

6105 Windows Server og datanett

Labøving 8b: Transportprotokoller i Windows (TCP og UDP)

Forkunnskaper og forutsetninger

Du bør se gjennom leksjon *8b Transportlaget TCP og UDP* før du gjør denne øvingen.

Introduksjon

Windows kommandoen **netstat** gir bl.a. en oversikt over åpne TCP- og UDP-porter (sockets) på maskinen din. En *åpen* port er i denne sammenhengen en (lokal) port som er åpnet av et program på maskinen.

Se oversikt over alle opsjoner til netstat- kommandoen i "Jon Kvisli: *Datakommunikasjon og maskinvare*, kapittel 3.4.6.

Øvingen er skrevet for å gjøre den på den virtuelle klientmaskinen din - innlogget med en bruker som har lokale administratorrettigheter, f.eks. **WORKSTATION\admin**.

Siden klientmaskinen bruker tjenermaskinen som DNS-tjener, må denne også være startet.

Du **kan** også gjøre øvingen på en fysisk maskin, men da vil du nok oppleve at maskinen vil ha ganske mange andre TCP/IP forbindelser som vises i resultatene fra **netstat** kommandoen. Det kan derfor være vanskelig å finne de forbindelsene som «hører til» oppgaven.

Oppgave a: Oversikt over TCP porter på tjenersiden

1. Åpne et kommandovindu og kjør kommandoen **netstat**
 - Hvor mange **TCP**-porter vises i listen? _____
 - Hvilke ulike tilstander (*State*) finnes i listen? _____
 - Hva betyr tilstanden **ESTABLISHED**? _____
2. Kjør kommandoen **netstat -n**
 - Hva gjør **-n** opsjonen? _____
3. Kjør kommandoen **netstat -a**
 - Hva gjør **-a** opsjonen? _____
4. Kjør kommandoen **netstat -anp TCP** og svar på følgende:
 - Hvor mange åpne **TCP** porter (sockets) finnes på maskinen din? _____
 - Hva betyr tilstanden **LISTENING**? _____
 - Finner du noen forbindelse med portnr 80 (:80) eller 443 (:443) i kolonnen *Foreign Adress*? _____
 - Hvilken *applikasjonsprotokoll* bruker portene 80 og 443 som standard? _____
5. Bruk kommandoen **nslookup** for å finne IP-adressen til **www.usn.no** _____

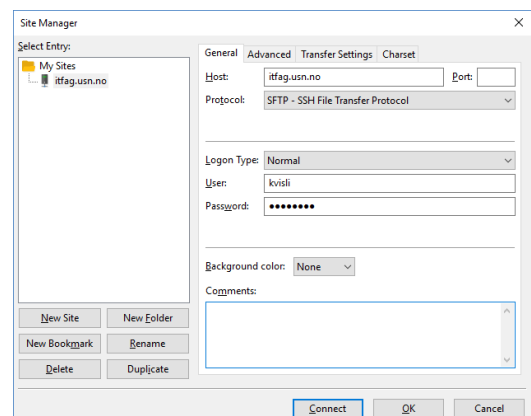
6. Start en webleser og slå opp websiden **www.usn.no**
7. Kjør kommandoen **netstat -anp TCP | findstr ":443"** og svar på følgende:
(**findstr** er "Windows-versjonen" av Linux kommandoen **grep**)
Finner du (flere) TCP forbindelser med port 80 i kolonnen *Foreign Adress* nå? _____
Hvorfor? _____
Finner du IP-adressen til **www.usn.no** under *Foreign adress* på noen forbindelser? ____
Hvilken status har disse forbindelsene? _____
8. Vent i 2 minutter og kjør **netstat -anp TCP | findstr ":443"** på nytt.
Finner du forbindelsene til **www.usn.no** nå? _____
Har de i så fall samme status som sist? _____
Hvorfor / Hvorfor ikke? _____
9. Bytt til nettleseren og refresh websiden (F5).
10. Kjør **netstat -anp TCP | findstr ":443"** på nytt.
Hvilken status har forbindelsene til **www.usn.no** nå? _____
11. Kjør kommandoen **netstat -anp UDP** og svar på følgende:
 - Hvor mange åpne **UDP** porter (sockets) finnes på maskinen din? _____
 - Hvorfor har ikke linjene med **UDP** data i kolumnene *Foreign Address* og *State*? _____

Oppgave b: Installere FileZilla på klientmaskin

I neste oppgave skal du sette opp en TCP basert klient/tjener forbindelse. Til dette trenger du et klientprogram for fil-overføring med FTP. Vi skal bruke **FileZilla FTP Client**, som du kanskje kjenner fra andre emner?



1. Last ned og installer siste versjon av **FileZilla Client** fra <https://filezilla-project.org/>
2. Når installasjonen er ferdig lukker du alle programmer på klientmaskinen unntatt kommandovinduet.
3. Start FileZilla, menyvalg **File** → **Site Manager** og knappen **New Site**.
4. Legg inn opplysninger for å logge deg på webtjeneren **itfag.usn.no** med ditt vanlige brukernavn/passord.
Bruk protokollen **SFTP SSH File Transfer Protocol**
Obs! Ikke logg inn ennå, men bruk knappen OK for å lagre innstillingene.
5. Hold FileZilla programmet oppe. Du trenger det i neste oppgave.



Oppgave c: TCP porter og forbindelser på klientsiden

1. Bruk kommandovinduet og kommandoen **nslookup** for å finne IP-adressen til maskinen **itfag.usn.no** _____
2. Kjør kommandoen **netstat -np TCP** som viser åpne TCP forbindelser.
Har noen av **TCP** forbindelser tilstanden ESTABLISHED? _____
Finner du noen forbindelser til IP-adressen for **itfag.usn.no**? _____
3. Bytt til FileZilla igjen og opprett en forbindelse (Connect) til **itfag.usn.no**
Obs! USN benytter nå to-faktor autentisering så du må godkjenne med appen Microsoft Authenticator.
Du får en sikkerhetsadvarsel første gang du kobler til, men det er ok. Klikk **Yes**
4. Kjør kommandoen **netstat -np TCP** på nytt.
5. Finn linjen som samsvarer med FileZilla forbindelsen til **itfag.usn.no** (se etter tjenerens IP-adresse i listen).
Svar på følgende:
Hvilken tilstand har TCP forbindelsen som brukes av FileZilla? _____
Hvilket *portnummer* har FileZilla forbindelsen på **tjenersiden**? _____
Hva er *socketadressen* til FileZilla forbindelsen på **tjenersiden**? _____
Hva er **lokalt** *portnummer* har denne forbindelsen på **klientsiden**? _____
Hva er *socketadressen* til FileZilla forbindelsen på **klientsiden**? _____
6. Bytt til FileZilla og bruk menyvalget **Server | Disconnect** for å **bryte** forbindelsen til **itfag.usn.no**.
7. Kjør **netstat -np TCP** på nytt
Er forbindelsen til itfag.usn.no er borte? _____
Hvis ikke: Hvilken tilstand (*State*) har forbindelsen? _____
8. Bytt til **FileZilla** og logg inn på **itfag.usn.no** på nytt med menyvalget **Server | Reconnect**
9. Kjør **netstat -np TCP** enda en gang til
Hva er **lokalt** portnummer har den nye (etablerte) forbindelsen? _____
Hvorfor er dette *forskjellig* fra **lokalt** portnr i pkt. 5. _____
Hvilket portnummer har FileZilla forbindelsen på **tjenersiden**? _____
Hvorfor er dette det *samme* som i pkt. 5. _____
10. Bytt til FileZilla, logg av forbindelsen til **itfag.usn.no**, og lukk alle programmer

Slutt på øvingen