Basal TCP/IP fejlfinding

Dette notat beskriver en række enkle metoder til fejlfinding på TCP/IP problemer. Metoderne er baseret på kommandoer, som er en fast bestanddel af Windows. Notatet er opbygget af følgende afsnit:

- Begreber; En kort gennemgang af begreber vedr. TCP/IP – såsom IP adresser, subnet etc. Såfremt du allerede har styr på de mest elementære IP begreber, kan du springe dette afsnit over.
- Kommandoer; Her beskrives de kommandoer i Windows, som kan bruges til fejlsøgning på TCP/IP problemer.
- Løsning af TCP/IP problemer (checkliste); Her er der beskrevet en række fejlsituationer og vist en metode (checkliste) til at løse disse.

1. Begreber

Det følgende er en kort gennemgang af nogle basale begreber knyttet til TCP/IP. Begreberne er simplificeret en smule for at gøre dem lettere forståelige.

1.1 IP adresse

I et TCP/IP baseret net har alle pc'er (og andre enheder) en entydig adresse, der gør det muligt at kommunikere med disse. En IP adresse ser normalt således ud ”86.11.252.100”, hvilket jo bare ligner en tilfældig samling af tal, men faktisk er der en nøje opbygning af denne adresse. Adressen er delt i to dele, hvoraf den ene siger, hvilket net pc'en er tilsluttet, mens den anden del af adressen, angiver hvilken pc i det givne net der er tale om. Dette kan sammenlignes lidt med et telefonnummer, hvor de første cifre afgør hvilken central der er tale om, mens de sidste cifre peger på den konkrete abonnent. Hvor stor en del af IP adressen, den indeholder adressen på nettet, afgøres af en såkaldt subnetmask.

1.2 Subnetmask

Subnetmasken viser hvor stor en del af en IP adresse, der angiver nettets adresse, og hvor stor en del der anvendes til at angive den enkelte pc's adresse indenfor nettet - subnetmasken kan f.eks. se således ud ”255.255.240.0”. Hvis subnetmasken oversættes til binære værdier, vil 1-bittene være den del af IP adressen, som indeholder nettet adresse, mens 0-bittene afgør hvor stor en del af adressen, der peger på den individuelle pc. Et net skal i denne forbindelse forstås som et lokalnet der ikke er forbundet via WAN og routere (se senere).

1.3 DHCP (Dynamic Host Configuration Protocol)

For at undgå manuelt at skulle tildele hver eneste pc en IP adresse, kan man anvende en DHCP server, som "låner" en pc en IP adresse, hver gang pc'en bootes. DHCP har dels den fordel, at man slipper for manuelt at skulle holde styr på hvem der har hvilken IP adresse, dels den fordel at hvis man flytter sin pc til et andet net vil man via DHCP få en adresse i det net hvor pc er tilsluttet. Ulempen ved DHCP er at det kan være svært at afgøre hvem der f.eks. i går kl. 15 havde en given IP adresse (et problem der er aktuel ved f.eks. sikkerhedslogning).

1.4 Host navn

Da det kan være svært at huske IP adresse, findes der et system til at oversætte disse til logiske navne. Et sådant logisk navn kaldes for et "host-navn" - også selv om der er tale om navnet på en pc eller en printer. For at oversætte mellem host-navne og IP adresser, skal der bruges en slags telefonbog. Man kan vælge at have sin egen telefonbog (kaldet en host-fil), som er en ganske almindelig tekst fil med navnet "hosts", eller man kan lade en server styre denne telefonbog. En server der oversætter mellem IP adresser og host-navne kaldes en Domain Name Server (DNS) - det er f.eks. denne der oversætter www.vm-online.dk til en IP adresse.

1.5 WINS

I et Microsoft baseret netværk anvendes ofte et system der hedder WINS, som udfører en funktion der minder om DNS, idet WINS oversætter mellem IP adresser og NetBios navne (et NetBios navn minder om et hostnavn, men er noget andet) - der er række tekniske forskelle, men disse ligger udenfor rammerne af denne korte vejledning.

1.6 Router/gateway

Ved at anvende IP adresser, får man lavet en række separate net (forskellige net adresser), og disse skal så på en eller anden måde bindes sammen, sådan at man f.eks. fra Aalborg kan kommunikere med en server i London. Dette gøres ved at anvende en router (i IP verdenen ofte kaldet "default gateway"), som har til opgave at sende trafikken rundt mellem IP subnet i hele verden. Routeren gør dette ud fra net-delen af IP adressen, som jo netop angiver hvilket net, der er tale om - en router i USA skal derfor ikke kende adressen på din pc, men den skal kende adressen på dit IP net, som set fra USA er et stort subnet.

1.7 Firewall

En firewall er en særlig type router, der laver en række sikkerhedsfunktioner - f.eks. kan man i en firewall blokere brugere i et subnet fra at få adgang til serverer i et andet subnet.

1.8 NAT adresse

I forbindelse med firewall's tales der ofte om NAT adresser (Network Address Translation), som er en fælles adresse, som anvendes af alle pc'er – eksempelvis har alle pc'er hos et firma, som er på Internettet, samme IP adresse på Internettet, mens de har entydige IP adresser internt i firmaet (firewall'en konverterer mellem de pågældende adresser). Årsagen til at der anvendes NAT, er at dette gør det muligt at anvende de samme IP adresser i flere virksomheder, hvis pc'er (IP adresser) ikke har behov for at kommunikere med hinanden – man kan dermed spare på globalt entydige IP adresser som er en mangelvare. Anvendelse af NAT har endvidere en sikkerhedsmæssig fordel, idet det er langt sværere for en hacker at trænge gennem et NAT baseret net, end det er at hacke en pc som direkte på Internettet med egen IP adresse – i NAT miljøet skal hackere "nare" firewall'en (som er beregnet til at holde hackere ude) for at kommer gennem nettet, mens der i miljøer uden NAT er direkte IP adgang til de enkelte pc'er, som typisk ikke er så godt beskyttede som en firewall.

1.9 MAC-adresse

Udover en IP adresse opererer lokalnet også med en MAC-adresse. En MAC adresse er en entydig adresse på den lokalnet adapter, som sidder i pc'en, og denne er den samme uanset om man kører TCP/IP, SNA eller IPX. Alle LAN adaptere (kaldet NIC - Network Interface Card) er født med en global entydig MAC adresse, men denne kan ændres af brugeren.

2. Kommandoer

Her beskrives de kommandoer i Windows NT/2000/XP, som kan bruges til fejlsøgning på TCP/IP problemer.

2.1 IPCONFIG

Ipconfig viser en liste hvoraf der bl.a. fremgår følgende: IP adressen, subnetmasken, router (default gateway) adressen, DNS serveren, evt. DHCP og WINS servere. Hvis kommandoen kaldes uden parametre, vises kun de vigtigste informationer, men man kan "tvinge" kommandoen til at vise alt via parameteren "/all".

Kommandoen bruges bl.a. til at se hvilken IP adresse man har – hvis man da har en. Hvis pc'en lige er blevet flyttet, kan kommandoen bruges til at checke om man nu har en adresse som passer i det subnet, som pc'en rent fysisk sidder i. Hvis IPCONFIG svarer "ERROR" (eller viser tomme felter, så betyder det at TCP/IP ikke blev initialiseret korrekt). Ved fornyelse af DHCP adresser er det sikreste at anvende følgende to kommandoer "ipconfig /release" og "ipconfig /renew"

Eksempel: ipconfig /all

2.2 PING

Ping er en kommando der sender en dataframe til en given modtager, som så svarer med en tilsvarende frame. Kommandoen viser hvor lang tid det tager at få et svar retur. Ping kaldes med enten en IP adresse eller et host-navn som parameter. Såfremt ping kaldes med et host navn vil systemet prøve at oversætte dette via host-tabellen og via DNS serveren. Herudover vil man i Microsoft miljøer opleve at ping ligeledes søger efter navnet i WINS samt via NetBios broadcast. Da et NetBios navn kan være oprettet på flere pc'er, kan man komme ud for, at svaret kan komme fra forskellige pc'er, hvis kommandoen gentages.

Ping kan bl.a. kaldes med følgende parameteren "ping –t ", som får ping kommandoen til at forsætte med at sende pakker, indtil der tastes <break> - normalt sendes der kun fire pakker.

I et TokenRing net (og enkelte store router baserede net) vil man ofte komme ud for, at den første pakke som ping kommandoen udsender ikke bliver besvaret, hvilket ikke er en fejl, men skyldes den måde som Microsoft har implementeret ping kommandoen på.

Ved at pinge 127.0.0.1 kan ping anvendes til at teste om TCP/IP er installeret (og kører) korrekt, idet 127.0.0.1 er en såkaldt loop-back adresse, som besvares internt på pc'en. Så hvis man ikke kan pinge denne adresse, er der problemer på selve pc'en, og så er der ingen grund til at bruge tid på at undersøge nettet.

"Ping –a" anvendes såfremt man har en IP adresse og ønsker at få vist navnet (fra f.eks. DNS serveren) på den enhed der har den pågældende adresse. "Ping –a" tjener dermed samme formål som "nslookup" kommandoen på andre systemer.

Eksempel: ping -t 86.11.10.1

2.3 NSLOOKUP

NSLOOKUP anvendes til at oversætte mellem IP adresser og hostnavne.

Eksempel: nslookup 86.11.10.10

Eksempel-2: nslookup www.tfc.dk

2.4 ARP

ARP kommandoen bruges til at se hvilke IP adresser, der svarer til hvilke MAC-adresser. Man kan kun se MAC-adressen på enheder i samme net som en selv, da data der skal ud af nettet altid sendes til routeren. ARP kommandoen fungerer ved at aflæse en lille tabel i pc'en RAM, som "slettes" efter nogle få minutter, så før man bruger arp kommandoen bør man lave en ping af den enhed, hvis MAC-adresse man ønsker at kende.

"ARP –a" viser alle elementer i arp-tabellen.

"ARP –d ip-adresse" sletter det pågældende element fra ARP tabellen.

Eksempler: arp –a

Eksempel-2: arp –d 86.11.10.254

2.5 TRACERT

Tracert bruges til at vise hvilke routerer der passeres mellem den pc der udsender pingen og den enhed der pinges. Tracert kaldes med enten IP adresse eller host-navn som parameter. Såfremt forbindelsen til enhed, der ønskes fundet, går via firewalls, kan man risikere at "tracert" ikke virker.

Eksempel: tracert www.tdc.dk

2.6 Netstat

Netstat kan anvendes til at vise protokolstatistikker og oplysninger om TCP/IP tilslutninger (TCP/IP porte etc.) Da Netstat er en rimelig "teknisk" kommando, og derfor ligger udenfor rammerne af denne vejledning, er den ikke detaljeret beskrevet her, men der skal dog nævnes følgende om kommandoen:

- Netstat –e: viser en statistik på Ethernet laget
- NetStat –s: viser statisikoplysninger vedr. TCP, UDP og IP. Vær opmærksom på at de oplysninger som Netstat viser vedr. "header" og "address" fejl kan være fejlagtige, idet programmet, på net hvor der er flere subnet som kommunikerer på det samme fysiske netsegment, optæller en række helt legale hændelser som fejl (fejlen er beskrevet i bl.a. Microsoft PSS Q155758).

De oplysninger som Netstat viser vedr. hvilke TCP/IP porte som er aktive, skal tages med et vist forbehold, da de ikke altid er fyldestgørende – der kan være aktive TCP/IP porte, som ikke vises af Netstat.

2.7 NbtStat

NbtStat kan anvendes til at vise en række oplysninger vedr. NetBios. Da brugen af denne kommando ligger udenfor denne vejlednings rammer, henvises eventuelle interesserede til div. information desangående fra Microsoft (prøv f.eks. Internettet og Technet).

Eksempel: ”nbtstat –A 192.168.1.2”
Eksempel-2: ”nbtstat –a TESTPC”

3. Løsning af TCP/IP problemer (checkliste)

Her er der beskrevet en generel metode til at løse en almindelige TCP/IP fejl af typen "TCP/IP virker ikke" eller "der er ikke forbindelse til enhed ???".

1. Før du går i gang med at checke en masse tekniske oplysninger, så check lige om kablet er sat i et stik, der er kablet op med en kørende switch/hub, som er på nettet.
2. Check om der er en kørende IP stak på pc'en. Dette kan f.eks. gøres ved at se om pc'en har en IP adresse (Ipconfig /all og winipcfg i Windows 95/98 miljøer). Hvis IP adressen er af 169.x.x.x typen, har pc'en ikke kunne få en IP adresse fra DHCP serveren, hvilken enten skyldes at der ikke er netværksforbindelse til DHCP serveren, eller at denne ikke er konfigureret til at uddele IP adresser i det IP subnet du sidder i. Hvis du ikke har fået en DHCP adresse, kan du forsøge at tildele pc'en en fast konfigureret IP adresse – her skal du være varsom med ikke at vælge en IP adresse, der anvendes af en anden enhed (normalt checker operativsystemet dette, men vær alligevel varsom).

3. Kontroller om IP oplysninger nu også er som de skal være – er eksempelvis IP adresse, subnetmask og adressen på default gateway korrekte (hvis ikke findes der sikkert en uautoriseret DHCP server på nettet). Er der problemer med at IP adressen ikke er valid i et DHCP baseret net, så prøv at frigøre denne (ipconfig /rerelase) og skaf en ny IP adresse (ipconfig /renew) – det er vigtigt at frigive IP adressen, før der skaffes en ny, da pc'en ellers vil anvende en del af de "gamle" oplysninger.
4. Ping adressen 127.0.0.1. Dette vil vise om maskinen kan se sig selv og om TCP/IP er loaded korrekt.
5. Ping pc'ens egen IP adresse. Hvis dette fejler, check da TCP/IP opsætningen. Hvis kommandoen ping 127.0.0.1 virker - men man kan ikke pinge andre enheder i netværket, så ligger problemet oftest i forbindelsen (kablet, HUB/Switch). Husk at adressen 127.0.0.1 er en "loopback" adressen på netkortet, hvilket betyder, at netkortet og opsætning i maskinen virker.
6. Hvis det lykkedes at pinge maskinens IP adresse, ping da Default Gateway som det næste. Hvis dette fejler, check så lige pc'ens konfiguration igen, og check om routeren virker (f.eks. fra en anden pc).
7. Prøv at slukke pc'en og pinge dens (formodede) IP adresse fra en anden pc. Hvis der svares skyldes problemet at der er flere pc'er som har fået tildelt samme IP adresse.
8. Ping nu en IP adresse på en pc på den anden side af den lokale Router. Dette vil checke om WAN forbindelsen virker. Det er naturligvis et krav at den enhed der pinges kører !. Hvis dette kikser ligger problemet omkring routningen. Såfremt pc'en lige er blevet flyttet (f.eks. til en anden netværks segment), kan man komme ud for, at der går en lille time før routeren "accepterer" dette, og lader trafik fra pc'en passere.
9. Ping DNS serveren. Hvis denne ikke svarer er denne enten nede eller adressen er konfigureret forkert – prøv udelukkende at anvende IP adresser frem for host-navne.
10. Prøv nu at pinge via nogle navne frem for via IP adresser, for at checke at DNS og Wins kører – og for at checke at de navne du tror du skal anvendes, nu også er de rigtige. Hvis dette ikke virker er der problemer med oversættelsen mellem IP adressen og host navnene – typiske fejlårsager er forkert host-navn, forkert opsat adresse på DNS serveren eller fejl i host-filen.
11. Såfremt den pc du skal i forbindelse med kører NetBios (gælder næsten alle Windows pc'er), kan du prøve om kommandoer "net use \\pc-navn\share" eller "net view \\pc-navn" virker – bemærk at svar om "uautoriseret adgang" faktisk viser at der er forbindelse, da dette afslører at dit brugerid/kendeord er blevet valideret.
12. Lav en Tracert kommando mod den enhed du skal i forbindelse med. Du skulle nu kunne se hvor lang rundt i nettet du kommer før der opstår fejl.

Forhåbentligt skulle fejlen nu være løst - eller i hvert fald isoleret til et kendt problem.