Nätverksdiagnostik i kommandotolken

I denna laboration ska ni träna på att använda vanliga verktyg för undersökning/felsökning av nätverk i kommandotolken.

Antal: Enskilt

Material: En dator med operativsystemet Windows, fungerar även med de flesta Linuxdistributioner men det är inte säkert att riktigt alla verktyg finns med från början utan kanske måste installeras.

Tips: Vi kommer att titta på följande kommandon (verktyg):

- IPCONFIG
- ARP
- PING
- TRACERT
- HOSTNAME
- NETSTAT
- PATHPING
- NSLOOKUP
- ROUTE
- NETSH
- NET
- NBTSTAT
- GETMAC

Utförande:

1. Starta kommandotolken med administrativa rättigheter. Tryck på Windows-tangenten och skriv (sök) på ***cmd***. Högerklicka och välj ***kör som administratör*** alternativt så kan man CTRL+SHIFT-klicka programmet för att det ska köras som administratör (förutsatt att du har rättigheter till det såklart).
2. Kör kommandot **IPCONFIG**
3. Observera alla nätverksinterface som finns. Ange vilka nätverksinterface som är anslutna samt vilka IP-inställningar dessa nätverkskort har.

Namn på nätverkskort	**IP-inställningar**
	IP-nummer:
	Nätmask:
	Default Gateway:
	IP-nummer:
	Nätmask:
	Default Gateway:
	IP-nummer:
	Nätmask:
	Default Gateway:

4. För att få mer information om ett kommando (i Windows) så kan man använda växeln **/?** efter ett kommando. Kör kommandot **IPCONFIG /?** och observera vilka olika växlar dom finns till kommandot.
5. Vilken växel till kommandot ***ipconfig*** rensar all lagrad DNS-information i DNS cachen?

   _____

   _____

   _____

6. Kör kommandot **IPCONFIG /ALL** och observera att ni nu för betydligt mer information.

7. Vilken ***MAC-adress*** har ditt trådlösa nätverkskort?

8. Kör kommandot **ARP –A** och notera resultatet. Du får nu en utskrift av din dators ARP-tabell. Ange MAC-adressen till default gateway, alltså nätverkets primära router (för det trådlösa nätverket).

9. Fråga en kompis vilken IP-adress denna har på skolans nätverk (måste vara ett IP-nummer i samma serie som ditt annars är något fel..). Kontrollera att du inte har någon information om detta IP-nummer i din ARP-tabell.
10. Prova att pinga din kompis IP-adress med kommandot **PING X.X.X.X** (där x:en är IP-numret). Kolla sedan din ARP-tabell och skriv ner din kompis MAC-adress. (OBS detta fungerar även om din kompis dator ej svarar på ping. Alltså kan man på detta sett se om datorn är igång ändå).

11. Använd hjälpväxeln (se uppgift 4) till kommandot **PING** och ange vilken växel som används för att pinga en adress kontinuerligt tills man avbryter det hela. Ange även vilken tangentbordskombination som används för att avbryta ett kommando som körs (står i hjälpen om denna växel – Tips ni behöver inte leta så långt).

12. Prova att pinga din default gateway adress med växeln (från förra uppgiften). Att kontinuerligt pinga en adress kallas ibland för en ping-snurra och kan vara bra vid felsökning i vissa fall. Avbryt kommandot när ni testat klart.
13. Kör kommandot **HOSTNAME** och notera din dators namn

14. Prova att pinga ditt datornman med kommandot **PING DATORNAMN**. Observera att det sker en namnöversättning. Har man IPv6 aktiverat vilket är standard sedan Windows Vista så får du svar av din Link-local adress (IPv6 tack vare LLMNR).
15. För att tvinga användandet av enbart IPv4 kan man använda växeln **-4.** Prova kommandot **PING -4 DATORNAMN** och notera att datornamnet översätt till IPv4-adress (via NetBIOS broadcast).
16. Med kommandot **TRACERT** kan man spåra den ”väg” som ett paket tar genom att lista alla router-hopp tillsammans med fördröjningar. Prova kommandot **TRACERT bahnhof.se** för att se alla router-hopp mellan din dator och bahnhofs webbserver.
17. Ange skolans internetleverantörs (bahnhofs) router som ansluter skolans router med bahnhofs nät (det är adressen efter default gateway).

18. Prova kommandot **PATHPING bahnhof.se** och notera resultatet. Detta tar drygt 3 minuter. Pathping fungerar som tracert men ger ett mer noggrant resultat.
19. Vad anger procenttalen man får ut av kommandot pathping?

20. Kommandot **NETSTAT** används för att lista aktiva TCP-anslutningar. Prova kommandot **NETSTAT –a** för att lista alla TCP-anslutningar. I kolumnen *state* ser man info om anslutningarna. ***LISTENING*** innebär att din dator lyssnar efter inkommande anslutningar.
21. Kolla upp port 445. Lyssnar din dator på denna port? Vad används den till (använd google/wikipedia).
22. Prova kommandot **GETMAC.** Vad gör kommandot?
23. Kommandot **NSLOOKUP** används för felsökning av DNS. Prova kommandot **NSLOOKUP** ni märker att prompten ändras (programmet körs nu) och DNS-servern som används listas. Skriv kommandot **HELP** så visas alla alternativ som finns.
24. För att göra ett namnuppslag så skriver man bara in domänadressen man vill undersöka. Prova att skriva in adressen ***wiki.ntilund.se*** vilket IP-nummer har denna adress?
25. Kan man lite om DNS så vet man att det finns olika typer av *records* i en DNS-servers databas. Man kan ändra vilken typ av record man frågar efter med kommandot **SET TYPE=**. Prova att ändra typ till *MX (Mail Exchanger, dvs. mailserveradress)* med kommandot **SET TYPE=MX**. Prova sedan att göra ett namnuppslag på adressen ***ntilund.se*** vilken adress (domännamn) har mailservern för lund.se?
26. Avsluta nslookup med kommandot **QUIT**
27. Kommandot **ROUTE** används för att visa och ändra i datorns routingtabell. Prova kommandot **ROUTE PRINT** som visar din dators routingtabell.
28. Kommandot **NBTSTAT** används för NetBIOS över TCP/IP och visar statistik och information (likt nslookup men för NetBIOS). Prova kommandot **NBTSTAT –R** som visar vilka datornamn som din dator har översatt med hjälp av NetBIOS. Det är inte säkert att ni har något namn i listan.
29. Ta reda på en kompis datornamn (som sitter på samma nätverk såklart) och prova att pinga detta datornamn. Prova sedan kommandot från förra uppgiften igen. Finns din kompis datornamn med i listan så har NetBIOS över TCP/IP använts till namnuppslagning.
30. Kommandot **NET** används för att utföra en mängd nätverksrelaterade saker. Detta och liknande kommandon lever vidare i Powershell (kan ses om en nyare och kraftfullare kommandotolk). Kör kommandot **NET** för att se alla alternativ.

31. Prova kommandot **NET VIEW** vilket visar en lista på alla datorer (och skrivare/enheter) i det lokala nätverket som aktiverat fil och skrivardelning. Du får samma resultat om du ”bläddrar” i nätverket grafiskt (använder utforskaren).
32. Med kommandot **NET USE** kan man mappa upp utdelade resurser. Detta är dock inget vi kommer att göra i denna laboration men det är viktigt att känna till.
33. Kommandot **NETSH** används för att visa eller ändra i en dators nätverkskonfiguration, allt från inställningar för nätverkskorten till inställningar för brandväggen (Windows-brandväggen). Kör kommandot **NETSH** för att starta programmet, observera att prompten ändras.
34. Skriv **HELP** för att se alla alternativ som finns.
35. Prova kommandot **WLAN SHOW ALL** som visar massa information om inställningar för trådlösa nätverk. Vilken standard använder det trådlösa nätverk (SSID) som du är ansluten till just nu?

    _____

    _____

36. Skriv **EXIT** för att avsluta netsh.