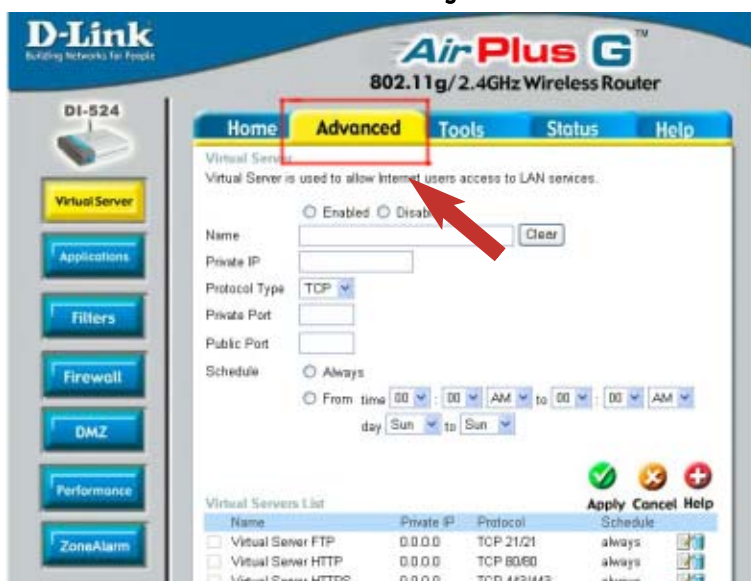
Välj lösenord som är svåra för inkräktare att komma på genom att använda både siffror samt stora och små bokstäver.

Klicka på knappen "Apply" (verkställ) för att spara lösenorden.

5. Aktivering av MAC-adressfiltrering

Med D-Links routrar har du möjlighet att aktivera MAC-adressfiltrering (Media Access Control). MAC-adressen är en unik serie av siffror och bokstäver som alla nätverksenheter tilldelas. När MAC-adressfiltreringen är aktiverad har endast trådlösa enheter med vissa MAC-adresser åtkomst till det trådlösa nätverket. Du kan till exempel ange att endast datorer i ditt hem ska ha åtkomst till det trådlösa nätverket. Det skulle vara mycket svårt för en hackare att få åtkomst till ditt nätverk med hjälp av en slumpvis vald MAC-adress.

Så här aktiverar du MAC-adressfiltreringen:



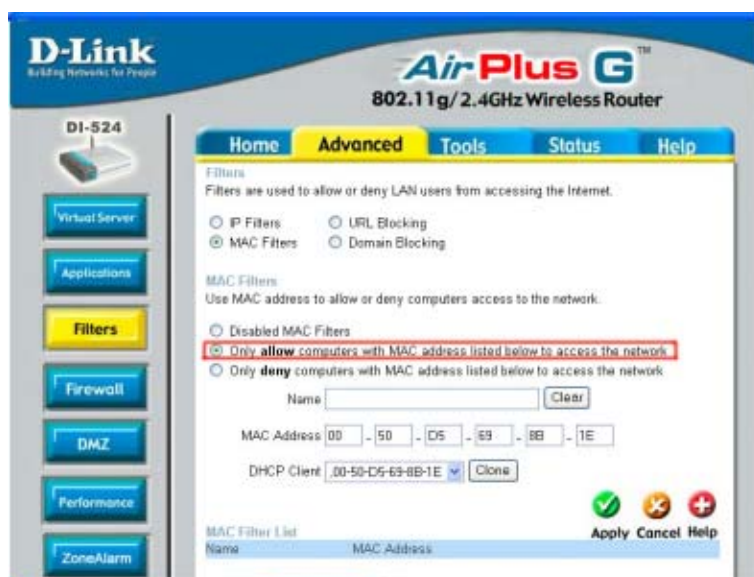
Klicka på knappen "Advanced" (avancerat) i menyn högst upp.



Klicka på knappen "Filters" (filter) i menyn till vänster.



Klicka på knappen "MAC filters" (MAC-filter) och vänta tills sidan laddats om.



Markera alternativknappen "Only allow..." (Tillåt endast).

Ange ett namn på datorn.

Skriv antingen in en MAC-adress manuellt eller välj en från listan över DHCP-klienter och klicka på "Clone" (kopiera) för att kopiera adressen till MAC-adressfältet.

Klicka på knappen "Apply" (verkställ) för att lägga till klienten på listan över godkända MAC-adresser.

Upprepa proceduren för alla datorer som du vill ska ha åtkomst till nätverket.

Om du följer dessa allmänna riktlinjer och vidtar dessa säkerhetsåtgärder lär du få mycket glädje av ditt trådlösa nätverk från D-Link och du kommer att kunna arbeta säkert. Som alltid när det är fråga om trådlös utrustning kan miljöfaktorer störa signalerna olika mycket på olika platser.

Produkter:

Här följer en kort lista över produkter i de olika sortimenten. För en komplett produktlista är du välkommen att besöka D-Links hemsida.

AirPlus G

AirPlus G-sortiment av 54Mbps-konsumentprodukter till låga priser:



DI-524
54Mbps trådlös bredbandsrouter



DWL-G122
54Mbps trådlös USB adapter



DWL-G630
54Mbps trådlöst PC-Card



DWL-G510
54Mbps trådlöst PCI card

AirPlus Xtreme G

AirPlus Xtreme G-sortiment av högpresterande 108Mbps SuperG-produkter:



DI-624
108Mbps SuperG trådlös
bredbandsrouter



DWL-G132
108Mbps SuperG trådlös
USB adapter



DWL-G650
108Mbps SuperG trådlöst PC-Card



DWL-G520
108Mbps SuperG trådlöst PCI card



AirPlus Xtreme G-sortiment av högpresterande 108Mbps MIMO-produkter:



DI-634M
108Mbps SuperG MIMO
trådlös bredbandsrouter



DWL-G520M
108Mbps SuperG MIMO
trådlöst PCI card



DWL-G650M
108Mbps SuperG MIMO
trådlöst PC-Card



GamerLounge-sortiment av högpresterande 108Mbps-spelprodukter:



DGL-4300
108Mbps SuperG trådlös
Gigabit bredbandsrouter



Air-sortiment av antenner avsedda för konsumentmarknaden:



ANT24-0501
5dBi 11b/11g omni-directional
antenn



ANT24-0600
5dBi 11b/11g omni-directional
antenn