Denne guide er oprindeligt udgivet på Eksperten.dk

COMPUTERWORLD

Opsætning af router med trådløst netværk trin1 - eksempel med Linksys router

Her vil jeg beskrive hvordan du opsætter en router og bruger Linksys routeren wrt54g som eksempel. Men min gennemgang kan fint bruges på andre routere også.
Jeg vil bl.a prøve at forklare fordele ved at have en router...

Skrevet den **24. Mar 2009** af **serverservice** I kategorien **Netværk / Routers/Switches** | ★★☆☆☆

Er I flere brugere på et netværk er det en fordel at anvende en router af flere grunde.

1.Flere computere på samme netværk. Det er muligt at uddele op til 253 ip adresser og derved have et større antal pcér på nettet.
2.Økonomi. Du skal ikke betale for ekstra ip adresser ved en udbyder - som det bl.a er ved nogle selskaber f.x TDC.
3.Sikkerhed. Routeren har firewall og du er placeret bagved på dit lokale netværk, hvilket giver en god sikkerhed.
4.Firewall. Du har mulighed for selv at sætte ekstra sikkerhed op ved at begrænse åbne porte i et range du vælger.
5.Qos. Det er muligt at administrere/dele trafikken til computerne på netværket med Qos.
6.Deling over netværk - Det er muligt at dele filer og printere.

Når Routeren er forbundet til internettet og pcérne til lan porte på routeren kan du gå i gang med at konfigurere den.
Du konfigurerer fra din browser via adressen http://192.168.1.1 , som er gateway ip.
Vil du være ekstra sikker starter du med at konfigurere routeren lokalt fra en pc og tilslutter den så bagefter til internettet.

Som de fleste andre routere har wrt54g også en sikkerheds brist - nemlig at den som standard har et åben adgang til trådløs netværk og trådløs netværk aktiveret.

For hver faneblad skal man huske at gemme med "save settings" knappen. I det følgende er **Faneblade** med understreget+fed og **undermenuer** med fed

Wireless
Vi starter derfor med at konfigurere det trådløse netværk og sætte password på.

Som grundlæggende er der 3 ting som er vigtige i wireless setup.

Ssid (det trådløse netværks navn)
Channel (kanal frekvens)
Sikkerhed (krypteringsteknologi)

Basic wireless.

Wireless Network Mode: Her vælger du enten B (11Mbit) eller G (54Mbit) eller mixed for b+g
Wireless Network Name (SSID): Det trådløse netværksnavn
Wireless Channel: Kanal - som standard er valgt ch11
Wireless SSID Broadcast: Du kan skjule dit trådløse netværk ved at disable Ssid broadcast

Ved at skjule Ssid får du en bedre sikkerhed da navnet ikke kan ses - ulempen er så at du skal indstille det manuelt på din pc´s trådløse netkort.

Wireless Security
Her bør du som standard vælge min. wpa og ikke wep som regnes for mindre sikker og kan hackes.
Derefter vælger du dit trådløse password.

Administration
Af sikkerhedsgrunde bør du sætte dit eget password til login på routeren - det forhindrer andre på dit netværk i at få adgang med standard password.
Har du brug for administration via internet enabler du remote management - det samme gør du hvis vil have adgang udefra via trådløs = Wireless Access Web. For max sikkerhed bør du vælge Https.

Firmware upgrade
Her kan du opgradere firmware ("bios") på din router - men du skal bruge routerens model og versions nummer for at søge den rigtige - og gøre det via kabel tilslutning.
En firmware opdaterer softwaren på routeren og giver ofte flere muligheder - der findes også alternative firmware lavet af programmører bla. Kan nævnes tomatoo.
Har du ikke brug for andre settings eller er du i tvivl om firmware - så lad være med at opgradere.

Setup
Som standard står den her til Automatisk Ip for internetporten - har du en fast ipadresse skal du indstille det her.

Local Ip adress 192.168.1.1 = Roterens ip = gateway for pcérne
subnet mask 255.255.255.000 (standard)
DHCP er enabled

Mht. router Ip har jeg set tilfælde hvor man havde 2 routere i forlængelse af hinanden - her er det vigtigt at de er nattet rigtigt - dvs. adskilt med forskellige ipadresser ellers kan man ikke opnå routing. Det er en standard regel indenfor netværk.

Router som gateway
Anvendes routeren kun som gateway til internettet skal dhcp slåes fra.
Det anvendes ofte på server netværk , hvor serveren er DHCP og DNS - og routeren gateway til internettet.

Mac adress cloning
Vil du clone (kopiere) macadressen fra din pc til routeren gør du det her. Eneste tilfælde jeg lige kan komme i tanke om at det er brugbart er ved de udbydere hvor man fra start registrerer brugernes macadresser og det findes der flere eksempler på.

Security
Under security sættes indstillingerne for den indbyggede firewall og som standard er sat:

Block Anonymous Internet Requests x
Filter Multicast x

Filter Internet NAT Redirection
Filter IDENT(Port 113) x

Access restrictions
Her kan du selv indstille firewallen for begrænsninger i trafik til internettet. Du kan oprette en policy og vælge hvilke dage der skal være adgang eller ikke. Du kan desuden vælge hvilke pcér den skal gælde for ved at anvende mac filtrering.

Mac filtrering
Her bestemmer du hvilke macadresser (netkort) der skal have adgang til routerens netværk - og er god som en ekstra sikkerhed på mindre netværk op til 8 pcér.
Blocked services - her kan du blokere et antal porte i firewallen så ikke alle porte står åbent til internettet. Det er med til at skabe ekstra sikkerhed mod hacking.

Website Blocking by URL Address - Website Blocking by Keyword.
Det er en form for filter der skulle virke som en slags forældrekontrol , men af en eller anden grund fungerer det ikke som det skal. Det er muligt at det vil virke med anden firmware.

Application and Gaming
Denne fane er til at administrere serveradgang udefra internettet og ind på dit netværk - det kan være hvis du har en spilserver eller webserver på lannetværket.

Port range forwarding
Her sætter du port forwarding op - du viderestiller al trafik fra en bestemt port til en ipadresse på lannetværket - f.x port 80 dirigeres til en webserver der har ip 192.168.1.20 osv.
Dvs - skal andre kunne se din webserver fra internettet skal du anvende port forwarding

Andre eksempler kunne være remote desktop - hvis man er interesseret i adgang udefra via fjernskrivebord - så er det port 3389 man skal forwarde til en ip eller iprange.

Qos
Her kan der sættes forskellig prioritet på services på din server og der kan dele båndbredden mellem computere på Lannetværket.

DMZ
Demilitariseret zone - her åbner du alle porte ud til internettet til en bestemt ip på netværket. Det er det samme som at have sin pc koblet direkte til en offentlig ip på internettet udenom routeren - og du har fuld adgang men også laveste sikkerhed.

Status
Her kan du forny eller frigøre ip. Er god i tilfælde af fejlfinding hvor du mangler internet forbindelse. Eller bare kontrollere at ip er til stede - en anden god ide ved fejl er at slukke og tænde routeren igen, hvis den ikke umiddelbart vil forny ipadressen.