

PROTOCOL

to exercise

Wireshark

HTL
St. Pölten

EL

Group / Class 5 / 3BHEL	Secretary HOFSTÄTTER A.	Signature
Exercise- / Delivery date 17th March 2014	Employee	Signature
Teacher GRASINGER	Employee	Signature
Grade	Employee	Signature

Wireshark

Used Programs

Nr.	Device	Manufacturer	Type	Version
1.	Wireshark	-	Tool	1.10.5

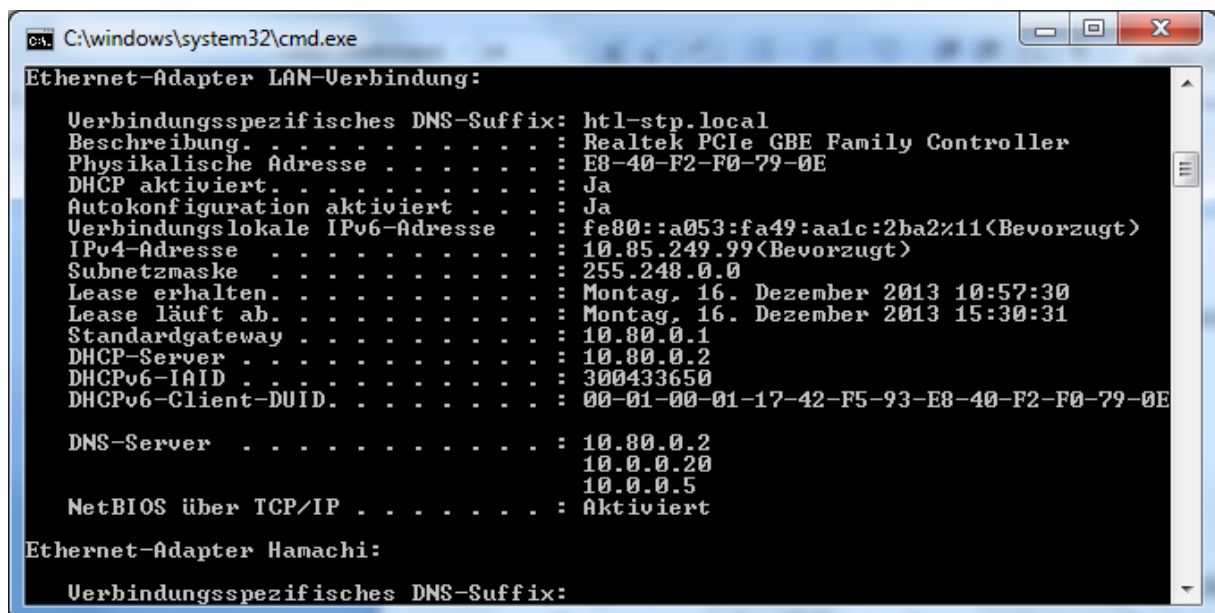
Task

Describing the following commands:

1. Ipconfig /all
2. ping
3. tracert

1.) Ipconfig /all

This command is used to display all current network configurations. With “/all” you get more details.



```
C:\windows\system32\cmd.exe
Ethernet-Adapter LAN-Verbindung:
    Verbindungsspezifisches DNS-Suffix: htl-stp.local
    Beschreibung. . . . . : Realtek PCIe GBE Family Controller
    Physikalische Adresse . . . . . : E8-40-F2-F0-79-0E
    DHCP aktiviert. . . . . : Ja
    Autokonfiguration aktiviert . . . . . : Ja
    Verbindungslokale IPv6-Adresse . . . . . : fe80::a053:fa49:aa1c:2ba2%11(Bevorzugt)
    IPv4-Adresse . . . . . : 10.85.249.99(Bevorzugt)
    Subnetzmaske . . . . . : 255.248.0.0
    Lease erhalten. . . . . : Montag, 16. Dezember 2013 10:57:30
    Lease läuft ab. . . . . : Montag, 16. Dezember 2013 15:30:31
    Standardgateway . . . . . : 10.80.0.1
    DHCP-Server . . . . . : 10.80.0.2
    DHCPv6-IAID . . . . . : 300433650
    DHCPv6-Client-DUID. . . . . : 00-01-00-01-17-42-F5-93-E8-40-F2-F0-79-0E

    DNS-Server . . . . . : 10.80.0.2
                        : 10.0.0.20
                        : 10.0.0.5
    NetBIOS über TCP/IP . . . . . : Aktiviert

Ethernet-Adapter Hamachi:
    Verbindungsspezifisches DNS-Suffix:
```

Fig.1: Ipconfig/all a very small part of the whole command

In this part of the command you can see my current ip address, standard gateway etc...

2.) Ping

Ping is a simple command which is sending a package to an ip address and tests the connectivity. If the package arrives at the ip address a response will be send back.

```

C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Simon>ping 10.85.250.64

Ping wird ausgeführt für 10.85.250.64 mit 32 Bytes Daten:
Antwort von 10.85.250.64: Bytes=32 Zeit=1ms TTL=64
Antwort von 10.85.250.64: Bytes=32 Zeit<1ms TTL=64
Antwort von 10.85.250.64: Bytes=32 Zeit<1ms TTL=64
Antwort von 10.85.250.64: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 10.85.250.64:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 1ms, Mittelwert = 0ms

C:\Users\Simon>_

```

Fig.2: Ping command to Lorenz Hirsch

Normally 4 packages will be send. You can also see the time, the size of one package and how many packages arrived.

Wireshark is able to capture all pings and other traffic.

632814	7229.86658	10.85.248.118	10.85.249.99	ICMP	106 Echo (ping) request	id=0x0001, seq=145/37120, ttl=1 (reply in 632815)
632815	7229.86671	10.85.249.99	10.85.248.118	ICMP	106 Echo (ping) reply	id=0x0001, seq=145/37120, ttl=128 (request in 632814)
632816	7229.86767	10.85.248.118	10.85.249.99	ICMP	106 Echo (ping) request	id=0x0001, seq=146/37376, ttl=1 (reply in 632817)
632817	7229.86777	10.85.249.99	10.85.248.118	ICMP	106 Echo (ping) reply	id=0x0001, seq=146/37376, ttl=128 (request in 632816)
632818	7229.86861	10.85.248.118	10.85.249.99	ICMP	106 Echo (ping) request	id=0x0001, seq=147/37632, ttl=1 (reply in 632819)
632819	7229.86870	10.85.249.99	10.85.248.118	ICMP	106 Echo (ping) reply	id=0x0001, seq=147/37632, ttl=128 (request in 632818)

Fig.3: A ping captured with wireshark

3.) Tracert

Tracert (also called Traceroute) is a program which calculates the route of a package. It tells which router and internet knots ip data packages it had to pass to arrive at the computer.

```

tracert to wikipedia.de (130.94.122.197), 30 hops max, 40 byte packets
 1  fli41.Netz1 (192.168.0.1)  0.765 ms  0.651 ms  0.497 ms

```

```

2  217.5.98.7 (217.5.98.7)  14.499 ms  14.648 ms  21.394 ms
3  217.237.152.46 (217.237.152.46)  14.831 ms  13.655 ms  13.403 ms
4  62.154.14.134 (62.154.14.134)  118.090 ms  119.522 ms  119.665 ms
5  p16-1-0-3.r20.asbnva01.us.bb.verio.net (129.250.9.141)  117.004 ms  117.370
ms  117.073 ms
6  p64-0-0-0.r21.asbnva01.us.bb.verio.net (129.250.2.35)  119.105 ms  119.284
ms  119.206 ms
7  p16-0-1-2.r20.plalca01.us.bb.verio.net (129.250.2.192)  180.035 ms  195.498
ms  178.704 ms
8  p16-1-0-0.r06.plalca01.us.bb.verio.net (129.250.3.81)  177.280 ms  177.263
ms  176.692 ms
9  p4-0-3-0.r00.sndgca01.us.bb.verio.net (129.250.3.10)  194.322 ms  193.477
ms  193.743 ms
10 ge-1-1.a03.sndgca01.us.da.verio.net (129.250.27.84)  192.527 ms  193.003 ms
192.464 ms
11 Pliny.wikipedia.org (130.94.122.197)  192.604 ms  193.875 ms  194.254 ms

```

Fig.4: Short sample of traceroute