Deaktivering af tjenester i Windows 2000 Pro

En frisk installation af Win2000 har flere netværkstjenester kørende, som desværre kan udnyttes af computer-orme og andet snavs, som kan gøre livet surt for brugeren. Denne artikel er en kort gennemgang af de tjenester, man med fordel kan slå fra, for at sikre sin computer lidt bedre, inden den slippes løs på internettet

Hvilke tjenester man har behov for afhænger af, hvad computerens rolle er, men i mit tilfælde drejer det sig om en enkeltstående computer, som ikke skal yde netværkstjenester til andre computere. Computeren skal bare have adgang til internettet via en ADSL-bredbåndsforbindelse (DHCP uden router og med dynamisk IP-adresse). Dog vil denne vejledning også beskrive, hvad der skal køre for at få et LAN til at fungere.

Win2000 er nyinstalleret og netstikket er rykket ud af netkortet. Først når diverse netværkstjenester er lukket ned, bliver netstikket sat i. Erfaringen har vist mig, at man slipper for en del efterfølgende oprydningsarbejde, hvis man får lukket af for unødvendige tjenester, inden computeren får lov at komme på nettet.

Ved at starte en kommandoprompt og starte: netstat -an, kan man hurtigt få et overblik over, hvilke porte Win2000 har åbnet op for.

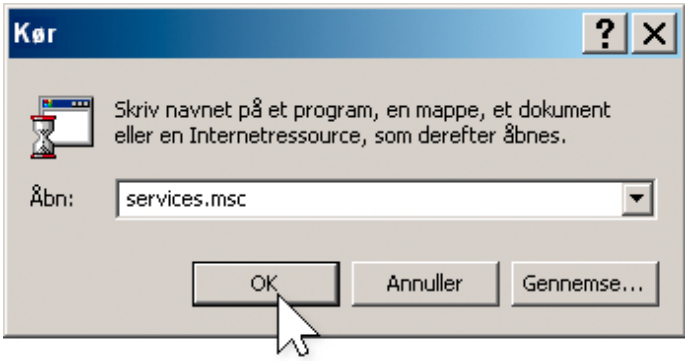
c:\>netstat -an

Aktive forbindelser

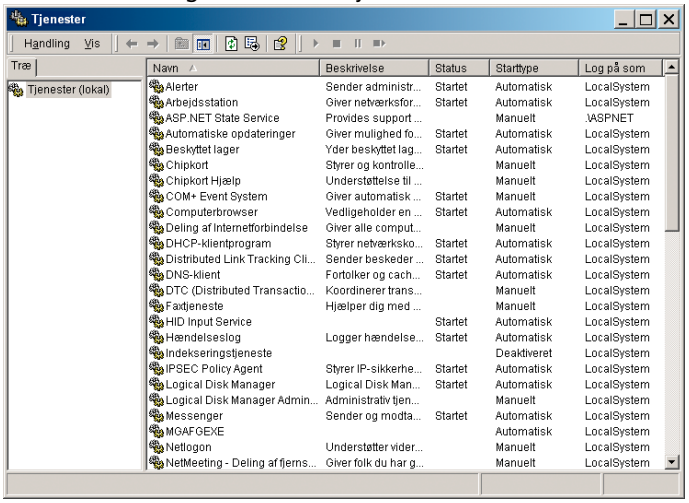
Proto	*Lokal adresse*	*Fjernadresse*	*Status*
TCP	*0.0.0.0:135*	*0.0.0.0:0*	*LISTENING*
TCP	*0.0.0.0:445*	*0.0.0.0:0*	*LISTENING*
TCP	*0.0.0.0:1025*	*0.0.0.0:0*	*LISTENING*
TCP	*0.0.0.0:1027*	*0.0.0.0:0*	*LISTENING*
UDP	*0.0.0.0:135*	**:**	
UDP	*0.0.0.0:445*	**:**	
UDP	*0.0.0.0:1026*	**:**	

Planen med denne artikel er, at få lukket ovenstående porte ved at deaktivere de netværkstjenester, som holder dem åbne.

Tjenesterne kan man komme ind til på flere måder. Man kan højreklikke på Denne Computer på skrivebordet og vælge punktet Administrer, man kan gå til Kontrolpanelet og vælge Administration > Tjenester, eller man kan gå ned i Start > Kør og starte services.msc, som vist på billedet herunder.



Dette skulle gerne starte Tjenester, som vist herunder.



Jeg starter med at højreklikke på tjenesten IPSEC Policy Agent, hvorefter der vælges Egenskaber. Det resulterer i et nyt vindue, hvor man har mulighed for at klikke på en stop-knap. Man har også mulighed for at vælge starttypen på tjenesten, som kan være enten Automatisk, Manuelt eller Deaktiveret. Jeg vælger Deaktiveret (se næste side).

Hvis en tjeneste står til Automatisk, vil den starte op, når Windows startes. Hvis den står til Manuelt, vil den kun blive startet, når der er behov for den, og når den står til Deaktiveret, vil den ikke blive startet sammen med Windows, uanset om der er behov for den eller ej.

Tjenesten ved navn Messenger og Remote Access Connection Manager deaktiveres også. Du skal være opmærksom på, at hvis du har netværksforbindelser oprettet, som forbinder via et analogt modem eller en ISDN-adapter, vil disse forbindelser forsvinde inde fra Start > Netværksforbindelser, når Remote Access Connection Manager bliver deaktiveret (det sker først efter en genstart af Windows). Hvis du har sådanne forbindelser oprettet, eller har planer om at oprette dem på et senere tidspunkt, vil det derfor være klogest at lade den tjeneste køre, men da jeg kun har brug for en LAN-forbindelse, vælger jeg at deaktivere den, for en sådan netværksforbindelse forsvinder ikke.

Hvis man forsøger at stoppe Remote Access Connection Manager, vil man muligvis få en advarsel som vist på nederste billede herude til højre. Hvis man får det, klikker man blot på OK og stiller starttypen til Deaktiveret. Tjenesten vil så ikke blive startet op ved næste genstart af Windows.

Tjenesten Opgavestyring, vælger jeg også at deaktivere, da ingen af mine programmer bruger den. Hvis man oplever problemer ved at have den tjeneste deaktiveret, kan man altid stille den til Automatisk igen. Visse tredjeparts-programmer som f.eks. antivirusprogrammers automatiske opdateringsfunktion, kan være afhængig af, at Opgavestyring kører, men det er de færreste.

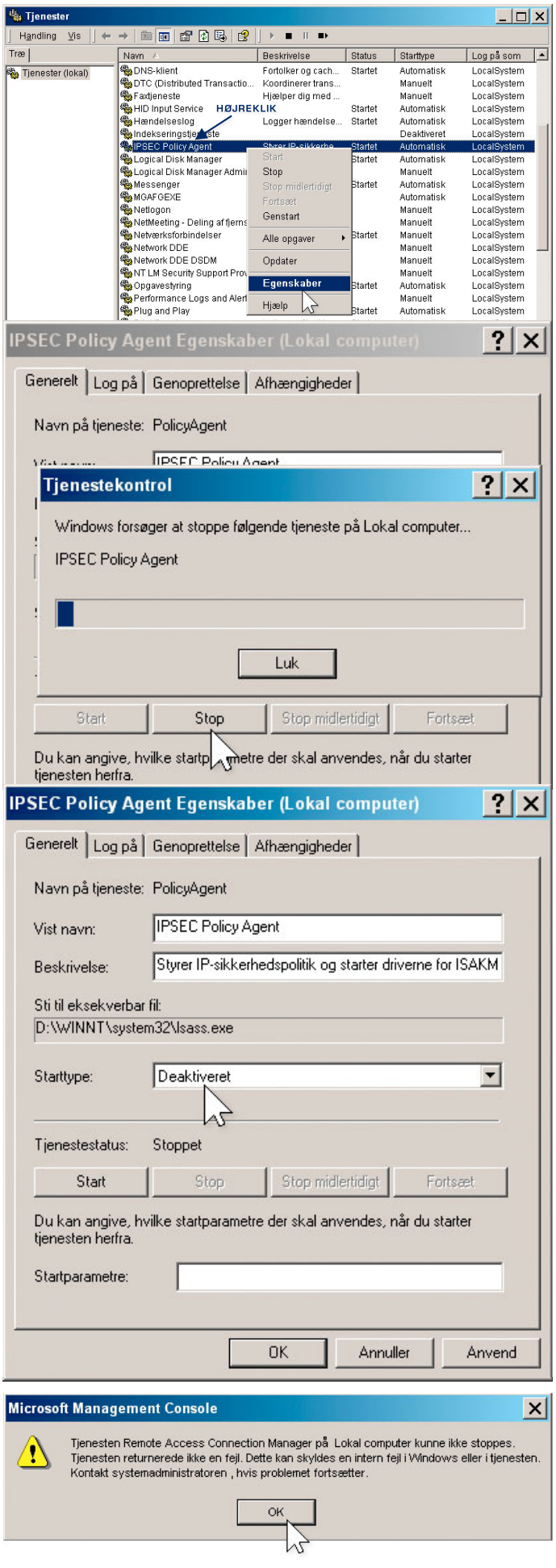
Efter en genstart, viser netstat -an i en kommandoprompt følgende:

c:\>netstat -an

Aktive forbindelser

Proto	*Lokal adresse*	*Fjernadresse*	*Status*
TCP	*0.0.0.0:135*	*0.0.0.0:0*	*LISTENING*
TCP	*0.0.0.0:445*	*0.0.0.0:0*	*LISTENING*
UDP	*0.0.0.0:445*	*:*	

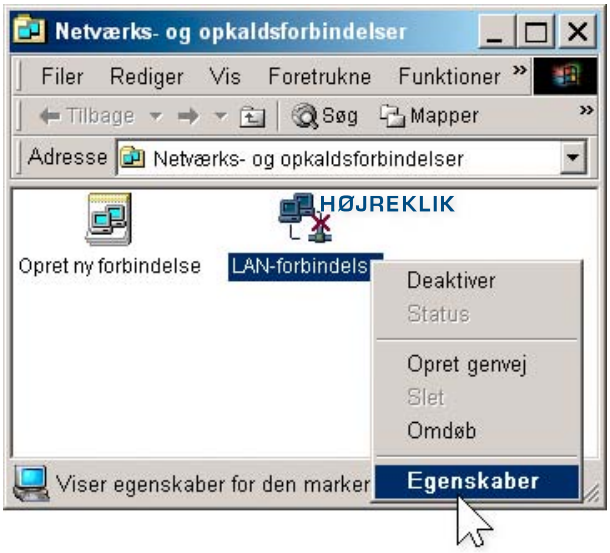
Vi har altså fået lukket for TCP:1025, TCP:1027, UDP:135 og UDP:1026 ved at deaktivere tjenesterne IPSEC Policy Agent, Messenger, Remote Access Connection Manager og Opgavestyring.



På denne side er beskrevet, hvad der skal køre for at få et LAN op at køre. Altså, et lokalt netværk imellem to eller flere computere. Hvis du ikke har brug for det, kan du springe denne side over og fortsætte på side 4.

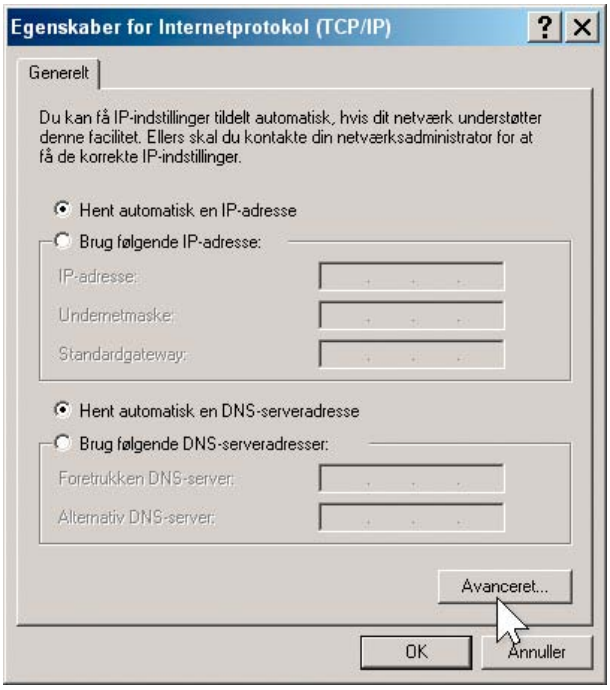
Ønsker man et LAN, kræver det, at man lader nogle tjenester køre, som rummer en vis risiko. Hvis man imidlertid benytter en router med NAT (det har de fleste) og en firewall (det har mange), så kan man godt have disse tjenester åbne, men en computer sat op på den måde, bør ikke sluttes direkte til internettet. I så fald kan man risikere at dele sin harddisk og filer med hele verden.

Klientprogram til Microsoft-netværk og fil- og udskriftsdeling skal være aktiverede, hvilket de er som standard. Du finder indstillingerne ved at gå i Start > Indstillinger > Netværksforbindelser, hvor du højreklikker på netværksforbindelsen og vælger Egenskaber.

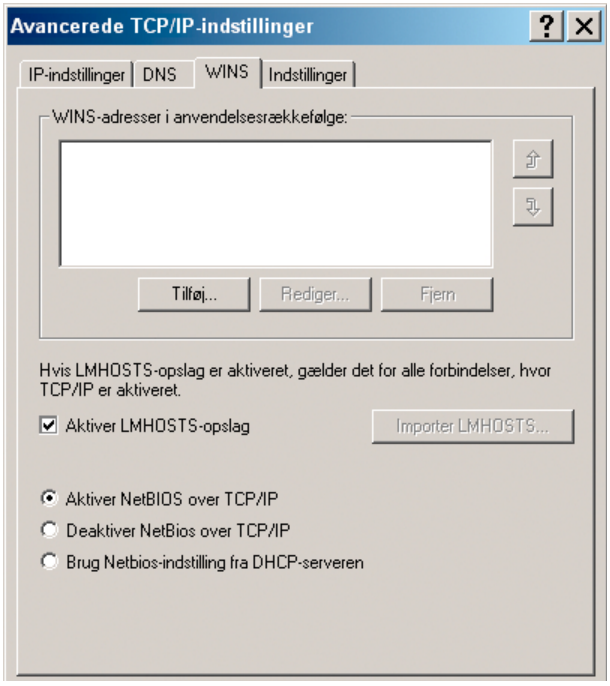


Under fanebladet Generelt, finder du indstillingerne.

Ved at markere protokollen Internetprotokol (TCP/IP) og vælge Egenskaber, kommer følgende skærmbillede:



Ved at klikke på Avanceret og derefter WINS-fanebladet, kommer man ind til følgende vindue, hvor NetBIOS skal være koblet til.

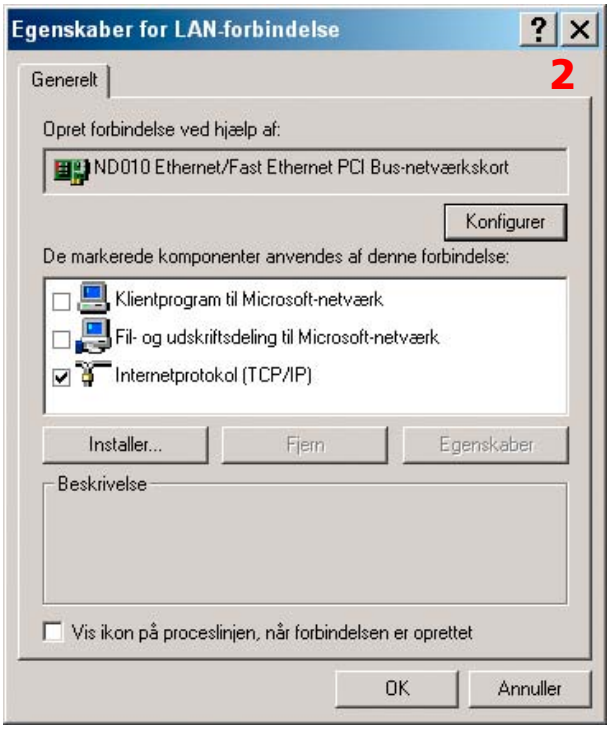


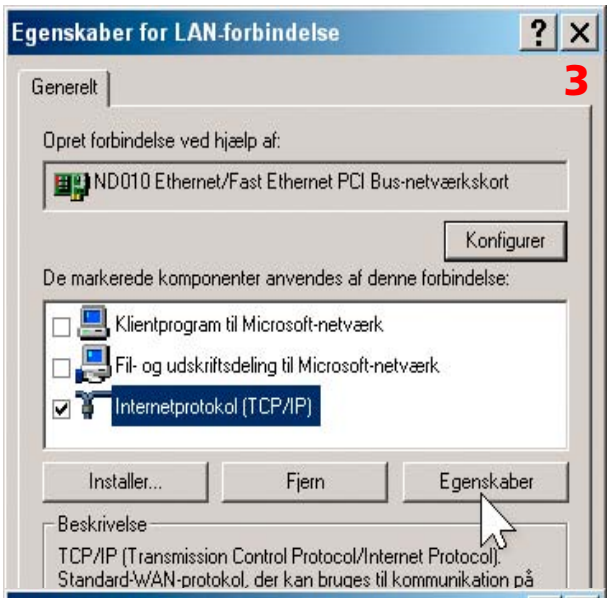
Derudover skal tjenesten TCP/IP NetBIOS Helper også køre, hvilket den også gør som standard.

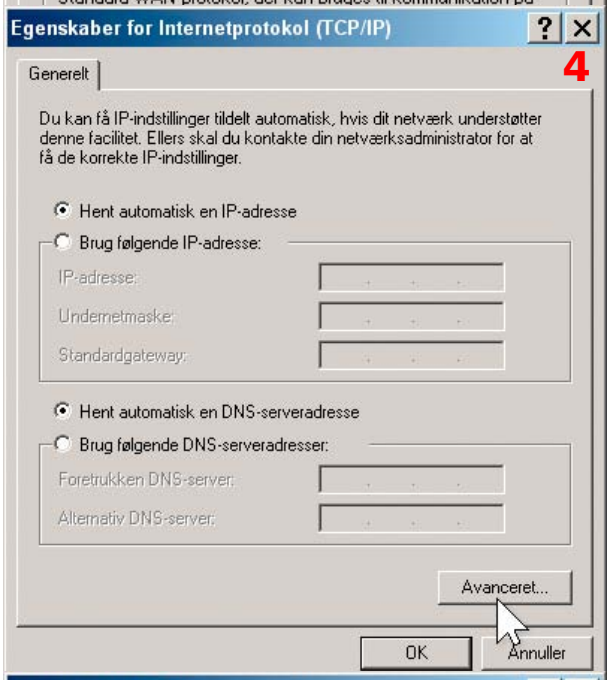
Hvis du ikke har behov for et LAN, kan Klientprogram til Microsoft-netværk, Fil- og udskriftsdeling til Microsoft-netværk samt NetBIOS over TCP/IP kobles fra, for de er ikke nødvendige for at få en enkeltstående computer på internettet. Disse kobles fra inde i Start > Indstillinger > Netværksforbindelser. Højreklik på netværksforbindelsen og vælg Egenskaber.

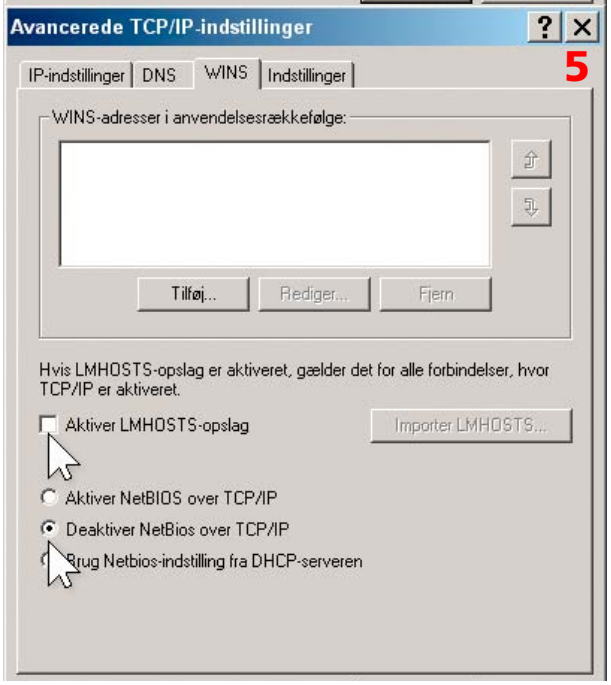
Fluebenet i Klientprogram til Microsoft-netværk og Fil- og udskriftsdeling til Microsoft-netværk fjernes.

Derefter markeres Internetprotokol (TCP/IP) og der klikkes på Egenskaber. Under fanebladet Generelt klikkes der på Avanceret og under fanebladet WINS fjernes fluebenet i „Aktiver LMHOSTS-opslag" og „Deaktiver NetBIOS over TCP/IP" kobles til.









TCP:445 holdes åben til SMB/CIFS-protokollen.
Man kan vælge helt at frakoble NetBIOS over TCP/IP-driveren (NetBT), men da tjenesten DHCP-klientprogram, som jeg har brug for, er afhængig af, at NetBT-driveren kører, vælger jeg i stedet at tilføje en værdi til registreringsdatabasen, som slår SMB-transporten over TCP:445 fra uden at frakoble NetBT-driveren. Dette gøres ved at gå ned i Start > Kør og starte: regedit.

Når man er inde i nøglen [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters], højreklikker man ovre i højre side og vælger punktet Ny > DWORD-værdi. Den nye værdi kaldes: SmbDeviceEnabled. Sørg for at værdien står til 0 (hvilket den burde stille sig til automatisk) og luk så registreringseditoren.

Efter endnu en genstart, viser netstat -an i en kommandoprompt dette:

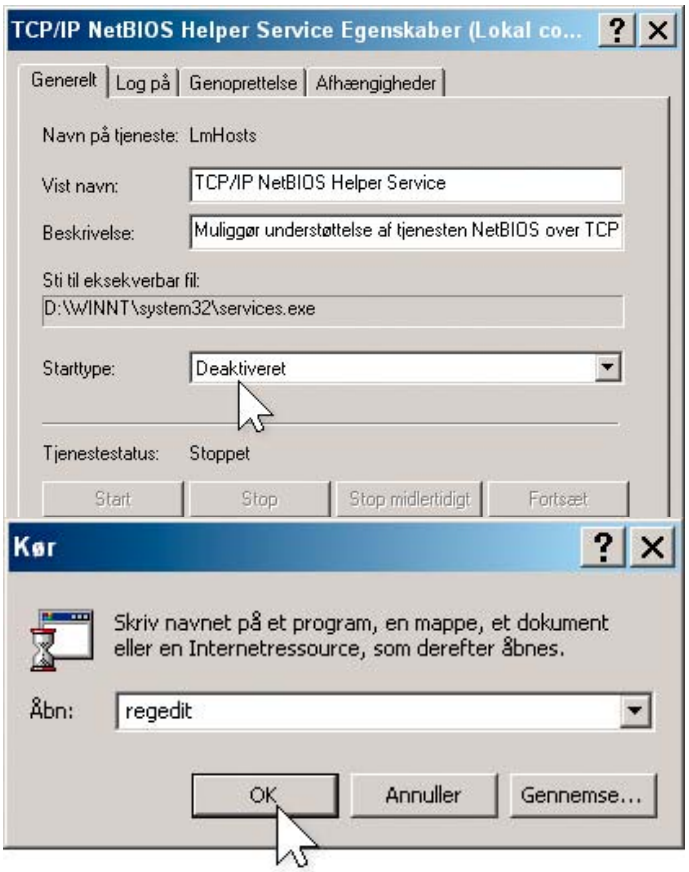
c:\>netstat -an

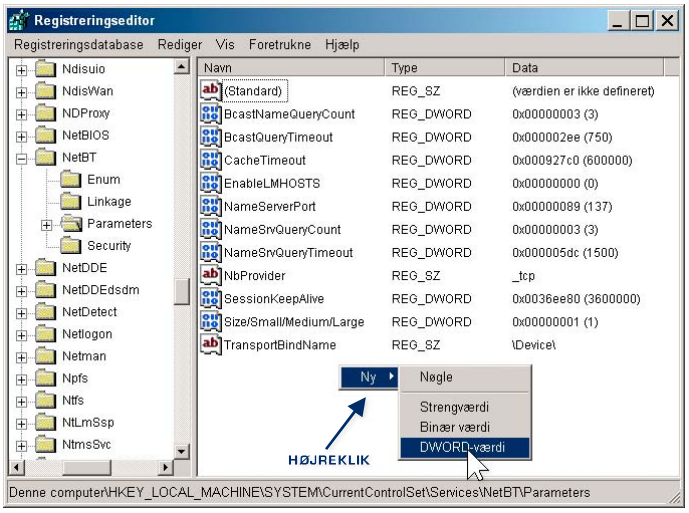
Aktive forbindelser

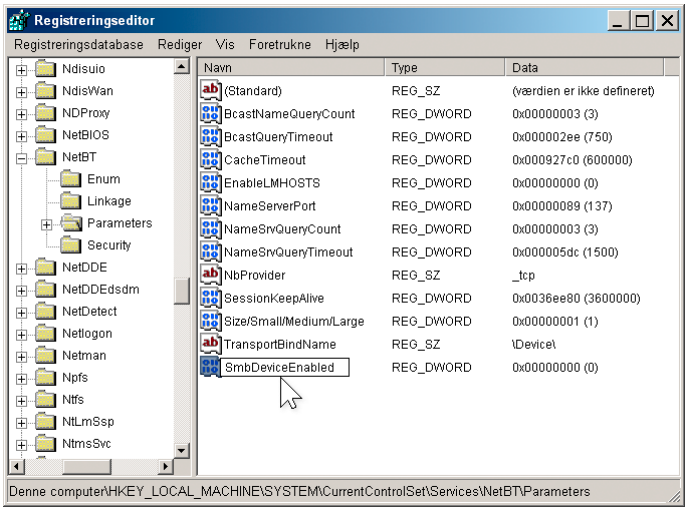
Proto	*Lokal adresse*	*Fjernadresse*	*Status*
TCP	*0.0.0.0:135*	*0.0.0.0:0*	*LISTENING*

TCP:135 holdes åben af RPC (Remote Procedure Call) og RPC kan ikke kobles fra, da den er en slags moder over alle tjenester, hvilket vil sige, at alle kørende tjenester er afhængige af RPC. Desværre er det sikkerhedshuller i netop RPC, som mange af dagens computer-orme forsøger at snige sig ind af (blaster-ormen f.eks.)

Heldigvis er der mulighed for at konfigurere Win2000, så RPC får lov at køre, men uden at TCP:135 åbnes og det kan bla. gøres med værktøjet Konfiguration af DCOM (se næste side).







Kontrolpanel > Administration > Component Services eller Start > Kør: dcomcnfg skulle gerne resultere i, at dialogboksen Egenskaber for Konfiguration af DCOM, kommer frem på skærmen. Under fanebladet Standardegenskaber fjernes fluebenet ud for „Aktiver DCOM på denne computer" og under fanebladet Standardprotokoller fjernes protokollen Forbindelsesorienteret TCP/IP, hvorefter der klikkes på OK for at lukke dialogboksen, som vist på billederne herude til højre.

Inden den sidste genstart, vælger jeg at deaktivere flere tjenester (med services.msc), som jeg ikke har behov for og det drejer sig om følgende i mit tilfælde:

Alerter
Computerbrowser
DNS-klient
DTC (Distributed Transaction Coordinator)
Tjenesten Remote Registry
TCP/IP NetBIOS Helper Service (hvis NetBIOS over TCP/IP ikke køres)

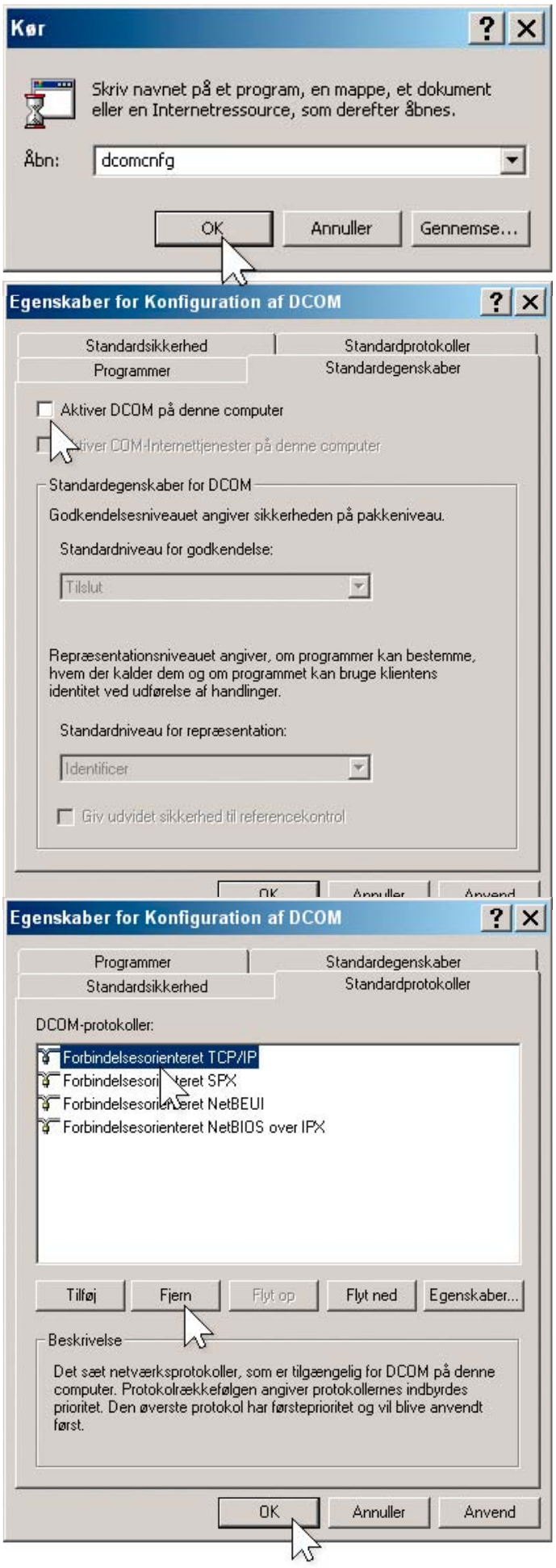
Efter en genstart, vil netstat -an i kommandoprompten vise dette:

c:\>netstat -an

Aktive forbindelser

Proto	*Lokal adresse*	*Fjernadresse*	*Status*

Du skal dog være opmærksom på, at RPC stadig kan finde på at åbne TCP:135. Det kan ske, hvis du f.eks. starter dcomcnfg. RPC vil i så fald blive ved med at holde TCP:135 åben indtil næste genstart.



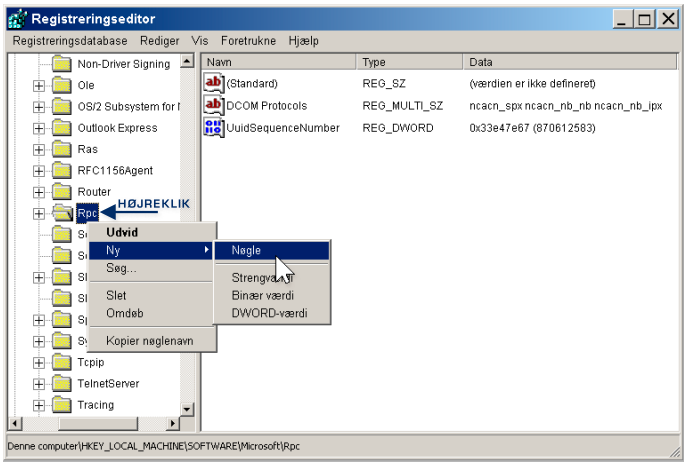
RPC's åbning af TCP:135 kan forhindres vha. en værdi i registreringsdatabasen, som tvinger den til ikke at lytte på internettet. Hvis du ønsker at tilføje den værdi, kan du gå ned i Start > Kør og starte regedit.

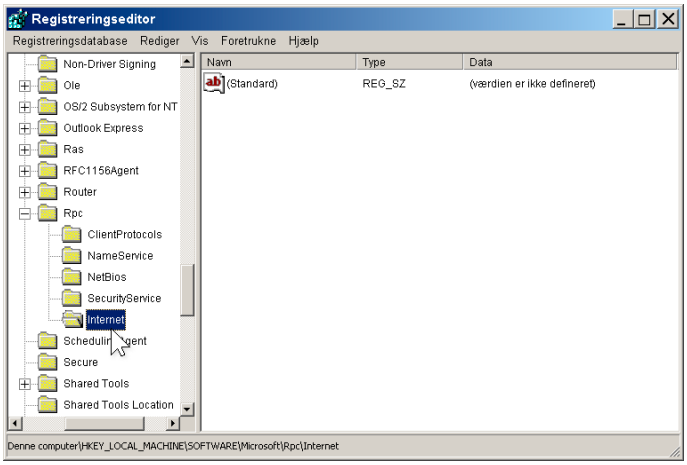
Find følgende nøgle: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc]. Når du har fundet den, højreklikker du på Rpc og vælger Ny > Nøgle (se billederne herude til højre). Den nye nøgle kaldes for internet (bemærk forskellen på store og små bogstaver).

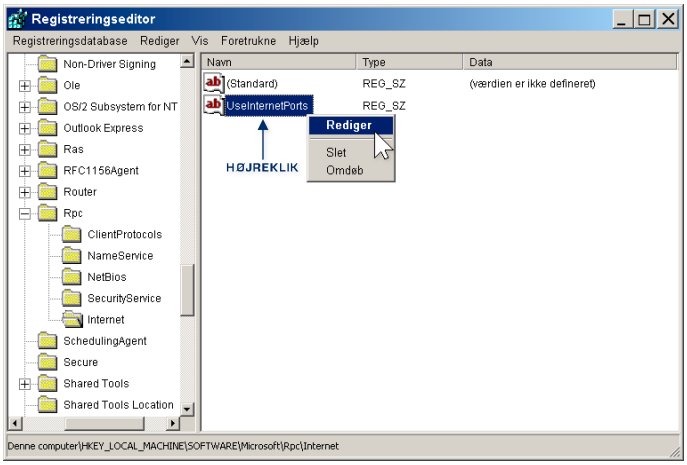
Når internet-nøglen er oprettet, sørger du for, at den er valgt, og klikker derefter ovre i højre side af vinduet, hvor du vælger Ny > Strengværdi. Den nye strengværdi kaldes for UseinternetPorts. Højreklik derefter på den nye strengværdi, vælg Rediger og skriv no i feltet Værdidata. Klik på OK og luk registreringseditoren.

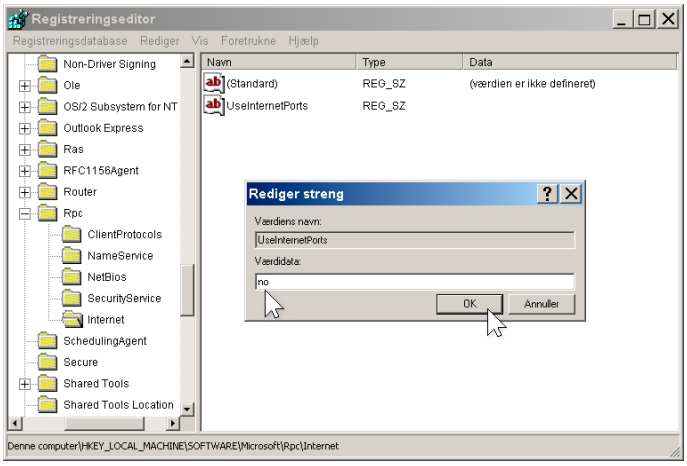
Jeg har endnu ikke oplevet problemer ved at have UseinternetPorts stillet til no for RPC inde i registreringsdatabasen. Det eneste lille minus er, at logbogen (Start > Kør: eventvwr.msc) vil komme med en advarsel (hændelses-id: 4358) og en fejl (hændelses-id: 4156) under kategorien Program, hvis man starter et program eller en funktion, som normalt ville få RPC til at åbne TCP:135. Hvis du oplever problemer med den indstilling, kan du blot slette internet-nøglen inde i [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc] og genstarte. Så er du tilbage til standardindstillingen.

Netkablet kobles til netkortet og computeren kan nu få lov til at komme på nettet. Det første man bør gøre er at besøge Windows Update og hente diverse sikkerhedsopdateringer og fejlrettelser og dette kan nu gøres i fred og ro uden at blive inficeret med diverse blaster-varianter, spammet med Messenger-spam osv. Det er en god idé at besøge Windows Update-siden ofte, for der bliver jævnligt udsendt sikkerhedsopdateringer.

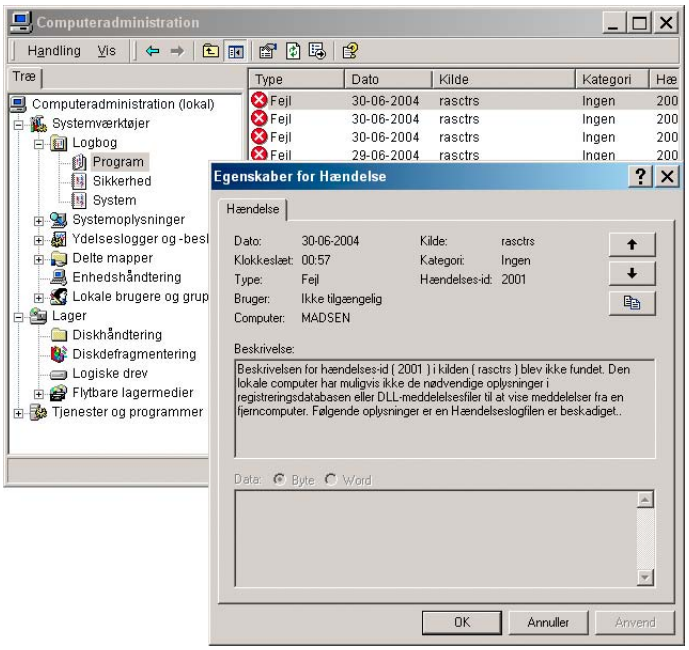




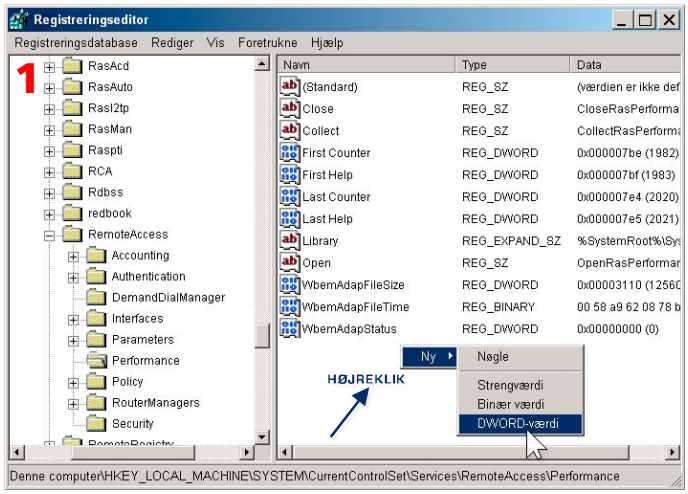


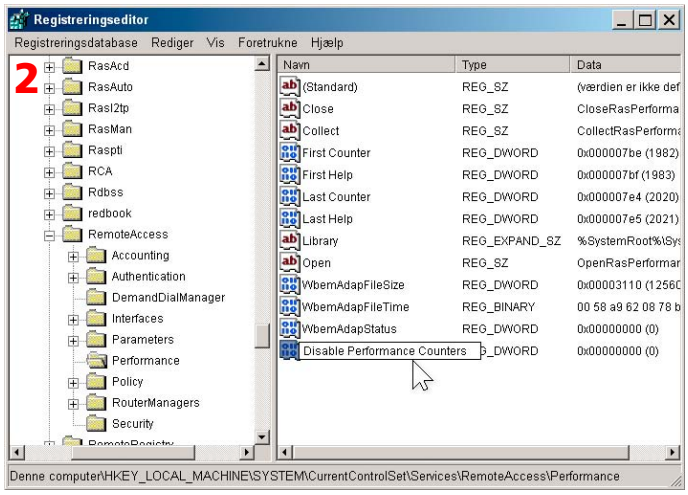


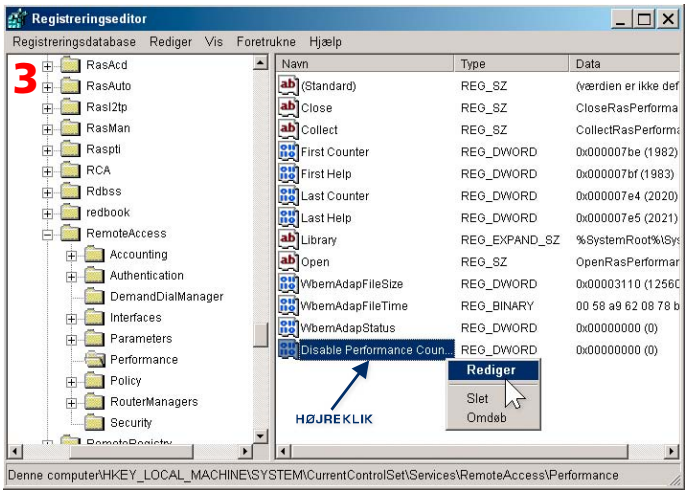
Hvis du har valgt at slå tjenesten Remote Access Connection Manager fra, som beskrevet på side 2, vil du muligvis opleve, at logbogen (Start > Kør: eventvwr.msc) bliver fyldt op med fejl i kilden rasctrs under punktet Program, som vist herude til højre. Fejlen opstår fordi Win2000 er udstyret med nogle såkaldte Performance Counters, som hele tiden står og måler hastigheden på mange forskellige ting og heriblandt Remote Access, men fordi vi har koblet Remote Access Connection Manager fra, kan rasctrs ikke længere måle hastigheden og det resulterer så i en fejl. Man kan vælge at ignorere fejlmeddelelsen i logbogen, eller man kan vælge at slå Performance Counteren for Remote Access fra, hvilket jeg vælger at gøre.

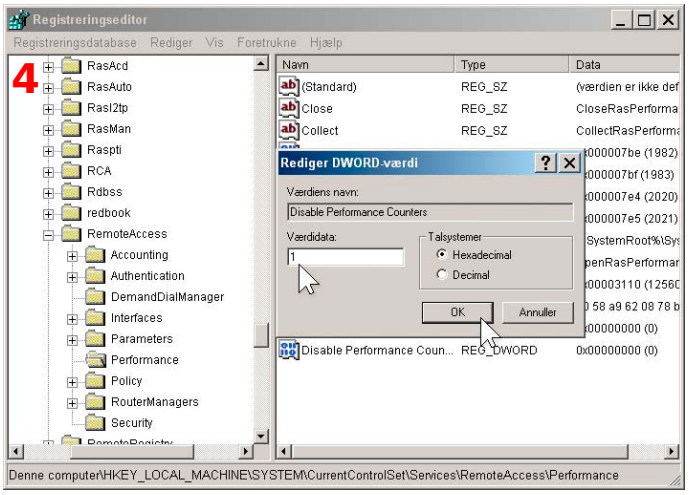


Start > Kør: regedit åbner som bekendt registreringseditoren, hvor man klikker sig frem til nøglen [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Performance]. Når man er inde i den nøgle, højreklikker man ovre i højre side og vælger punktet Ny > DWORD-værdi. Den ny værdi kaldes Disable Performance Counters. Når den er oprettet, højreklikker man på værdien og vælger Rediger, hvorefter man skriver 1 i feltet Værdidata, klikker på OK og lukker registreringseditoren.









Tak til brugerne af gruppen dk.edb.sikkerhed for hjælpen til indholdet af dette dokument.