Deaktivering af tjenester i Windows XP (første udgave og SP1)

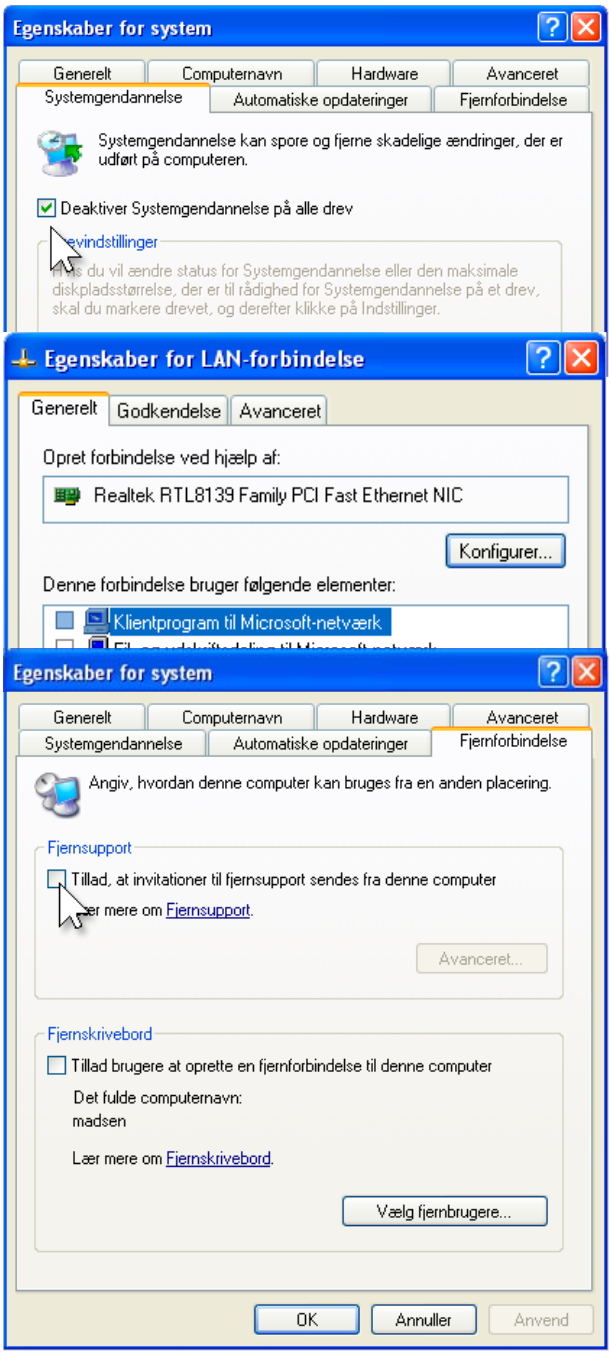
En standardinstallation af WinXP (Home og Pro) har flere netværkstjenester kørende, som desværre kan udnyttes af computerorme og andet snavs, som kan gøre livet surt for brugeren. Denne artikel er en kort gennemgang af de tjenester, man med fordel kan slå fra, for at sikre sin computer lidt bedre, inden 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.

WinXP 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.

Det første jeg plejer at gøre, på en frisk installeret WinXP, er at slukke for Systemgendannelse, Automatiske opdateringer(*), Fjernforbindelse og Fejlrapportering. Systemgendannelse er dog en god ting, da man har mulighed for at gå tilbage til et tidligere gemt gendannelsespunkt, hvis et eller andet går galt, men da jeg har valgt at investere i Drive Image fra Symantec, har jeg allerede lavet et image af installationen med Drive Image og har derfor ikke noget at bruge Systemgendannelse til. Om du vælger at slå funktionen fra eller ej er op til dig selv.

Systemgendannelse, Automatiske opdateringer og Fjernforbindelse findes inde i Kontrolpanel > System, som vist herude til højre. Under fanebladet Systemgendannelse er der sat et flueben i feltet „Deaktiver Systemgendannelse på alle drev". Under fanebladet Automatisk opdateringer er fluebenet „Hold computeren opdateret..." fjernet og under fanebladet Fjernforbindelse er fluebenet i „Tillad, at invitationer til fjernsupport sendes fra denne computer" også fjernet. Når det er gjort, går jeg i gang med at slukke for diverse netværkstjenester.



(*) Dermed ikke sagt, at Automatiske opdateringer altid bør kobles fra. Jeg foretrækker blot at opdatere manuelt ved at besøge Windows Update-siden engang imellem.

Ved at starte en kommandoprompt og starte: netstat -an, kan man hurtigt få et overblik over, hvilke porte WinXP 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	*0.0.0.0:5000*	*0.0.0.0:0*	*LISTENING*
UDP	*0.0.0.0:135*	**:**	
UDP	*0.0.0.0:445*	**:**	
UDP	*0.0.0.0:500*	**:**	
UDP	*0.0.0.0:1026*	**:**	
UDP	*127.0.0.1:123*	**:**	
UDP	*127.0.0.1:1900*	**:**	

Start > Kør: services.msc starter Tjenester, som vist herude til højre. Find tjenesten IPSEC Policy Agent på listen, højreklik på den og vælg Egenskaber. Klik derefter på Stop-knappen og stil den til Deaktiveret i feltet Starttype. Klik på OK for at lukke vinduet. Den ændring lukker for UDP:500.

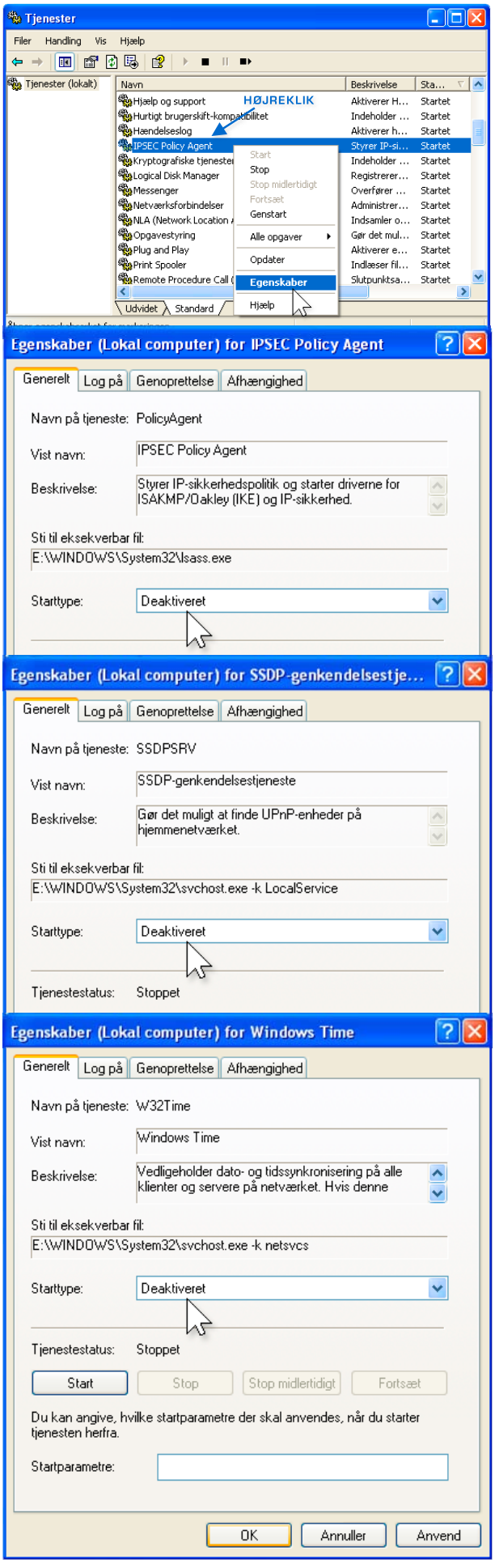
Find SSDP-genkendelsestjenesten og gør det samme ved den (Stop, Deaktiver og OK). Det lukker for TCP:5000 og UDP:1900. En efterfølgende netstat -an i kommandoprompten, vil derfor resultere i følgende:

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*
TCP	*0.0.0.0:1025*	*0.0.0.0:0*	*LISTENING*
UDP	*0.0.0.0:135*	**:**	
UDP	*0.0.0.0:445*	**:**	
UDP	*0.0.0.0:1026*	**:**	
UDP	*127.0.0.1:123*	**:**	

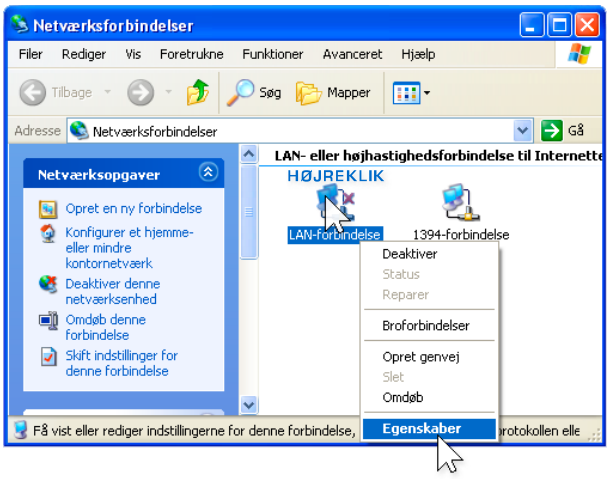
Tjenesten Windows Time (UDP:123), sørger for at holde uret opdateret ved jævnligt at kontakte en tidsserver på internettet. Den funktion har jeg ikke brug for, så den deaktiveres ved først at dobbeltklikke på uret i proceslinjen og under fanebladet Internettid, fjernes fluebenet i „Synkroniser automatisk med en tidsserver på internettet". Derefter stoppes og deaktiveres tjenesten Windows Time inde i Tjenester (Start > Kør: services.msc).



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.

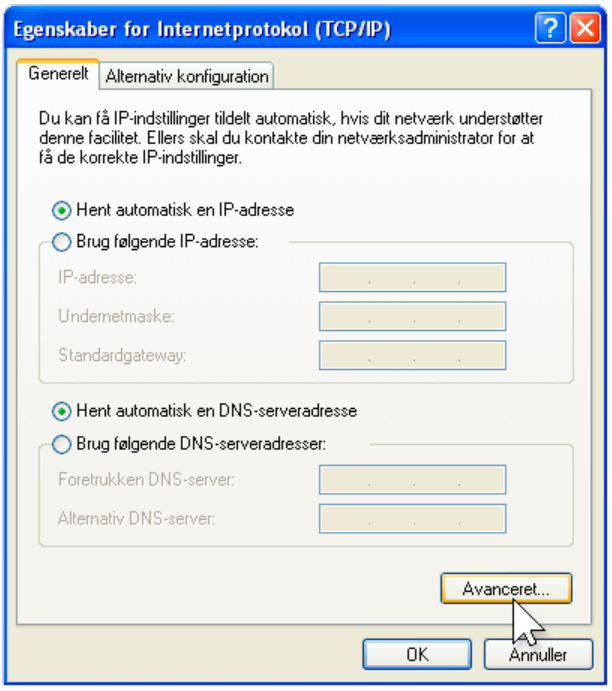
Ønsker man et LAN, kræver det, at man lader nogle tjenester køre, som rummer en vis risiko. Hvis man imidlertid benytter en router med NAT (det har de fleste) og en firewall (det har mange), så kan man godt have disse tjenester åbne, men en computer sat op på den måde, bør ikke sluttes direkte til internettet. 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 > Kontrolpanel > Netværks- og Internetforbindelser > Netværksforbindelser (eller blot Start > Indstillinger > Netværksforbindelser, hvis du kører med den klassiske startmenu), hvor du højreklikker på netværksforbindelsen og vælger Egenskaber.

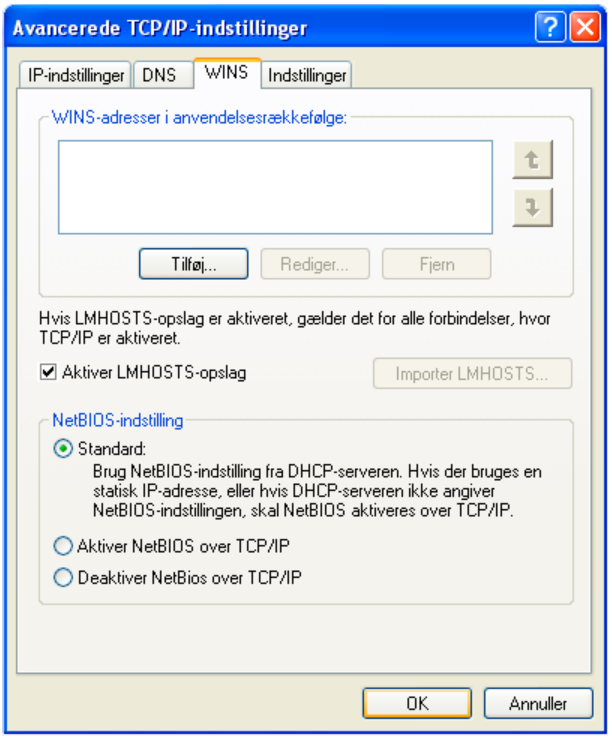


Under fanebladet Generelt, finder du indstillingerne.

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

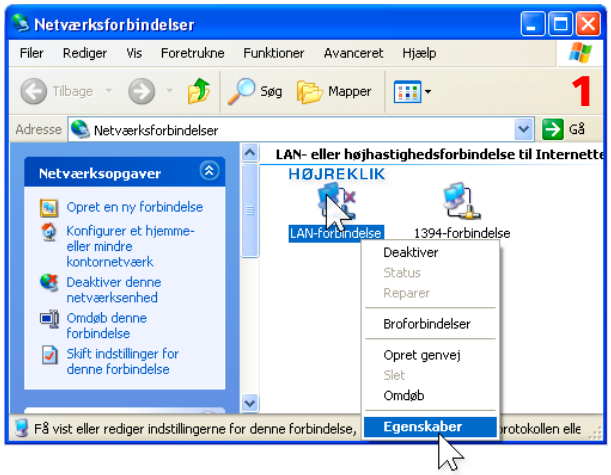


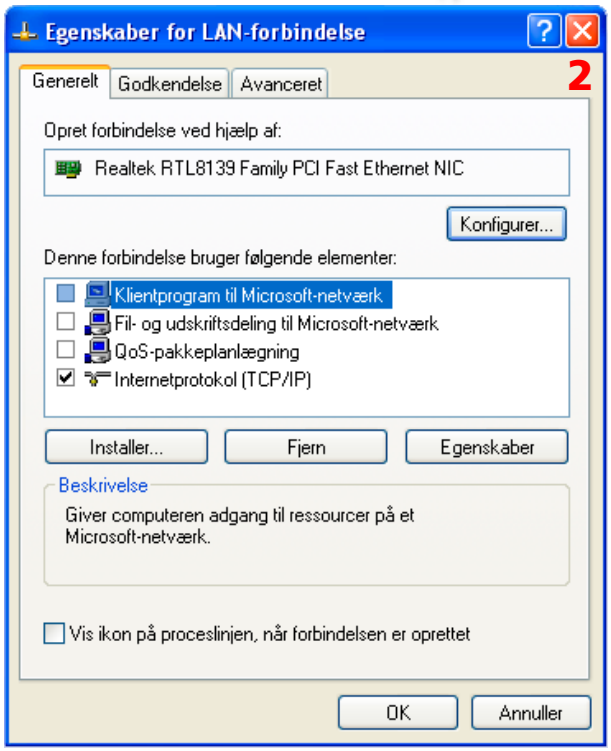
Ved at klikke på Avanceret og derefter WINS-fanebladet, kommer man ind til følgende vindue, hvor NetBIOS skal være koblet til. Derudover skal tjenesten TCP/IP NetBIOS Helper også køre, hvilket den også gør som standard.

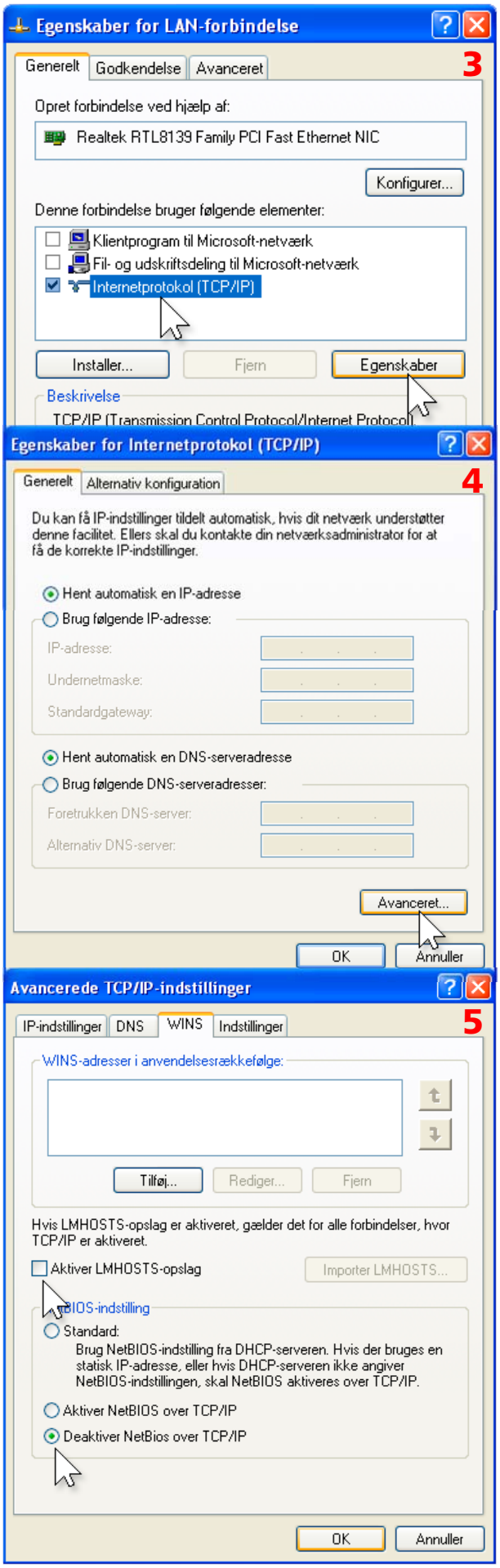


Hvis du ikke har behov for et LAN, kan Klientprogram til Microsoft-netværk, Fil- og udskriftsdeling til Microsoft-netværk samt NetBIOS over TCP/IP kobles fra, for de er ikke nødvendige for at få en enkeltstående computer på internettet. Disse kobles fra inde i Start > Kontrolpanel > Netværks- og Internetforbindelser > Netværksforbindelser (eller blot Start > Indstillinger > Netværksforbindelser, hvis du kører med den klassiske startmenu). Højreklik på netværksforbindelsen og vælg Egenskaber.

Fluebenet i Klientprogram til Microsoft-netværk og Fil- og udskriftsdeling til Microsoft-netværk fjernes og QoS-pakkeplanlægning afinstalleres evt. også, da de færreste har programmer installeret, som understøtter den funktion. 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.

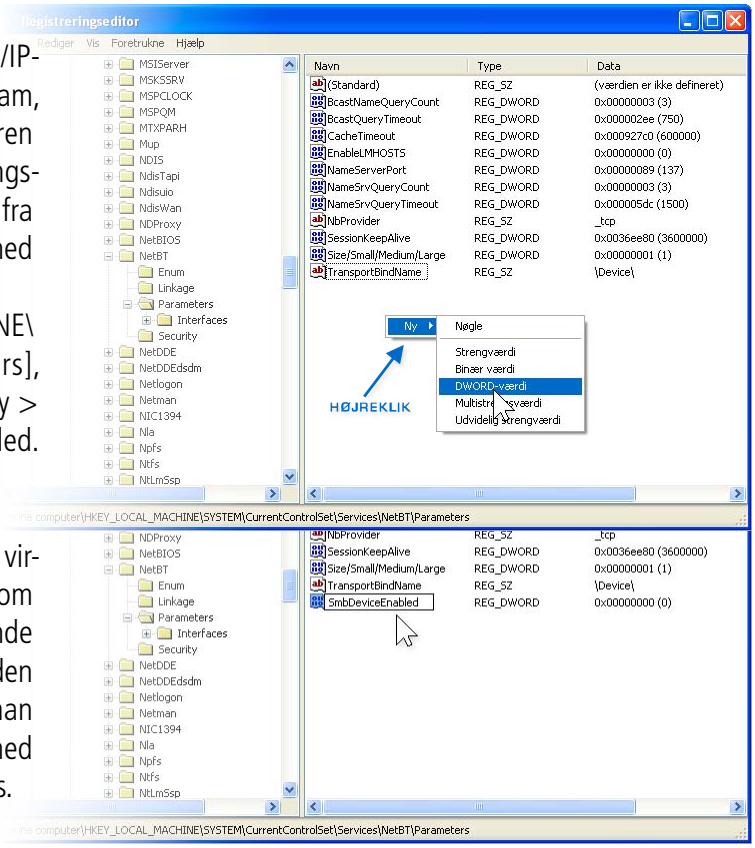






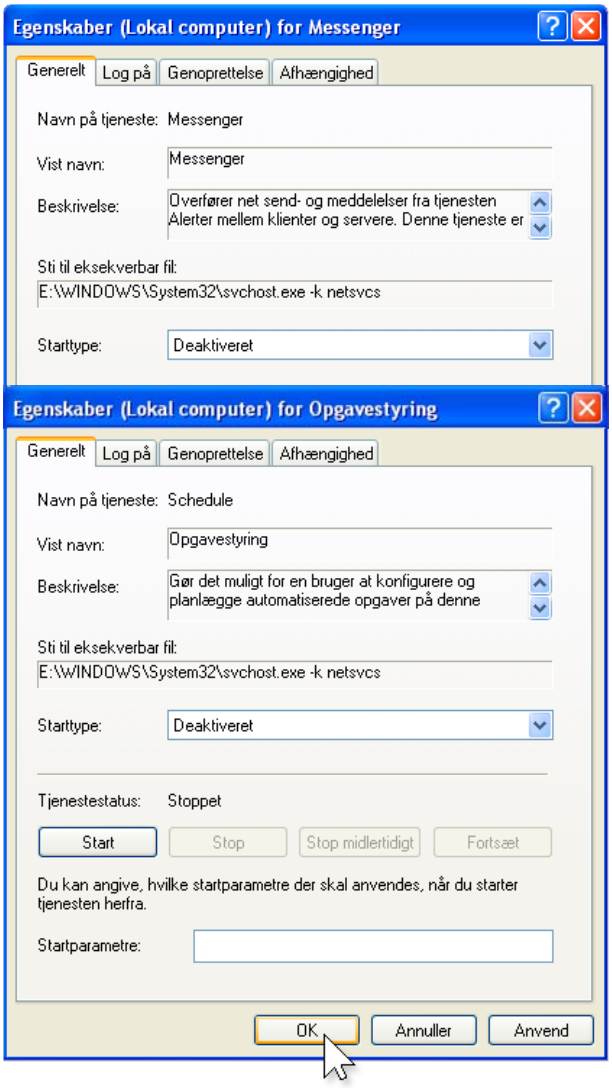
TCP:445 holdes åben til SMB/CIFS-protokollen.
Man kan vælge helt at frakoble NetBIOS over TCP/IP-driveren (NetBT), men da tjenesten DHCP-klientprogram, som jeg har brug for, er afhængig af, at NetBT-driveren kører, vælger jeg i stedet at tilføje en værdi til registrerings-databasen, som slår SMB-transporten 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 og luk så regedit.



Messenger-tjenesten er afhængig af NetBIOS, så den virker ikke efter NetBIOS over TCP/IP er koblet fra, hvilket som regel er en fordel, da det er blevet ret populært at sende spam til Messenger-tjenesten. Selvom den ikke virker uden NetBIOS, holder den dog stadig nogle porte åben, så man kan med fordel deaktivere Messenger-tjenesten helt (med services.msc), så den ikke starter sammen med Windows.

Det samme er tilfældet med tjenesten Opgavestyring / Task Scheduler (TCP:1025 i dette eksempel). Den tjeneste har jeg valgt at deaktivere, da ingen af mine programmer bruger den. Hvis man oplever problemer ved at have den deaktiveret, kan man jo altid stille den til Automatisk igen. (Visse tredjepartsprogrammer, som f.eks. antivirusprogrammers automatiske opdateringsfunktion, kan være afhængig af, at Opgavestyring kører).



Når Messenger og Opgavestyring er deakiveret genstartes computeren og efter genstarten, vil netstat -an i en kommandoprompt vise dette:

c:\>netstat -an

Aktive forbindelser

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

Hvis du oplever, at der holdes en TCP-port mere åben udover TCP:135 (f.eks. TCP:1025), så kan det være tjenesten Remote Access Connection Manager. Hvis det er tilfældet, kan du deaktivere den tjeneste, men 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 Netværksforbindelser (de forsvinder 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 Remote Access Connection Manager, for en sådan netværksforbindelse forsvinder ikke ved at deaktivere den tjeneste.

TCP:135 holdes aktiv af RPC (Remote Procedure Call) og RPC kan ikke kobles fra på WinXP, 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 computerorme forsøger at snige sig ind af (blaster-ormen f.eks.) Heldigvis er der mulighed for at konfigurere WinXP, så RPC får lov at køre, men uden at TCP:135 åbnes og det kan bla. gøres med værktøjet Komponenttjenester.

Start > Kør: dcomcnfg skulle gerne resultere i, at vinduet Komponenttjenester kommer frem på skærmen. I det vindue højreklikkes der på Denne computer under punktet Komponenttjenester > Computere og punktet Egenskaber vælges.

Under fanebladet Standardegenskaber fjernes fluebenet ud for „Aktiver DCOM på denne computer" og under fanebladet Standardprotokoller fjernes protokollen Forbindelsesorienteret TCP/IP.

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

Alerter
DNS-klient
(DTC) Distributed Transaction Coordinator
Tjenesten TCP/IP NetBIOS Helper (hvis NetBIOS over TCP/IP ikke køres. Se evt. side 3 & 4).
Remote Registry
Serienummer for bærbart medie
Automatiske opdateringer (fordi jeg foretrækker at opdatere via Windows Update, som skrevet nederst på side 1).

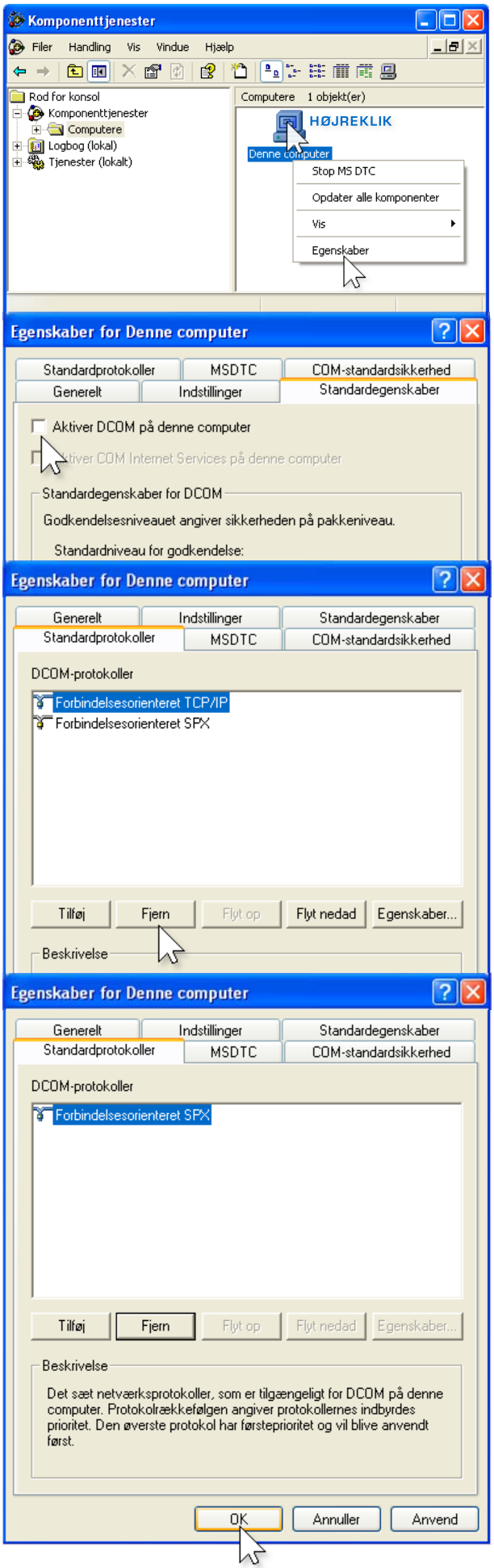
Efter en genstart, vil netstat -an i kommandoprompten vise dette:

c:\>netstat -an

Aktive forbindelser

Proto Lokal adresse Fjernadresse Status

Du skal 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 øveste screenshot 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.

Til dem som ønsker at gøre WinXP endnu sikrere, kan følgende PDF anbefales (den er på engelsk):
http://www.giac.org/practical/GSEC/Zach_Groves_GSEC.pdf
På side 16 i ovenstående PDF er der omtalt to VBS-filer (Tcpip_sec.vbs og Winsock.vbs), som kan hjælpe med til at styrke TCP/IP og winsock. Hvad disse to filer ændrer i registreringsdatabasen er nævnt på side 16 i ovenstående PDF og i Microsofts "Treats and Countermeasures Guide: Security Settings in Windows Server 2003 and Windows XP". De to VBS-filer kan hentes på følgende adresse:
http://home18.inet.tele.dk/madsen/winxp/tcpip_winsock.zip

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