



Betriebssysteme

Windows Netzwerke

Autor: Ronny Bodach

Stand 08.06.2023



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences



Fraunhofer
SIT



Bundeskriminalamt

[hs-mittweida.de](https://www.hs-mittweida.de)

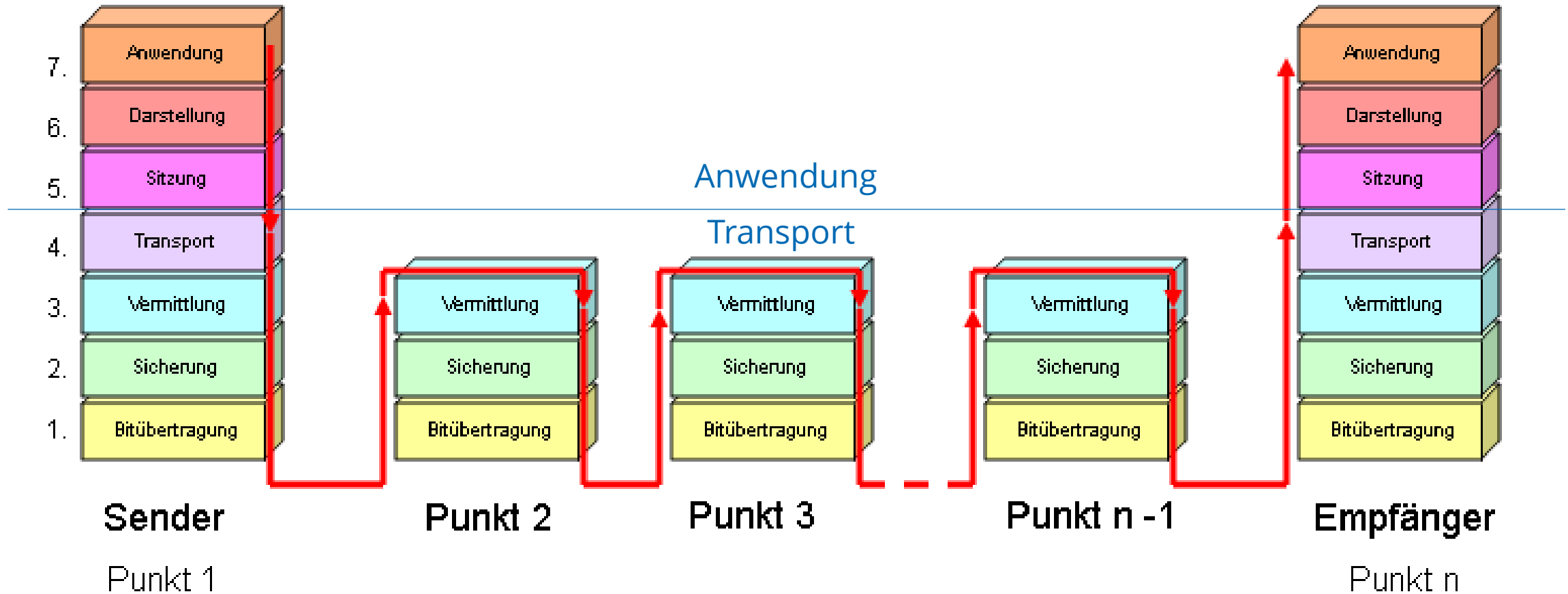
Agenda

1. Das ISO-OSI Modell (Einordnung Netzwerk)
2. Netzwerke unter Windows
 - Übersicht – Wichtige Begrifflichkeiten
 - Graphische Oberfläche
 - CMD-Befehle
 - PowerShell-Befehle

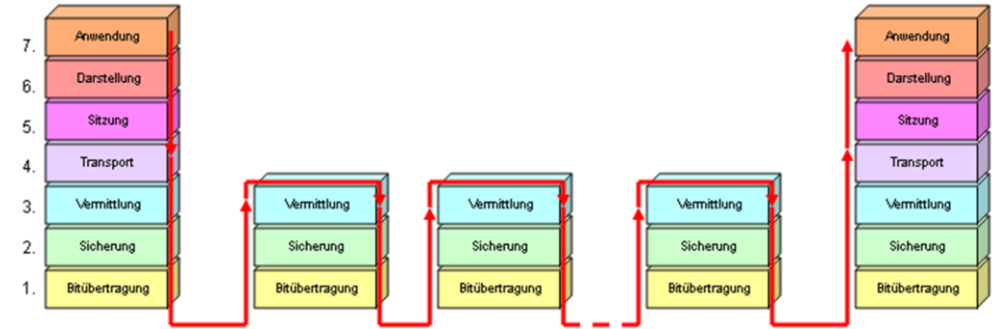
Das ISO-OSI Modell

Das OSI-Modell

Open System Interconnection



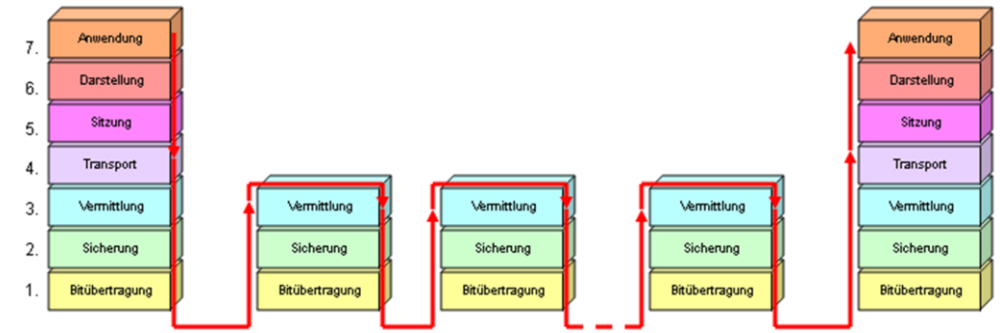
Das OSI-Modell



- Applikation Layer
 - Informationsaustausch zwischen Anwendungen
 - Teilnehmer Identifikation
 - Teilnehmer Verifikation und Sicherheitschecks
- Presentation Layer
 - Aufbereiten der Daten für Applikation Layer für einfachen Zugriff
 - Datenformatierung
 - Kompression
 - Übertragungsverschlüsselung
- Session Layer
 - High-Level Synchronisation zwischen Anwendungen
 - Regelung der Übertragungskommunikation (Wer spricht? Wer hört zu?)

Das OSI-Modell

- Transport Layer
 - Paketisierung der Daten
 - Organisation der ankommenden Daten (Reihenfolge)
 - Bereitstellen eines rein logischen Datenstromzugangs für Session Layer
- Network Layer
 - Paketzustellung (Routing)
 - Internetworkkommunikation
 - Logischer Netzwerkaufbau
- Data-Link Layer
 - Datenübertragung innerhalb eines Netzwerks
 - Daten erreichen nächsten Knoten auf der Route zum Zielrechner
 - Kollisionserkennung bei Übertragung
- Physical Layer
 - Übertragung von Bits zum nächsten Kommunikationsgerät



Windows Netzwerke

Übersicht

Wichtige Begrifflichkeiten

Heimnetzgruppen

- Ziel: Teilen eigener Ressourcen in einer Netzwerkgruppe
- Dezentrale Verwaltung von Ressourcen
 - Dateien (Bilder, Musik, ...)
 - Drucker
- Nur für Windows 7, 8, 8.1 vorhanden
- Passwortschutz für Heimnetzgruppe möglich
- Nur Beitritt zu bestehender Gruppe möglich für
 - Windows 7 Starter
 - Windows 7 Home Basic
 - Windows RT 8.1
- Share-Funktion für Windows 10 ersetzt Heimnetzgruppe

Netzwerkprofile

- Öffentlich
 - Gedacht für öffentliche Netze (WLAN im Hotel)
 - Nicht sichtbar im Netzwerk (Explorer-Auflistung unter Netzwerk)
 - Dateifreigabe gesperrt
 - Drucker gesperrt
- Privat
 - Gedacht für private Netze (Heimnetzwerk)
 - Sichtbar im Netzwerk (Explorer-Auflistung unter Netzwerk)
 - Dateifreigabe erlaubt (Einstellung bei Datei oder Ordner)
 - Drucker erlaubt (Einstellung bei Drucker)

Aktuellen Status auslesen

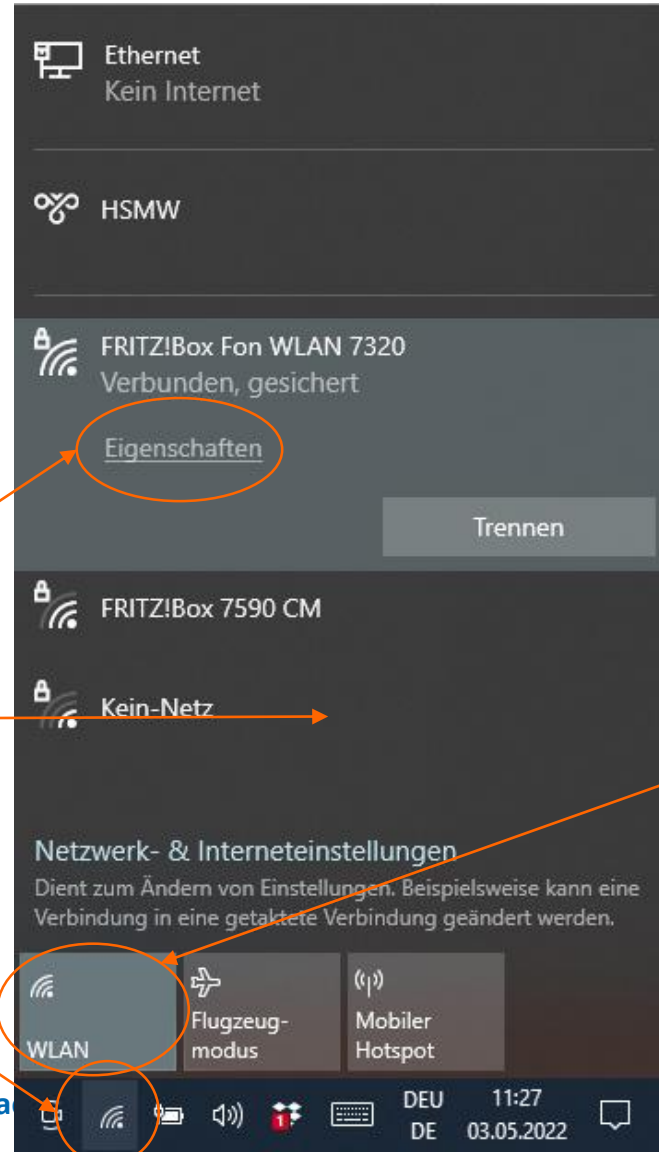
- Möglichkeiten zur Informationsgewinnung
 1. Graphische Oberfläche
 2. CMD-Befehle
 3. PowerShell-Befehle

Windows Netzwerke

Graphische Oberfläche

Windows Netzwerk Übersicht

- Netzwerke in Windows aufrufen (Taskleiste Netzwerk Symbol)



Ethernet (LAN Verbindungen)

VPN Verbindungen

Ethernet (WLAN Verbindungen)

Netzwerk Eigenschaften (Profil)

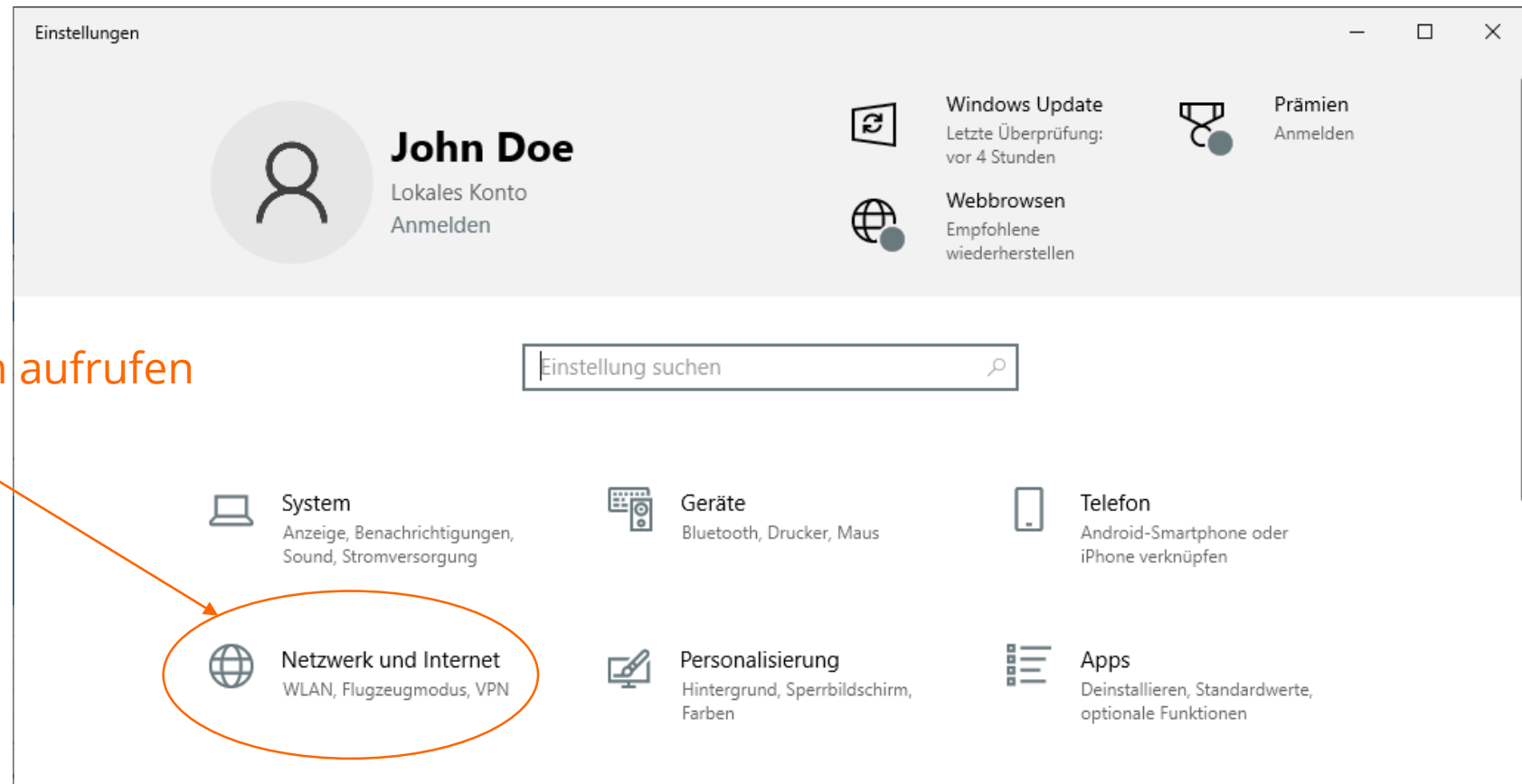
Netzwerkbereich Aufklappen

WLAN Aktivieren/Deaktivieren

Windows Netzwerk Übersicht

- Netzwerke in Windows einrichten (Startbutton rechts > Einstellungen)

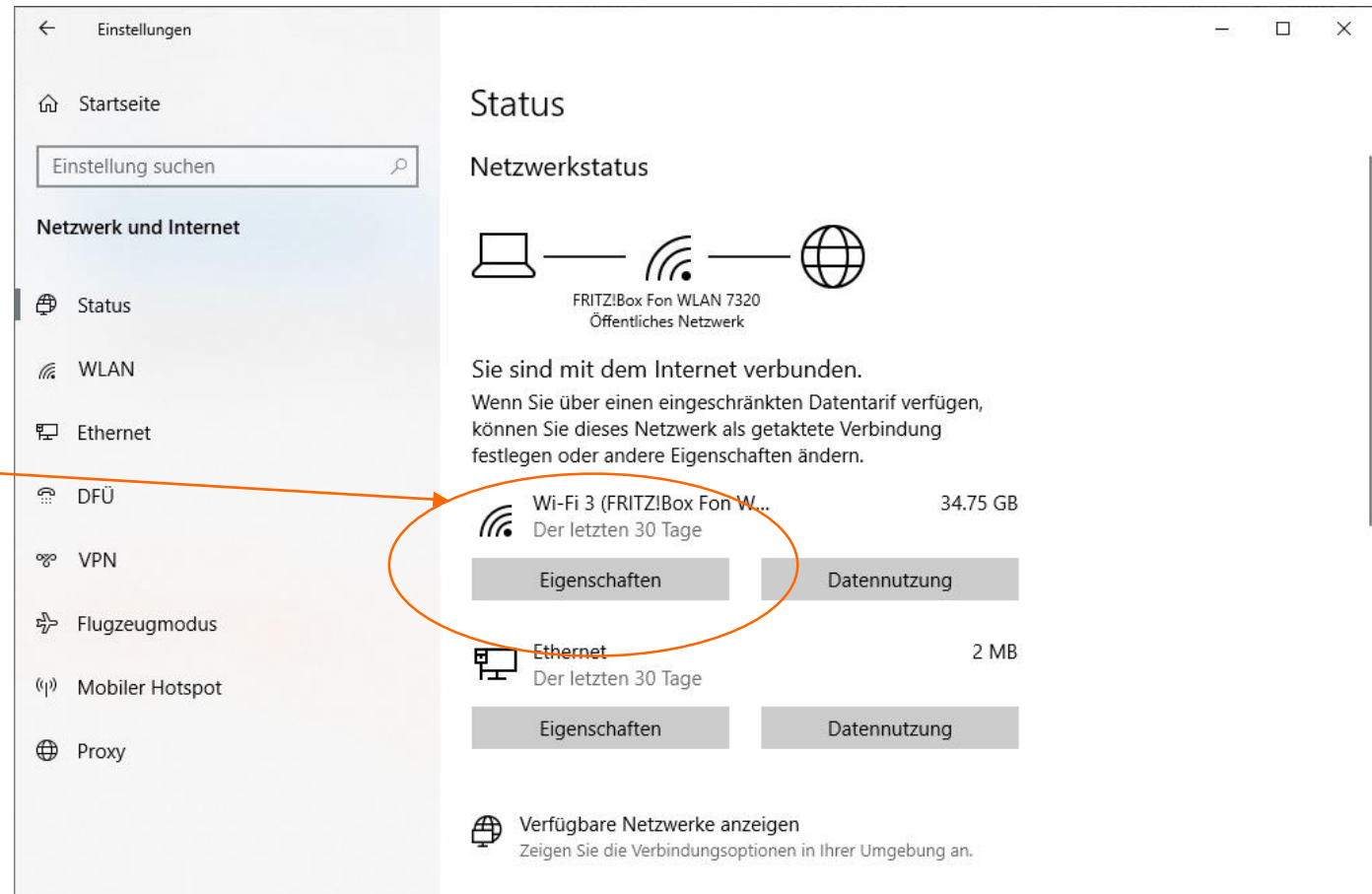
Netzwerkeinstellungen aufrufen



Netzwerkeinstellungen

- Auflistung des Netzwerkstatus (Verbindungen)

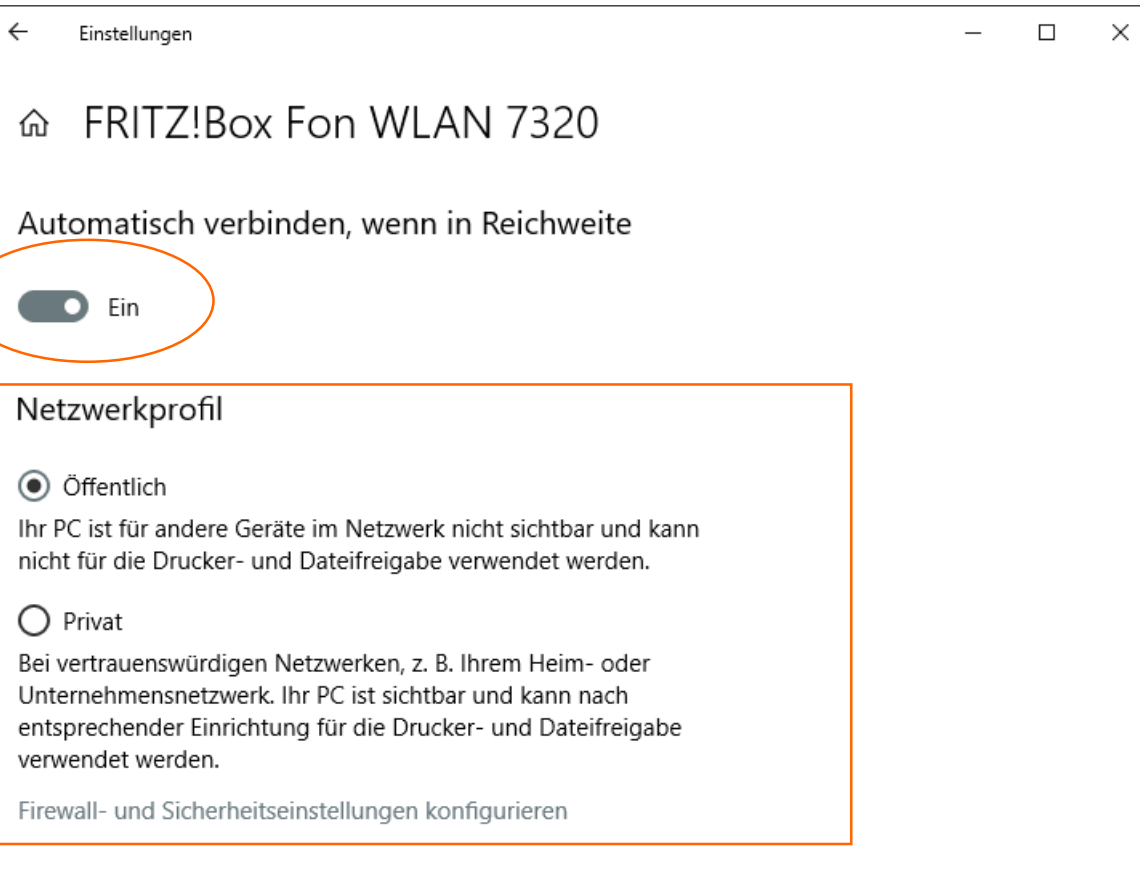
Netzwerkeigenschaften aufrufen



Netzwerkprofil

- Profileinstellungen

Verbindung aktiv



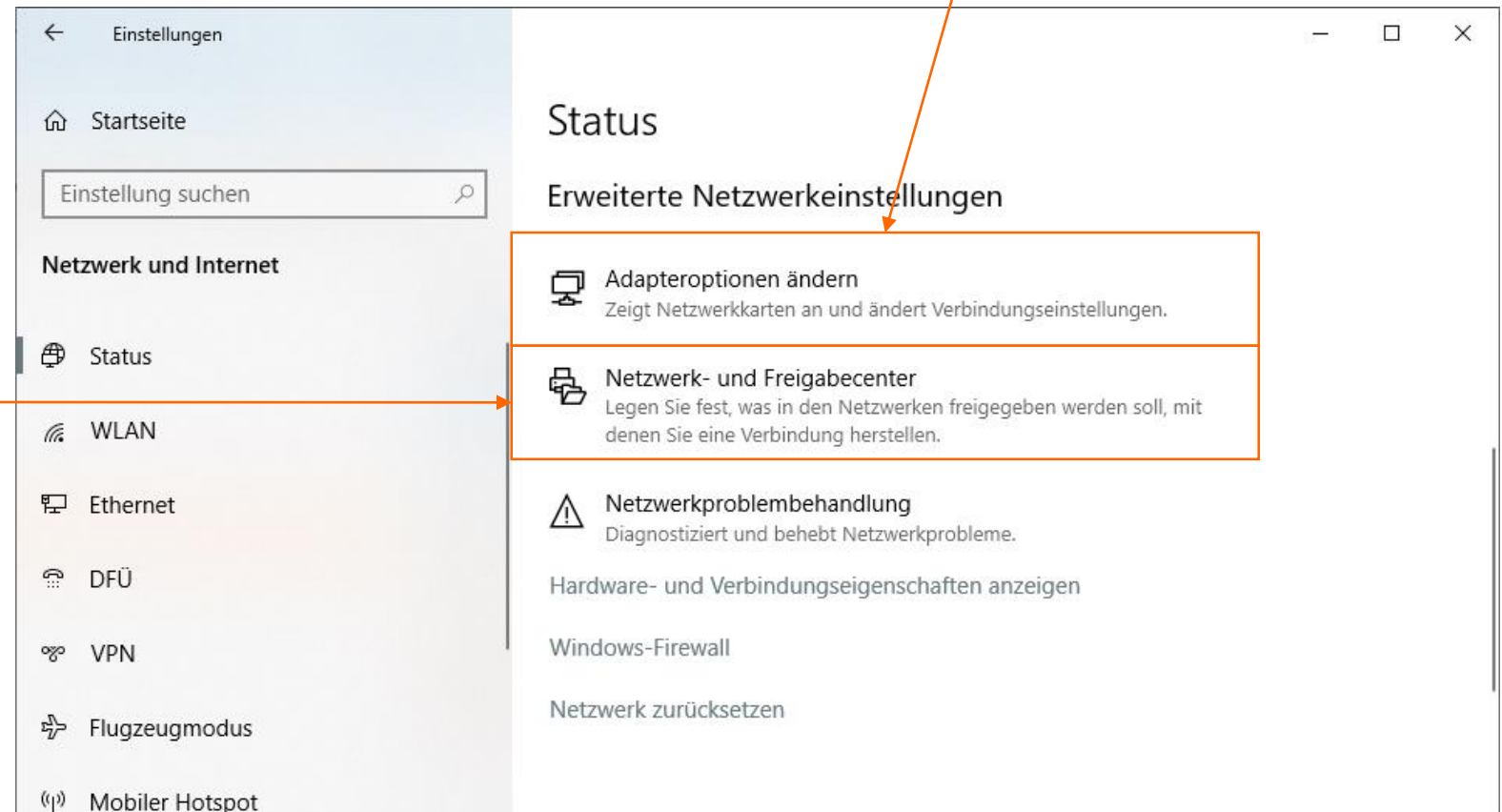
Netzwerkprofil Auswahl

Erweiterte Netzwerkeinstellungen

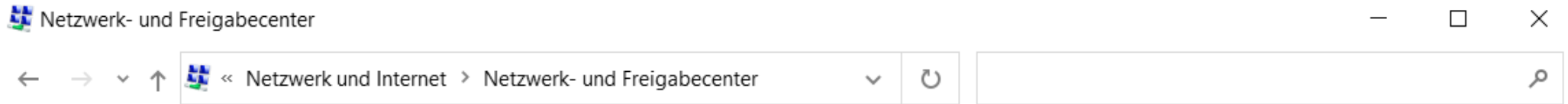
- Erweiterte Statusinformationen

Adapteroptionen aufrufen (IP Adressen)

Netzwerk und Freigabecenter



Netzwerk und Freigabecenter



Auflistung aller Netzwerkadapter

Startseite der Systemsteuerung

Adaptoreinstellungen ändern

Erweiterte Freigabeeinstellungen ändern

Medienstreamingoptionen

Grundlegende Informationen zum Netzwerk anzeigen und Verbindungen einrichten

Aktive Netzwerke anzeigen

Öffentliches Netzwerk

Freigabetyp

Auflistung von aktiven Verbindungen

Zugriffstyp: Internet

Verbindungen: WLAN

Link zu Details einer Verbindung

Netzwerkeinstellungen ändern



Neue Verbindung oder neues Netzwerk einrichten

Breitband-, DFÜ- oder VPN-Verbindung bzw. Router oder Zugriffspunkt einrichten.



Probleme beheben

Netzwerkprobleme diagnostizieren und reparieren oder Problembehandlungsinformationen abrufen.

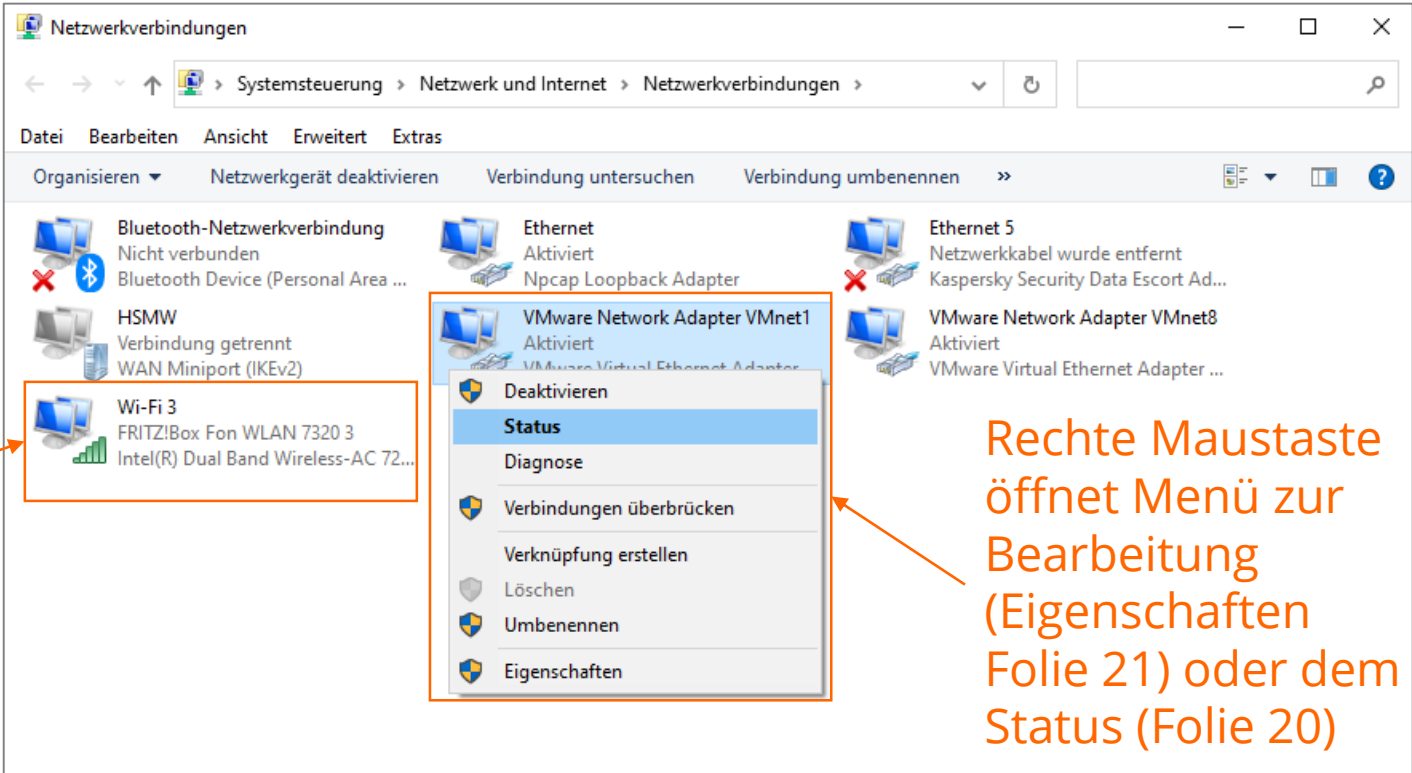
Siehe auch

Internetoptionen

Windows Defender Firewall

Adapteroptionen

- Übersicht aller Netzwerkadapter (Hardware und virtuell)

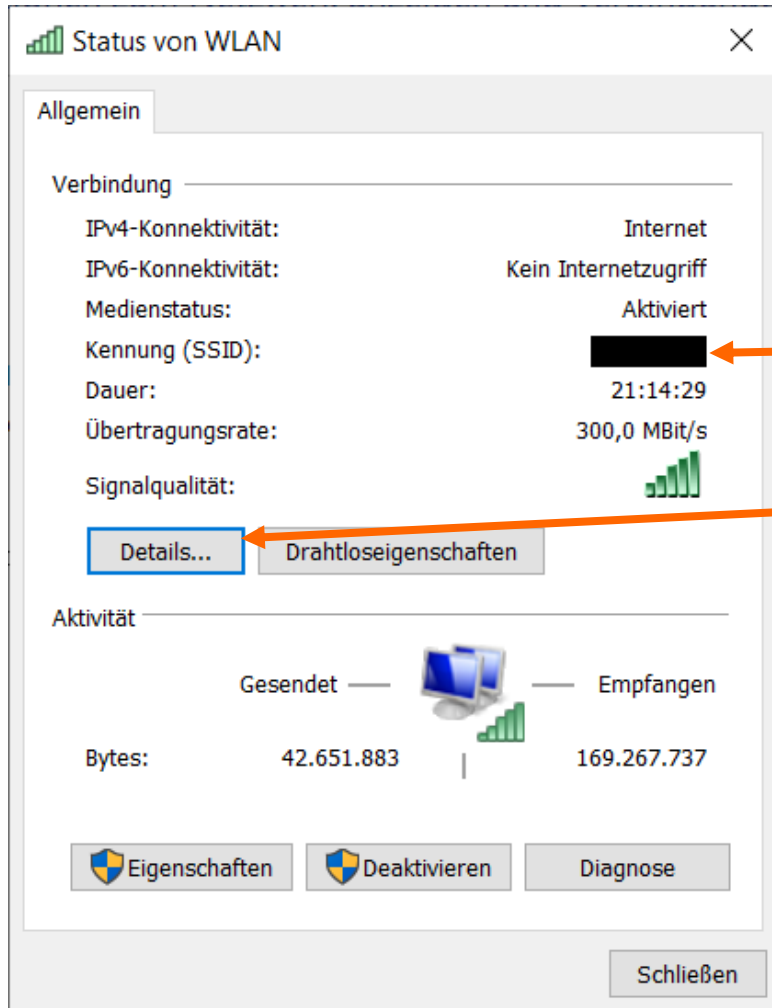


The screenshot shows the Windows 'Netzwerkverbindungen' (Network Connections) window. The window title is 'Netzwerkverbindungen' and the address bar shows the path: 'Systemsteuerung > Netzwerk und Internet > Netzwerkverbindungen'. The window contains a list of network adapters. One adapter, 'Wi-Fi 3', is highlighted with an orange box. A context menu is open over the 'VMware Network Adapter VMnet1' adapter, also highlighted with an orange box. The context menu options are: 'Deaktivieren', 'Status', 'Diagnose', 'Verbindungen überbrücken', 'Verknüpfung erstellen', 'Löschen', 'Umbenennen', and 'Eigenschaften'. An orange arrow points from the text 'Adapter mit Name' to the 'Wi-Fi 3' adapter. Another orange arrow points from the text 'Rechte Maustaste öffnet Menü zur Bearbeitung (Eigenschaften Folie 21) oder dem Status (Folie 20)' to the context menu.

Adapter mit Name

Rechte Maustaste öffnet Menü zur Bearbeitung (Eigenschaften Folie 21) oder dem Status (Folie 20)

Verbindungsdetails



Status von WLAN

Allgemein

Verbindung

IPv4-Konnektivität: Internet
IPv6-Konnektivität: Kein Internetzugriff
Medienstatus: Aktiviert
Kennung (SSID): [Redacted]
Dauer: 21:14:29
Übertragungsrate: 300,0 MBit/s
Signalqualität: [Signal strength icon]

Details... Drahtloseigenschaften

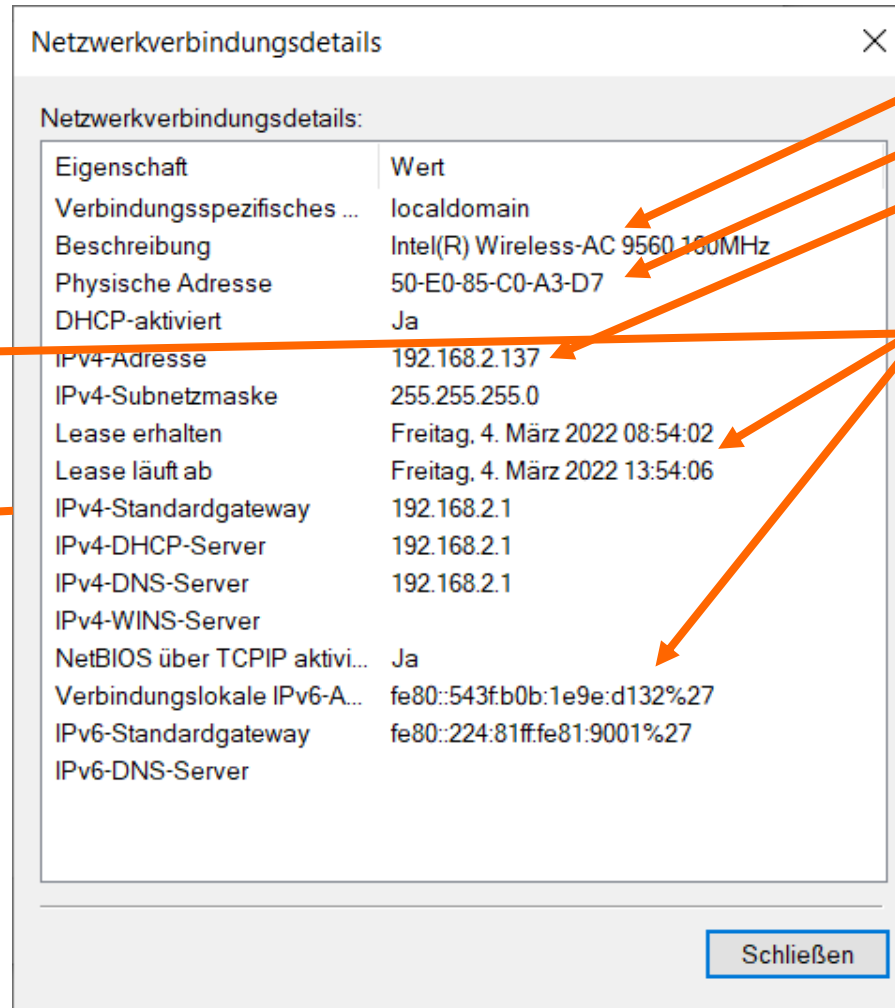
Aktivität

Gesendet — Empfangen

Bytes: 42.651.883 | 169.267.737

Eigenschaften Deaktivieren Diagnose

Schließen



Netzwerkverbindungsdetails

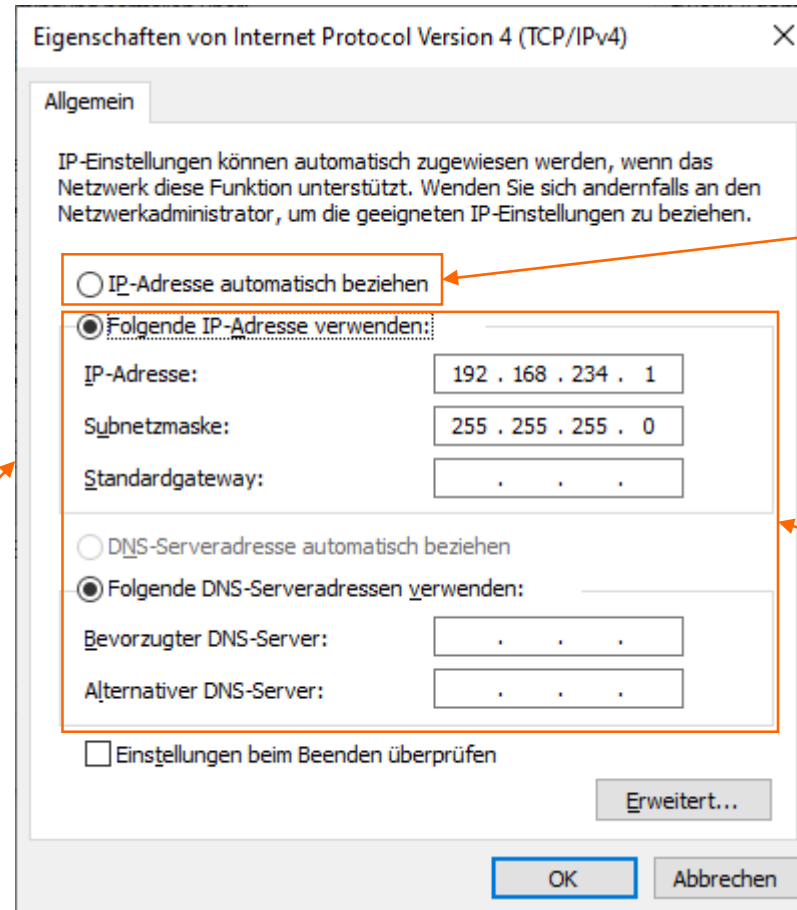
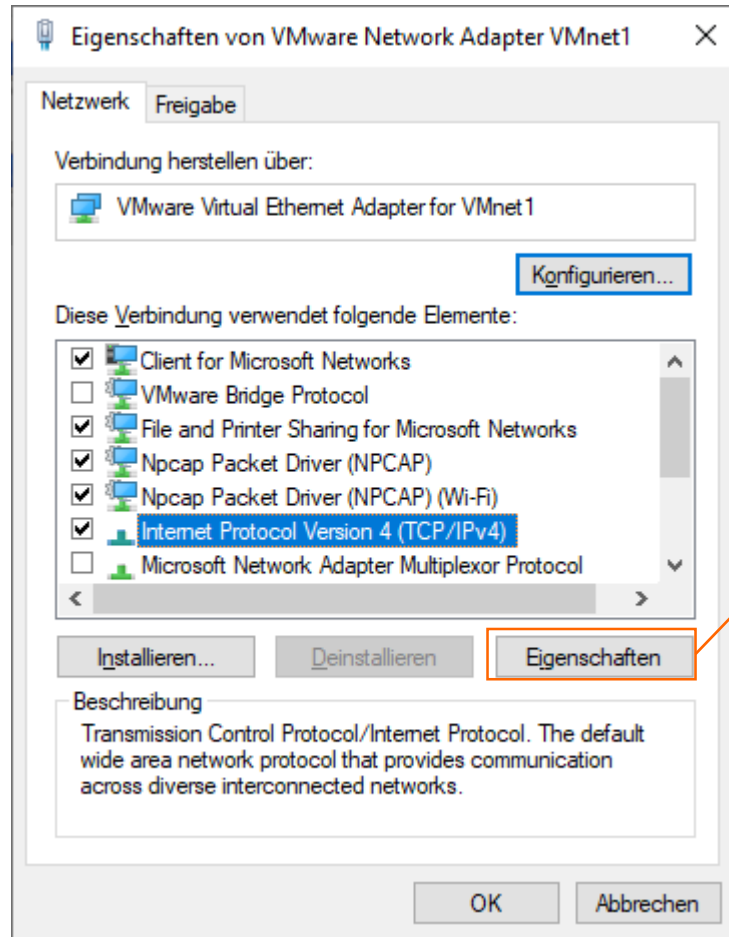
Netzwerkverbindungsdetails:

Eigenschaft	Wert
Verbindungsspezifisches ...	localdomain
Beschreibung	Intel(R) Wireless-AC 9560 160MHz
Physische Adresse	50-E0-85-C0-A3-D7
DHCP-aktiviert	Ja
IPv4-Adresse	192.168.2.137
IPv4-Subnetzmaske	255.255.255.0
Lease erhalten	Freitag, 4. März 2022 08:54:02
Lease läuft ab	Freitag, 4. März 2022 13:54:06
IPv4-Standardgateway	192.168.2.1
IPv4-DHCP-Server	192.168.2.1
IPv4-DNS-Server	192.168.2.1
IPv4-WINS-Server	
NetBIOS über TCPIP aktivi...	Ja
Verbindungslokale IPv6-A...	fe80::543f:b0b:1e9e:d132%27
IPv6-Standardgateway	fe80::224:81ff:fe81:9001%27
IPv6-DNS-Server	

Schließen

Interface
MAC-Adresse
IPv4-Adresse
IPv6-Adresse
DHCP-Details
SSID

Verbindungseinrichtung



DHCP Einstellung IPv4

Manuelle Einstellung IPv4 Adresse

Windows Netzwerke

CMD-Befehle

CMD-Befehle

- ipconfig
 - Network interfaces anzeigen
- getmac
 - MAC-Adressen von interfaces anzeigen
- netstat
 - Ports & offene TCP-Verbindungen
- systeminfo
 - Zusammenfassung des Systems (Hardware & OS)
- ping
 - Senden von ICMP-Requests
- tracert
 - Route mit TTL ermitteln
- pathping
 - Kombination von ping und tracert
- arp
 - ARP-Tabelle auswerten
- nslookup
 - DNS-Tabelle auswerten

ipconfig

- Network interfaces anzeigen
- Vorhandene Anschlüsse
 - Physikalisch
 - Virtuell
- IP-Adresse (v4 & v6)
- Subnetzmaske
- MAC-Adresse
- DHCP-Konfiguration
- DNS-Speicher auslesen

```
Eingabeaufforderung

Drahtlos-LAN-Adapter WLAN:

Verbindungsspezifisches DNS-Suffix: localdomain
Beschreibung. . . . . : Intel(R) Wireless-AC 9560 160MHz
Physische Adresse . . . . . : 50-E0-85-C0-A3-D7
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
Verbindungslokale IPv6-Adresse . . : fe80::543f:b0b:1e9e:d132%25(Bevorzugt)
IPv4-Adresse . . . . . : 192.168.2.137(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Lease erhalten. . . . . : Samstag, 26. März 2022 13:28:20
Lease läuft ab. . . . . : Mittwoch, 30. März 2022 16:18:30
Standardgateway . . . . . : fe80::224:81ff:fe81:9001%25
                               192.168.2.1
DHCP-Server . . . . . : 192.168.2.1
DHCPv6-IAID . . . . . : 139518085
DHCPv6-Client-DUID. . . . . : 00-01-00-01-29-AF-A7-C4-98-FA-9B-D6-8A-CF
DNS-Server . . . . . : 192.168.2.1
NetBIOS über TCP/IP . . . . . : Aktiviert
Suchliste für verbindungs-spezifische DNS-Suffixe:
                               localdomain

Ethernet-Adapter Bluetooth-Netzwerkverbindung:

Medienstatus. . . . . : Medium getrennt
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : Bluetooth Device (Personal Area Network)
Physische Adresse . . . . . : 50-E0-85-C0-A3-DB
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
```


getmac

- Interfaces anzeigen
- MAC-Adressen auflisten

```
C:\Users\fische11>getmac

Physisch. Adresse  Transportname
=====
50-E0-85-C0-A3-D7  Nicht zutreffend
98-FA-9B-D6-8A-CF  Medien ausgeworfen
50-E0-85-C0-A3-DB  Medien ausgeworfen
9C-9D-83-55-53-42  Medien ausgeworfen
00-15-5D-F5-B1-4D  Nicht zutreffend

C:\Users\fische11>
```

```
C:\Users\fische11>getmac /V

Verbindungsname  Netzwerkkadapter  Physisch. Adresse  Transportname
=====
=====
WLAN              Intel(R) Wirele  50-E0-85-C0-A3-D7  Nicht zutreffend
Ethernet          Intel(R) Ethern  98-FA-9B-D6-8A-CF  Medien ausgeworfen
Bluetooth-Netzw  Bluetooth Devic  50-E0-85-C0-A3-DB  Medien ausgeworfen
Mobilfunk         Generic Mobile   9C-9D-83-55-53-42  Medien ausgeworfen
vEthernet (WSL)  Hyper-V Virtual  00-15-5D-F5-B1-4D  Nicht zutreffend
```

netstat

- aktive TCP-Verbindungen anzeigen
- Offenen TCP-Ports auflisten

```
Eingabeaufforderung
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\John Doe>netstat -ano

Aktive Verbindungen

Proto Lokale Adresse Remoteadresse Status PID
TCP 0.0.0.0:135 0.0.0.0:0 ABHÖREN 1148
TCP 0.0.0.0:445 0.0.0.0:0 ABHÖREN 4
TCP 0.0.0.0:902 0.0.0.0:0 ABHÖREN 5356
TCP 0.0.0.0:912 0.0.0.0:0 ABHÖREN 5356
TCP 192.168.188.50:139 0.0.0.0:0 ABHÖREN 4
TCP 192.168.188.50:1047 20.199.120.85:443 HERGESTELLT 5528
TCP 192.168.188.50:1084 74.125.140.188:5228 HERGESTELLT 384
TCP 192.168.188.50:1180 52.97.137.146:443 HERGESTELLT 8632
TCP 192.168.188.50:1181 52.97.137.146:443 HERGESTELLT 8632
TCP 192.168.188.50:1531 52.114.76.233:443 HERGESTELLT 9240
TCP 192.168.188.50:1921 152.199.19.161:443 SCHLIESSEN_WARTEN 8632
TCP 192.168.188.50:2492 52.114.74.176:443 HERGESTELLT 13476
TCP 192.168.188.50:2514 162.125.19.131:443 HERGESTELLT 12392
TCP 192.168.188.50:2544 162.125.19.130:443 HERGESTELLT 12392
TCP 192.168.188.50:2595 142.250.185.99:443 WARTEND 0
TCP 192.168.188.50:2612 52.113.205.35:443 HERGESTELLT 13476
TCP 192.168.188.50:2618 62.67.238.142:443 WARTEND 0
```

netstat

- Routing-Tabellen auflisten
- Statistiken zu einzelnen Protokollen anzeigen

```
C:\Users\fische11>netstat -r

=====
Schnittstellenliste
19...98 fa 9b d6 8a cf .....Intel(R) Ethernet Connection (6) I219-V
15...50 e0 85 c0 a3 d8 .....Microsoft Wi-Fi Direct Virtual Adapter
 6...52 e0 85 c0 a3 d7 .....Microsoft Wi-Fi Direct Virtual Adapter #2
34...9c 9d 83 55 53 42 .....Generic Mobile Broadband Adapter
25...50 e0 85 c0 a3 d7 .....Intel(R) Wireless-AC 9560 160MHz
26...50 e0 85 c0 a3 db .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
61...00 15 5d f5 b1 4d .....Hyper-V Virtual Ethernet Adapter
=====

IPv4-Routentabelle
=====
Aktive Routen:
   Netzwerkziel   Netzwerkmaske   Gateway   Schnittstelle   Metrik
   0.0.0.0         0.0.0.0         192.168.2.1 192.168.2.137   45
   127.0.0.0         255.0.0.0       Auf Verbindung 127.0.0.1       331
   127.0.0.1         255.255.255.255 Auf Verbindung 127.0.0.1       331
127.255.255.255 255.255.255.255 Auf Verbindung 127.0.0.1       331
   172.22.16.0      255.255.240.0   Auf Verbindung 172.22.16.1     5256
   172.22.16.1      255.255.255.255 Auf Verbindung 172.22.16.1     5256
   172.22.31.255    255.255.255.255 Auf Verbindung 172.22.16.1     5256
   192.168.2.0       255.255.255.0   Auf Verbindung 192.168.2.137   301
   192.168.2.137    255.255.255.255 Auf Verbindung 192.168.2.137   301
   192.168.2.255    255.255.255.255 Auf Verbindung 192.168.2.137   301
   224.0.0.0         240.0.0.0       Auf Verbindung 127.0.0.1       331
   224.0.0.0         240.0.0.0       Auf Verbindung 192.168.2.137   301
   224.0.0.0         240.0.0.0       Auf Verbindung 172.22.16.1     5256
255.255.255.255 255.255.255.255 Auf Verbindung 127.0.0.1       331
255.255.255.255 255.255.255.255 Auf Verbindung 192.168.2.137   301
255.255.255.255 255.255.255.255 Auf Verbindung 172.22.16.1     5256
=====
```

systeminfo

- Informationen über das System (Computer)
- OS-Version
- Hostname
- Prozessor
- BIOS-Version
- Arbeitsspeicher
- Domainname
- Netzwerkkarte mit IPs

```
Eingabeaufforderung
C:\Users\fische11>systeminfo

Hostname:                DESKTOP-5MHG39V
Betriebssystemname:      Microsoft Windows 10 Pro
Betriebssystemversion:   10.0.19044 Nicht zutreffend Build 19044
Betriebssystemhersteller: Microsoft Corporation
Betriebssystemkonfiguration: Eigenständige Arbeitsstation
Typ des Betriebssystembuilds: Multiprocessor Free
Registrierter Benutzer:  fische11
Registrierte Organisation:
Produkt-ID:              00330-52309-76972-AAOEM
Ursprüngliches Installationsdatum: 01.03.2022, 10:54:40
Systemstartzeit:        09.03.2022, 23:53:31
Systemhersteller:       LENOVO
Systemmodell:            20QDS1N000
Systemtyp:               x64-based PC
Prozessor(en):           1 Prozessor(en) installiert.
                        [01]: Intel64 Family 6 Model 142 Stepping 12 GenuineInt
e1 ~1792 MHz
BIOS-Version:            LENOVO N2HET62W (1.45 ), 15.04.2021
Windows-Verzeichnis:    C:\Windows
System-Verzeichnis:     C:\Windows\system32
Startgerät:              \Device\HarddiskVolume1
Systemgebietsschema:    de;Deutsch (Deutschland)
Eingabegbietsschema:    de;Deutsch (Deutschland)
Zeitzone:                (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wi
en
Gesamter physischer Speicher: 16.156 MB
Verfügbarer physischer Speicher: 6.226 MB
Virtueller Arbeitsspeicher: Maximale Größe: 27.660 MB
Virtueller Arbeitsspeicher: Verfügbar: 3.104 MB
Virtueller Arbeitsspeicher: Zurzeit verwendet: 24.556 MB
Auslagerungsdateipfad(e): C:\pagefile.sys
Domäne:                  WORKGROUP
Anmeldeserver:           \\DESKTOP-5MHG39V
Hotfix(es):              5 Hotfix(e) installiert.
                        [01]: KB5010472
                        [02]: KB5003791
                        [03]: KB5011487
                        [04]: KB5011352
                        [05]: KB5005699
Netzwerkkarte(n):       5 Netzwerkkarte(n) installiert.
                        [01]: Intel(R) Wireless-AC 9560 160MHz
```

ping

- Erreichbarkeit einer IP-Adresse prüfen
- Standardmäßig TTL von 64
- Hops auf Route zum Ziel ermitteln
- ICMP-Error anzeigen

```
Eingabeaufforderung - ping -t 8.8.8.8
C:\Users\fische11>ping -t 8.8.8.8

Ping wird ausgeführt für 8.8.8.8 mit 32 Bytes Daten:
Antwort von 8.8.8.8: Bytes=32 Zeit=39ms TTL=117
Antwort von 8.8.8.8: Bytes=32 Zeit=46ms TTL=117
Antwort von 8.8.8.8: Bytes=32 Zeit=24ms TTL=117
Antwort von 8.8.8.8: Bytes=32 Zeit=23ms TTL=117
Antwort von 8.8.8.8: Bytes=32 Zeit=29ms TTL=117

C:\Users\fische11>ping -i 8 8.8.8.8

Ping wird ausgeführt für 8.8.8.8 mit 32 Bytes Daten:
Antwort von 142.250.214.197: Die Gültigkeitsdauer wurde bei der Übertragung überschritten.
Antwort von 142.250.214.197: Die Gültigkeitsdauer wurde bei der Übertragung überschritten.
Antwort von 142.250.214.197: Die Gültigkeitsdauer wurde bei der Übertragung überschritten.
Antwort von 142.250.214.197: Die Gültigkeitsdauer wurde bei der Übertragung überschritten.

Ping-Statistik für 8.8.8.8:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),

C:\Users\fische11>ping -i 9 8.8.8.8

Ping wird ausgeführt für 8.8.8.8 mit 32 Bytes Daten:
Antwort von 8.8.8.8: Bytes=32 Zeit=25ms TTL=117
Antwort von 8.8.8.8: Bytes=32 Zeit=27ms TTL=117
Antwort von 8.8.8.8: Bytes=32 Zeit=21ms TTL=117
Antwort von 8.8.8.8: Bytes=32 Zeit=21ms TTL=117

Ping-Statistik für 8.8.8.8:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
```

tracert

- Hops zum Ziel ermitteln
- Entspricht meistens Route zum Ziel
- Namensauflösung benötigt viel Zeit

```

c:\> Eingabeaufforderung

C:\Users\fische11>tracert 8.8.8.8

Routenverfolgung zu dns.google [8.8.8.8]
über maximal 30 Hops:

 1    2 ms    2 ms    4 ms  OPNsense.localdomain [192.168.2.1]
 2   16 ms   24 ms   15 ms  ██████████
 3   17 ms   17 ms   14 ms  ██████████
 4   16 ms   19 ms   14 ms  ██████████
 5   26 ms   25 ms   21 ms  be12-rb2-fra14.envia-tel.net [77.235.191.174]
 6   20 ms   21 ms   19 ms  72.14.212.52
 7   24 ms   22 ms   31 ms  209.85.142.109
 8   41 ms   28 ms   29 ms  142.250.214.197
 9   32 ms   22 ms   21 ms  dns.google [8.8.8.8]

Ablaufverfolgung beendet.

C:\Users\fische11>tracert -d 8.8.8.8

Routenverfolgung zu 8.8.8.8 über maximal 30 Hops

 1     5 ms    1 ms    2 ms  192.168.2.1
 2   14 ms   12 ms   11 ms  ██████████
 3   12 ms   15 ms   14 ms  ██████████
 4   19 ms   17 ms   19 ms  ██████████
 5   26 ms   31 ms   25 ms  77.235.191.174
 6   27 ms   21 ms   21 ms  72.14.212.52
 7   20 ms   21 ms   23 ms  209.85.142.109
 8   23 ms   22 ms   25 ms  142.250.214.197
 9   22 ms   26 ms   21 ms  8.8.8.8

Ablaufverfolgung beendet.

```

30 Sekunden

9 Sekunden

tracert

```
Eingabeaufforderung
C:\Users\fische11>tracert -d 192.168.1.15

Routenverfolgung zu 192.168.1.15 über maximal 30 Hops

 1    2 ms    1 ms    1 ms    192.168.2.1
 2    *      *      *      Zeitüberschreitung der Anforderung.
 3    *      *      *      Zeitüberschreitung der Anforderung.
 4    *      *      *      Zeitüberschreitung der Anforderung.
 5    *      ^C

C:\Users\fische11>tracert -d hsmw.de

Routenverfolgung zu hsmw.de [141.55.192.190]
über maximal 30 Hops:

 1     9 ms    3 ms    1 ms    192.168.2.1
 2    20 ms   12 ms   20 ms
 3    11 ms   11 ms   21 ms
 4    20 ms   17 ms   12 ms
 5    22 ms   19 ms   31 ms    77.235.191.174
 6    21 ms   22 ms   20 ms    77.235.191.185
 7    26 ms   21 ms   21 ms    80.156.160.161
 8    19 ms   31 ms   21 ms    217.0.203.18
 9    22 ms   20 ms   25 ms    80.150.169.190
10    28 ms   32 ms   22 ms    188.1.144.221
11    36 ms   36 ms   38 ms    188.1.144.246
12    32 ms   33 ms   34 ms    188.1.237.82
13    *      *      *      Zeitüberschreitung der Anforderung.
14    *      *      *      Zeitüberschreitung der Anforderung.
15    32 ms   37 ms   34 ms    141.55.192.190

Ablaufverfolgung beendet.
```

Host existiert nicht

Hops auf Route antworten nicht auf ICMP

pathping

- Detailliertere Auflistung als tracer
- Eigene IP-Adresse mit angezeigt
- Path schneller angezeigt
- Statistik langsamer, aber ausführlicher
- Adressiert Hops direkt
- Probleme im Netzwerk leichter identifizierbar
- **Achtung!** nicht path ping

```
Eingabeaufforderung
C:\Users\fische11>pathping -n 8.8.8.8

Routenverfolgung zu "8.8.8.8" über maximal 30 Hops

 0 192.168.2.137
 1 192.168.2.1
 2 [REDACTED]
 3 [REDACTED]
 4 [REDACTED]
 5 77.235.191.174
 6 72.14.212.52
 7 209.85.142.109
 8 142.250.214.197
 9 8.8.8.8

Berechnung der Statistiken dauert ca. 225 Sekunden...
Abs. Zeit   Quelle zum Abs.   Knoten/Verbindung
Verl./Ges.= %   Verl./Ges.= %   Adresse
 0          192.168.2.137
 1    3ms    0/ 100 = 0%      0/ 100 = 0%    192.168.2.1
 2   18ms    0/ 100 = 0%      0/ 100 = 0%    [REDACTED]
 3   15ms    0/ 100 = 0%      0/ 100 = 0%    [REDACTED]
 4   19ms    0/ 100 = 0%      0/ 100 = 0%    [REDACTED]
 5   23ms    0/ 100 = 0%      0/ 100 = 0%    77.235.191.174
 6   23ms    0/ 100 = 0%      0/ 100 = 0%    72.14.212.52
 7   25ms    0/ 100 = 0%      0/ 100 = 0%    209.85.142.109
 8   ---    100/ 100 =100%   100/ 100 =100% 142.250.214.197
 9   23ms    0/ 100 = 0%      0/ 100 = 0%    8.8.8.8

Ablaufverfolgung beendet.
```

1 Sekunde

4 Minuten

pathping

-n

```
Eingabeaufforderung
C:\Users\fische11>pathping -n 8.8.8.8

Routenverfolgung zu "8.8.8.8" über maximal 30 Hops

 0 192.168.2.137
 1 192.168.2.1
 2 [REDACTED]
 3 [REDACTED]
 4 [REDACTED]
 5 77.235.191.174
 6 72.14.212.52
 7 209.85.142.109
 8 142.250.214.197
 9 8.8.8.8

Berechnung der Statistiken dauert ca. 225 Sekunden...
Quelle zum Abs. Knoten/Verbindung
Abs. Zeit Verl./Ges.= % Verl./Ges.= % Adresse
 0 0/ 100 = 0% 0/ 100 = 0% 192.168.2.137
 1 3ms 0/ 100 = 0% 0/ 100 = 0% 192.168.2.1
 2 18ms 0/ 100 = 0% 0/ 100 = 0% [REDACTED]
 3 15ms 0/ 100 = 0% 0/ 100 = 0% [REDACTED]
 4 19ms 0/ 100 = 0% 0/ 100 = 0% [REDACTED]
 5 23ms 0/ 100 = 0% 0/ 100 = 0% 77.235.191.174
 6 23ms 0/ 100 = 0% 0/ 100 = 0% 72.14.212.52
 7 25ms 0/ 100 = 0% 0/ 100 = 0% 209.85.142.109
 8 --- 100/ 100 =100% 100/ 100 =100% 142.250.214.197
 9 23ms 0/ 100 = 0% 0/ 100 = 0% 8.8.8.8

Ablaufverfolgung beendet.
C:\Users\fische11>
```

1 Sekunde

4 Minuten

```
Eingabeaufforderung
C:\Users\fische11>pathping hsmw.de

Routenverfolgung zu "hsmw.de" [141.55.192.190]
über maximal 30 Hops:
 0 DESKTOP-5MHG39V.localdomain [192.168.2.137]
 1 OPNsense.localdomain [192.168.2.1]
 2 [REDACTED]
 3 [REDACTED]
 4 [REDACTED]
 5 be12-rb2-fra14.envia-tel.net [77.235.191.174]
 6 be11-rb2-fra7.envia-tel.net [77.235.191.185]
 7 80.156.160.161
 8 pd900cb12.dip0.t-ipconnect.de [217.0.203.18]
 9 80.150.169.190
10 cr-er12-be8.x-win.dfn.de [188.1.144.221]
11 cr-lap1-be7.x-win.dfn.de [188.1.144.246]
12 kr-hsmitw9.x-win.dfn.de [188.1.237.82]
13 * * *

Berechnung der Statistiken dauert ca. 300 Sekunden...
Quelle zum Abs. Knoten/Verbindung
Abs. Zeit Verl./Ges.= % Verl./Ges.= % Adresse
 0 0/ 100 = 0% 0/ 100 = 0% DESKTOP-5MHG39V.localdomain [192.168.2.137]
 1 3ms 0/ 100 = 0% 0/ 100 = 0% OPNsense.localdomain [192.168.2.1]
 2 20ms 0/ 100 = 0% 0/ 100 = 0% [REDACTED]
 3 17ms 0/ 100 = 0% 0/ 100 = 0% [REDACTED]
 4 20ms 0/ 100 = 0% 0/ 100 = 0% [REDACTED]
 5 25ms 0/ 100 = 0% 0/ 100 = 0% be12-rb2-fra14.envia-tel.net [77.235.191.174]
 6 25ms 0/ 100 = 0% 0/ 100 = 0% be11-rb2-fra7.envia-tel.net [77.235.191.185]
 7 24ms 0/ 100 = 0% 0/ 100 = 0% 80.156.160.161
 8 25ms 0/ 100 = 0% 0/ 100 = 0% pd900cb12.dip0.t-ipconnect.de [217.0.203.18]
 9 --- 100/ 100 =100% 100/ 100 =100% 80.150.169.190
10 --- 100/ 100 =100% 0/ 100 = 0% cr-er12-be8.x-win.dfn.de [188.1.144.221]
11 --- 100/ 100 =100% 0/ 100 = 0% cr-lap1-be7.x-win.dfn.de [188.1.144.246]
12 --- 100/ 100 =100% 0/ 100 = 0% kr-hsmitw9.x-win.dfn.de [188.1.237.82]
```

30 Sekunden

5 Minuten

arp

- ARP-Tabelle anzeigen
- Kommunikationspartner
- Teilnehmer des Netzwerkes
- Hersteller von Netzwerkkarten (Vendor Lookup)

```
Eingabeaufforderung
C:\Users\fische11>arp -a

Schnittstelle: 192.168.2.137 --- 0x19
  Internetadresse   Physische Adresse   Typ
  192.168.2.1      81-90-01            dynamisch
  192.168.2.255    ff-ff-ff-ff-ff-ff   statisch
  224.0.0.22       01-00-5e-00-00-16   statisch
  224.0.0.251     01-00-5e-00-00-fb   statisch
  224.0.0.252     01-00-5e-00-00-fc   statisch
  239.255.255.250  01-00-5e-7f-ff-fa   statisch
  255.255.255.255  ff-ff-ff-ff-ff-ff   statisch

Schnittstelle: 172.22.16.1 --- 0x3d
  Internetadresse   Physische Adresse   Typ
  172.22.31.255    ff-ff-ff-ff-ff-ff   statisch
  224.0.0.22       01-00-5e-00-00-16   statisch
  224.0.0.251     01-00-5e-00-00-fb   statisch
  224.0.0.252     01-00-5e-00-00-fc   statisch
  239.255.255.250  01-00-5e-7f-ff-fa   statisch
```

```
Eingabeaufforderung
C:\Users\fische11>arp -a 192.168.2.1

Schnittstelle: 192.168.2.137 --- 0x19
  Internetadresse   Physische Adresse   Typ
  192.168.2.1      81-90-01            dynamisch

C:\Users\fische11>
```

nslookup

- DNS-Adresse auflösen
- IP-Adresse in DNS auflösen
- **Achtung!**
 - Mehrere DNS-Adressen können auf die gleiche IP zeigen
 - Mehrere IP-Adressen können für eine DNS-Adresse hinterlegt werden (Anycast)

```
Eingabeaufforderung
C:\Users\fische11>nslookup www.hsmw.de
Server: OPNsense.localdomain
Address: 192.168.2.1

Nicht autorisierende Antwort:
Name: www.hsmw.de
Address: 141.55.192.190

C:\Users\fische11>nslookup www.google.de
Server: OPNsense.localdomain
Address: 192.168.2.1

Nicht autorisierende Antwort:
Name: www.google.de
Addresses: 2a00:1450:4001:811::2003
           142.250.185.163

C:\Users\fische11>nslookup fraunhofer.de
Server: OPNsense.localdomain
Address: 192.168.2.1

Nicht autorisierende Antwort:
Name: fraunhofer.de
Address: 192.102.162.236
```

nslookup

```
Eingabeaufforderung
C:\Users\fische11>nslookup 141.55.192.190
Server: OPNsense.localdomain
Address: 192.168.2.1

Name:      www.htwm.de
Address: 141.55.192.190

C:\Users\fische11>nslookup 141.55.192.190
Server: OPNsense.localdomain
Address: 192.168.2.1

Name:      www.mcn.hs-mittweida.de
Address: 141.55.192.190

Eingabeaufforderung
C:\Users\fische11>nslookup -type=any mail.hsmw.de
Server: OPNsense.localdomain
Address: 192.168.2.1

Nicht autorisierende Antwort:
mail.hsmw.de      internet address = 141.55.192.84
mail.hsmw.de      MX preference = 10, mail exchanger = c1021.mx.srv.dfn.de
mail.hsmw.de      MX preference = 10, mail exchanger = b1021.mx.srv.dfn.de
mail.hsmw.de      MX preference = 10, mail exchanger = a1021.mx.srv.dfn.de

hsmw.de nameserver = tigger.scc.uni-weimar.de
hsmw.de nameserver = dns.hs-mittweida.de
hsmw.de nameserver = deneb.dfn.de

C:\Users\fische11>
```

Reverse Lookup

-type=any

Windows Netzwerke

PowerShell-Befehle

PowerShell-Befehle

- Get-NetAdapter
 - Netzwerkadapter auflisten
- Get-NetAdapterAdvancedProperty
 - Einstellungen zu Netzwerkadaptern anzeigen
- Get-NetAdapterHardwareInfo
 - Hardware zu Netzwerkadaptern auflisten
- Get-NetAdapterPowerManagement
 - Energieverbraucheinstellungen zu Netzwerkadaptern anzeigen
- Get-NetAdapterStatistics
 - Sende- & Empfangsstatistik von Netzwerkadaptern

PowerShell-Befehle

- Get-NetIPAddress
 - Informationen zu IP-Adresse
- Get-NetNeighbor
 - Auflistung bekannter Netzwerkteilnehmer in angeschlossenen Netzwerken
- Get-NetRoute
 - Auflistung der Routingtabelle
- Get-NetTCPConnection
 - Auflistung aller TCP-Ports & TCP-Verbindungen
- Get-NetUDPEndpoint
 - Auflistung aller UDP-Ports

Get-NetAdapter

- Netzwerkadapter auflisten
 - Name
 - Interface
 - Interface Index
 - Status
 - MAC-Adresse
 - Verbindungsgeschwindigkeit

```
Administrator: Windows PowerShell
HINWEISE
Zum Aufrufen der Beispiele geben Sie Folgendes ein: "get-help Get-NetAdapter -examples".
Weitere Informationen erhalten Sie mit folgendem Befehl: "get-help Get-NetAdapter -detailed".
Technische Informationen erhalten Sie mit folgendem Befehl: "get-help Get-NetAdapter -full".
Geben Sie zum Abrufen der Onlinehilfe Folgendes ein: "get-help Get-NetAdapter -online"

PS C:\Users\fische11\Downloads> Get-NetAdapter -IncludeHidden

Name                               InterfaceDescription          ifIndex Status      MacAddress          LinkSpeed
----                               -
Mobilfunk 6                        Fibocom L850-GL                35 Not Present      0 bps
Mobilfunk                          Fibocom L850-GL                34 Disconnected 9C-9D-83-55-53-42 0 bps
LAN-Verbindung* 4                  WAN Miniport (IKEv2)          33 Disconnected 0 bps
LAN-Verbindung* 10                 WAN Miniport (Network Monitor) 32 Up            0 bps
Mobilfunk 7                        Fibocom L850-GL                31 Not Present      0 bps
Mobilfunk 10                       Fibocom L850-GL                30 Not Present      0 bps
Mobilfunk 8                        Fibocom L850-GL                29 Not Present      0 bps
LAN-Verbindung* 5                  WAN Miniport (L2TP)           28 Disconnected 0 bps
vSwitch (WSL)                     Hyper-V Virtual Switch Extension Ada... 59 Up            10 Gbps
Mobilfunk 14                       Fibocom L850-GL                27 Not Present      0 bps
Bluetooth-Netzwerkverb...         Bluetooth Device (Personal Area Netw... 26 Disconnected 50-E0-85-C0-A3-DB 3 Mbps
WLAN                               Intel(R) Wireless-AC 9560 160MHz      25 Up            300 Mbps
Mobilfunk 11                       Fibocom L850-GL                24 Not Present      0 bps
LAN-Verbindung* 3                  WAN Miniport (SSTP)           23 Disconnected 0 bps
Mobilfunk 16                       Fibocom L850-GL                22 Not Present      0 bps
Mobilfunk 3                        Fibocom L850-GL                21 Not Present      0 bps
Teredo Tunneling Pseud...         20 Not Present      0 bps
Ethernet                           Intel(R) Ethernet Connection (6) I219-V 19 Disconnected 98-FA-9B-D6-8A-CF 0 bps
Mobilfunk 0                       Fibocom L850-GL                18 Not Present      0 bps
```


Get-NetAdapterAdvancedProperty

- Eigenschaften von Netzwerkadaptern anzeigen
 - Interface
 - Eigenschaft
 - Wert
 - Registry-Keyword
 - Registry-Value

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetAdapterAdvancedProperty -IncludeHidden
```

Name	DisplayName	DisplayValue	RegistryKeyword	RegistryValue
Mobilfunk 6	Selective Suspend	Enabled	*SelectiveSu...	{1}
Mobilfunk	Selective Suspend	Enabled	*SelectiveSu...	{1}
Mobilfunk 7	Selective Suspend	Enabled	*SelectiveSu...	{1}
Mobilfunk 10	Selective Suspend	Enabled	*SelectiveSu...	{1}
Mobilfunk 8	Selective Suspend	Enabled	*SelectiveSu...	{1}
Mobilfunk 14	Selective Suspend	Enabled	*SelectiveSu...	{1}
WLAN	Medientrennung beim Aufrech...	Deaktiviert	*DeviceSleep...	{0}
WLAN	Paketzusammenfügung	Aktiviert	*PacketCoale...	{1}
WLAN	ARP-Offload für WoWLAN	Aktiviert	*PMARPOffload	{1}
WLAN	NS-Offload für WoWLAN	Aktiviert	*PMNSOffload	{1}
WLAN	GTK führt Neuverschlüsselun...	Aktiviert	*PMWiFiRekey...	{1}
WLAN	Aktivierung durch Magic Packet	Aktiviert	*WakeOnMagic...	{1}
WLAN	Aktivierung durch Musterübe...	Aktiviert	*WakeOnPattern	{1}
WLAN	Globale Blockierung von BG-...	Nie	BgScanGlobal...	{0}
WLAN	Kanalbreite für 2,4 GHz	Auto	ChannelWidth24	{1}
WLAN	Kanalbreite für 5 GHz	Auto	ChannelWidth52	{1}
WLAN	Schutz f. gemischte Umgebungen	RTS/CTS aktiviert	CtsToItself	{0}
WLAN	Fat Kanal Intolerant	Deaktiviert	FatChannelIn...	{0}
WLAN	Übertragungsleistung	5. Am höchsten	IbssTxPower	{100}
WLAN	Wireless-Modus 802.11n/ac	3. 802.11ac	IEEE11nMode	{2}

Get-NetAdapterHardwareInfo

- Netzwerkhardware auflisten
- Physikalische Interfaces

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetAdapterHardwareInfo

Name                Segment Bus Device Function Slot NumaNode PcieLinkSpeed PcieLinkWidth Version
-----
WLAN                 0     0    20     3                Unknown        0 1.0
Ethernet            0     0    31     6                Unknown

PS C:\Users\fische11\Downloads> Get-NetAdapterHardwareInfo -IncludeHidden

Name                Segment Bus Device Function Slot NumaNode PcieLinkSpeed PcieLinkWidth Version
-----
WLAN                 0     0    20     3                Unknown        0 1.0
Ethernet            0     0    31     6                Unknown
LAN-Verbindung* 1   0     0    20     3                Unknown        0 1.0
LAN-Verbindung* 2   0     0    20     3                Unknown        0 1.0
```

Get-NetAdapterPowerManagement

- Strom Management Features auflisten
- Physikalische Interfaces
- Logische Interfaces (Beispielsweise Hyper-V)

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetAdapterPowerManagement

InterfaceDescription : Fibocom L850-GL
Name                 : Mobilfunk
ArpOffload           : Unsupported
NSOffload            : Unsupported
RsnRekeyOffload      : Unsupported
D0PacketCoalescing  : Unsupported
SelectiveSuspend     : Enabled
DeviceSleepOnDisconnect : Inactive
WakeOnMagicPacket    : Unsupported
WakeOnPattern        : Unsupported

InterfaceDescription : Bluetooth Device (Personal Area Network)
Name                 : Bluetooth-Netzwerkverbindung
ArpOffload           : Unsupported
NSOffload            : Unsupported
RsnRekeyOffload      : Unsupported
D0PacketCoalescing  : Unsupported
SelectiveSuspend     : Unsupported
DeviceSleepOnDisconnect : Inactive
WakeOnMagicPacket    : Unsupported
WakeOnPattern        : Unsupported

InterfaceDescription : Intel(R) Wireless-AC 9560 160MHz
Name                 : WLAN
ArpOffload           : Enabled
NSOffload            : Enabled
RsnRekeyOffload      : Enabled
D0PacketCoalescing  : Enabled
SelectiveSuspend     : Unsupported
DeviceSleepOnDisconnect : Disabled
WakeOnMagicPacket    : Enabled
WakeOnPattern        : Enabled
```

Get-NetAdapterStatistics

- Auflistung von Netzwerk-Adapttern
- Gesendete Bytes
 - Direkt
 - Unicast
- Empfangene Bytes
 - Direkt
 - Unicast

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetAdapterStatistics

Name                               ReceivedBytes ReceivedUnicastPackets SentBytes SentUnicastPackets
----                               -
Mobilfunk                           0                0           0           0
WLAN                                5769578745       6951401     875886064     2615190
Ethernet                             0                0           0           0
vEthernet (WSL)                      1146             0           3016063       0

PS C:\Users\fische11\Downloads> Get-NetAdapterStatistics -IncludeHidden

Name                               ReceivedBytes ReceivedUnicastPackets SentBytes SentUnicastPackets
----                               -
Mobilfunk                           0                0           0           0
WLAN                                5769590646       6951432     875891597     2615221
Ethernet                             0                0           0           0
LAN-Verbindung* 1                   0                0           0           0
LAN-Verbindung* 2                   0                0           0           0
vEthernet (WSL)                      1146             0           3016063       0
```

Get-NetIPAddress

- IP-Adressen anzeigen
 - IPv4
 - IPv6
- Zuordnungstyp
 - Wellknown (IP-Standard)
 - Link (self-assigned)
 - DHCP (DHCP-Server)
 - RouterAdvertisement (IPv6)
 - Other (andere)

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetIPAddress -AddressFamily IPv6

IPAddress      : fe80::c5a5:4979:d55c:e007%61
InterfaceIndex : 61
InterfaceAlias : vEthernet (WSL)
AddressFamily  : IPv6
Type           : Unicast
PrefixLength   : 64
PrefixOrigin   : WellKnown
SuffixOrigin   : Link
AddressState   : Preferred
ValidLifetime  : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource   : False
PolicyStore    : ActiveStore
```

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetIPAddress | Format-Table

ifIndex IPAddress                               PrefixLength PrefixOrigin SuffixOrigin AddressState PolicyStore
-----
61 fe80::c5a5:4979:d55c:e007%61                64 WellKnown Link Preferred ActiveStore
26 fe80::8d2c:3730:c1b7:affc%26                64 WellKnown Link Deprecated ActiveStore
6 fe80::2175:c413:f63a:47bf%6                 64 WellKnown Link Deprecated ActiveStore
15 fe80::5d9e:ba03:de04:4f9d%15                64 WellKnown Link Deprecated ActiveStore
19 fe80::4890:6129:677c:6831%19                64 WellKnown Link Deprecated ActiveStore
34 fe80::5982:9428:48fa:f957%34                64 WellKnown Link Deprecated ActiveStore
25 fe80::543f:b0b:1e9e:d132%25                 64 WellKnown Link Preferred ActiveStore
1 ::1                                           128 WellKnown WellKnown Preferred ActiveStore
61 172.22.16.1                                  20 Manual Manual Preferred ActiveStore
26 169.254.175.252                              16 WellKnown Link Tentative ActiveStore
6 169.254.71.191                                16 WellKnown Link Tentative ActiveStore
15 169.254.79.157                               16 WellKnown Link Tentative ActiveStore
19 169.254.104.49                              16 WellKnown Link Tentative ActiveStore
34 169.254.249.87                              16 WellKnown Link Tentative ActiveStore
25 192.168.2.137                                24 Dhcp Dhcp Preferred ActiveStore
1 127.0.0.1                                     8 WellKnown WellKnown Preferred ActiveStore
```

Get-NetNeighbor

- Bekannte Nachbarn im Netzwerk auflisten
- Geräte im gleichen Subnetz
- IP-Adresse
- MAC-Adresse
- Entspricht ARP-Cache

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetNeighbor

ifIndex IPAddress                               LinkLayerAddress      State      PolicyStore
-----
61 ff02::1:ff74:2cb1                             33-33-FF-74-2C-B1     Permanent ActiveStore
61 ff02::1:ff5c:e007                             33-33-FF-5C-E0-07     Permanent ActiveStore
61 ff02::1:2                                     33-33-00-01-00-02     Permanent ActiveStore
61 ff02::fb                                       33-33-00-00-00-FB     Permanent ActiveStore
61 ff02::16                                       33-33-00-00-00-16     Permanent ActiveStore
61 ff02::2                                       33-33-00-00-00-02     Permanent ActiveStore
61 ff02::1                                       33-33-00-00-00-01     Permanent ActiveStore
61 fe80::224:81ff:fe81:9001                       00-00-00-00-00-00     Unreachable ActiveStore
26 ff02::1:ff74:2cb1                             33-33-FF-74-2C-B1     Permanent ActiveStore
26 ff02::1:3                                     33-33-00-01-00-03     Permanent ActiveStore
26 ff02::1:2                                     33-33-00-01-00-02     Permanent ActiveStore
26 ff02::fb                                       33-33-00-00-00-FB     Permanent ActiveStore
26 ff02::16                                       33-33-00-00-00-16     Permanent ActiveStore
26 ff02::2                                       33-33-00-00-00-02     Permanent ActiveStore
26 fe80::543f:b0b:1e9e:d132                       00-00-00-00-00-00     Unreachable ActiveStore
26 fe80::224:81ff:fe81:9001                       00-00-00-00-00-00     Unreachable ActiveStore
```

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetNeighbor -State Reachable

ifIndex IPAddress                               LinkLayerAddress      State      PolicyStore
-----
25 192.168.2.1                                00-24-81-81-90-01     Reachable  ActiveStore

PS C:\Users\fische11\Downloads> Get-NetNeighbor -State Reachable | Get-NetAdapter

Name                InterfaceDescription      ifIndex Status      MacAddress      LinkSpeed
-----
WLAN                Intel(R) Wireless-AC 9560 160MHz      25 Up           50-E0-85-C0-A3-D7 300 Mbps

PS C:\Users\fische11\Downloads>
```

Get-NetRoute

- Routing-Tabelle auslesen
 - IPv4
 - IPv6
- Metrik (Priorität)

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetRoute

ifIndex DestinationPrefix NextHop RouteMetric ifMetric PolicyStore
-----
61 255.255.255.255/32 0.0.0.0 256 5000 ActiveStore
6 255.255.255.255/32 0.0.0.0 256 25 ActiveStore
15 255.255.255.255/32 0.0.0.0 256 25 ActiveStore
25 255.255.255.255/32 0.0.0.0 256 50 ActiveStore
34 255.255.255.255/32 0.0.0.0 256 25 ActiveStore
26 255.255.255.255/32 0.0.0.0 256 65 ActiveStore
19 255.255.255.255/32 0.0.0.0 256 5 ActiveStore
1 255.255.255.255/32 0.0.0.0 256 75 ActiveStore
```

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetRoute -DestinationPrefix "0.0.0.0/0" | Select-Object -ExpandProperty "NextHop"
192.168.2.1
PS C:\Users\fische11\Downloads> Get-NetRoute -DestinationPrefix ":::/0" | Select-Object -ExpandProperty "NextHop"
fe80::224:81ff:fe81:9001
PS C:\Users\fische11\Downloads>
```

Get-NetRoute

```

Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetRoute

ifIndex DestinationPrefix NextHop RouteMetric ifMetric PolicyStore
-----
61 255.255.255.255/32 0.0.0.0 256 5000 ActiveStore
6 255.255.255.255/32 0.0.0.0 256 25 ActiveStore
15 255.255.255.255/32 0.0.0.0 256 25 ActiveStore
25 255.255.255.255/32 0.0.0.0 256 50 ActiveStore
34 255.255.255.255/32 0.0.0.0 256 25 ActiveStore
26 255.255.255.255/32 0.0.0.0 256 65 ActiveStore
19 255.255.255.255/32 0.0.0.0 256 5 ActiveStore
1 255.255.255.255/32 0.0.0.0 256 75 ActiveStore
61 224.0.0.0/4 0.0.0.0 256 5000 ActiveStore
6 224.0.0.0/4 0.0.0.0 256 25 ActiveStore
15 224.0.0.0/4 0.0.0.0 256 25 ActiveStore
25 224.0.0.0/4 0.0.0.0 256 50 ActiveStore
34 224.0.0.0/4 0.0.0.0 256 25 ActiveStore
26 224.0.0.0/4 0.0.0.0 256 65 ActiveStore
19 224.0.0.0/4 0.0.0.0 256 5 ActiveStore
1 224.0.0.0/4 0.0.0.0 256 75 ActiveStore
25 192.168.2.255/32 0.0.0.0 256 50 ActiveStore
25 192.168.2.137/32 0.0.0.0 256 50 ActiveStore
25 192.168.2.0/24 0.0.0.0 256 50 ActiveStore
61 172.22.31.255/32 0.0.0.0 256 5000 ActiveStore
61 172.22.16.1/32 0.0.0.0 256 5000 ActiveStore
61 172.22.16.0/20 0.0.0.0 256 5000 ActiveStore
1 127.255.255.255/32 0.0.0.0 256 75 ActiveStore
1 127.0.0.1/32 0.0.0.0 256 75 ActiveStore
1 127.0.0.0/8 0.0.0.0 256 75 ActiveStore
25 0.0.0.0/0 192.168.2.1 0 50 ActiveStore
61 ff00::/8 :: 256 5000 ActiveStore
6 ff00::/8 :: 256 25 ActiveStore
15 ff00::/8 :: 256 25 ActiveStore
25 ff00::/8 :: 256 50 ActiveStore
34 ff00::/8 :: 256 25 ActiveStore
26 ff00::/8 :: 256 65 ActiveStore
19 ff00::/8 :: 256 5 ActiveStore
1 ff00::/8 :: 256 75 ActiveStore
61 fe80::c5a5:4979:d55c:e007/128 :: 256 5000 ActiveStore
26 fe80::8d2c:3730:c1b7:affc/128 :: 256 65 ActiveStore
15 fe80::5d9e:ba03:de04:4f9d/128 :: 256 25 ActiveStore
34 fe80::5982:9428:48fa:f957/128 :: 256 25 ActiveStore
25 fe80::543f:b0b:1e9e:d132/128 :: 256 50 ActiveStore
19 fe80::4890:6129:677c:6831/128 :: 256 5 ActiveStore
6 fe80::2175:c413:f63a:47bf/128 :: 256 25 ActiveStore
61 fe80::/64 :: 256 5000 ActiveStore
6 fe80::/64 :: 256 25 ActiveStore
15 fe80::/64 :: 256 25 ActiveStore
25 fe80::/64 :: 256 50 ActiveStore
34 fe80::/64 :: 256 25 ActiveStore
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetRoute -DestinationPrefix "0.0.0.0/0" | Select-Object -ExpandProperty "NextHop"
192.168.2.1
PS C:\Users\fische11\Downloads> Get-NetRoute -DestinationPrefix "::/0" | Select-Object -ExpandProperty "NextHop"
fe80::224:81ff:fe81:9001
PS C:\Users\fische11\Downloads>
  
```


Get-NetTCPConnection

- Auflisten von TCP-Ports
- Listening-Port
- Aktive Verbindungen
- Port-Mapping

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetTCPConnection
```

LocalAddress	LocalPort	RemoteAddress	RemotePort	State	AppliedSetting	OwningProcess
::	49670	::	0	Listen		696
:::1	49669	::	0	Listen		5880
::	49668	::	0	Listen		4320
::	49667	::	0	Listen		2748
::	49666	::	0	Listen		2000
::	49665	::	0	Listen		964
::	49664	::	0	Listen		936
::	445	::	0	Listen		4
::	135	::	0	Listen		1380
0.0.0.0	64342	0.0.0.0	0	Bound		14152
0.0.0.0	60325	0.0.0.0	0	Bound		14132
0.0.0.0	60291	0.0.0.0	0	Bound		24048
0.0.0.0	60052	0.0.0.0	0	Bound		5384

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetTCPConnection -State Established
```

LocalAddress	LocalPort	RemoteAddress	RemotePort	State	AppliedSetting	OwningProcess
192.168.2.137	64342	20.199.120.151	443	Established	Internet	14152
192.168.2.137	60325	18.66.97.118	443	Established	Internet	14132
192.168.2.137	60291	52.112.120.20	443	Established	Internet	24048
127.0.0.1	60052	127.0.0.1	60051	Established	Internet	5384
127.0.0.1	60051	127.0.0.1	60052	Established	Internet	5384
127.0.0.1	60049	127.0.0.1	60048	Established	Internet	20172

Get-NetUDPEndpoint

- UDP-Ports auflisten
 - Local
 - Remote
- IP-Adresse

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetUDPEndpoint

LocalAddress          LocalPort
-----
fe80::c5a5:4979:d55c:e007%61 61100
::1                    61099
fe80::543f:b0b:1e9e:d132%25 61098
::                    56754
::                    51716
::                    51287
::                    5355
::                    5353
::                    4500
fe80::c5a5:4979:d55c:e007%61 1900
fe80::543f:b0b:1e9e:d132%25 1900
::1                    1900
::                    500
127.0.0.1              65505
172.22.16.1            61103
127.0.0.1              61102
192.168.2.137          61101
127.0.0.1              58550
0.0.0.0                56753
0.0.0.0                56752
127.0.0.1              49664
0.0.0.0                5355
0.0.0.0                5353
0.0.0.0                5050
0.0.0.0                4500
192.168.2.137          1900
172.22.16.1            1900
127.0.0.1              1900
0.0.0.0                500
192.168.2.137          138
```

```
Administrator: Windows PowerShell
PS C:\Users\fische11\Downloads> Get-NetUDPEndpoint -LocalAddress 192.168.2.137

LocalAddress          LocalPort
-----
192.168.2.137          61101
192.168.2.137          1900
192.168.2.137          138
192.168.2.137          137
```

Zusammenfassung

Zusammenfassung

Sie kennen nun die Funktion Heimnetzgruppe, sowie die Teilen-Funktion unter Windows 10.

Es wurde das ISO-Modell kurz wiederholt und auf die Schichten 1-3 genauer eingegangen. Dabei wurde eine Protokollübersicht präsentiert und wichtige Protokolle für einen Windows-Client hervorgehoben.

Abschließend wurden Ihnen die verschiedenen Möglichkeiten vorgestellt, Netzwerkkonfigurationen unter Windows auszulesen. Dabei wurden 3 Wege offen gelegt. Diese lauten: graphisch, mit CMD-Befehlen und mit PowerShell-Befehlen.

Auf die wichtigsten Befehle und deren Einsatzmöglichkeiten wurde detailliert eingegangen.

Vielen Dank

Prof. Ronny Bodach

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

T +49 (0) 3727 58-1011

F +49 (0) 3727 58-21011

bodach@hs-mittweida.de

www.cb.hs-mittweida.de

Haus 8 | Richard-Stücklen Bau | Raum 8-205
Am Schwanenteich 6b | 09648 Mittweida



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences

[hs-mittweida.de](https://www.hs-mittweida.de)