

- Nach der Installation der Rechner und dem Einbinden in das Netzwerk müssen Sie in der Lage sein, jederzeit den Status der Netzwerkverbindung zu prüfen



3.6 Netzwerkfunktion der Clients prüfen und warten



Lernfeld 3.6:

Netzwerkfunktion der Clients prüfen und warten

- 3.6.1 Verbindungstests durchführen
- 3.6.2 Namensauflösung prüfen
- 3.6.3 Management und vorbeugende Wartung

- Mit welchen Befehlen lassen sich Verbindungen überprüfen?



3.6.1 Verbindungstests durchführen

Verbindungstests durchführen

PING

- Zum Überprüfen der Erreichbarkeit von Netzwerkteilnehmern
 - Zeigt an, ob eine IP zu erreichen ist
 - und wie lange der Weg hin und wieder zurück dauert
 - Funktioniert in praktisch jedem OS
- Benutzt ICMP (Internet Control Message Protocol)
- **Firewalls können ICMP blockieren!**

```
C:\Users\CTaus>ping google.com

Ping wird ausgeführt für google.com [216.58.214.14] mit 32 Bytes Daten:
Antwort von 216.58.214.14: Bytes=32 Zeit=20ms TTL=112
Antwort von 216.58.214.14: Bytes=32 Zeit=19ms TTL=112
Antwort von 216.58.214.14: Bytes=32 Zeit=21ms TTL=112
Antwort von 216.58.214.14: Bytes=32 Zeit=17ms TTL=112

Ping-Statistik für 216.58.214.14:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 17ms, Maximum = 21ms, Mittelwert = 19ms
```

Ping auf den Namen einer Website:
Man erkennt auch, ob die Namensauflösung funktioniert.

```
C:\Users\CTaus>ping 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=12ms TTL=115
Antwort von 8.8.8.8: Bytes=32 Zeit=10ms TTL=115
Antwort von 8.8.8.8: Bytes=32 Zeit=12ms TTL=115
Antwort von 8.8.8.8: Bytes=32 Zeit=8ms TTL=115

Ping-Statistik für 8.8.8.8:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 8ms, Maximum = 12ms, Mittelwert = 10ms
```

Ping auf die **IP-Adresse** einer Website:
Funktioniert der Ping auf einen Namen nicht, kann man so überprüfen, ob es überhaupt eine Verbindung gibt.

Verbindungstests durchführen

Tracert / traceroute

- Statt wie beim Ping nur die Erreichbarkeit zu prüfen, werden mit diesen Befehlen der gesamte Weg überprüft
 - Windows: tracert
 - Linux: traceroute
- Tracert nutzt ICMP und die TTL
 - Pakete werden mit steigender TTL losgeschickt und melden die letzte Stelle, die sie erreichen
- TTL: Time to Live

```
C:\Users\CTaus>tracert 8.8.8.8

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

 1  <1 ms    <1 ms    <1 ms    fritz.box [192.168.10.1]
 2  15 ms    16 ms    10 ms    ip1f1000fe.dynamic.kabel-deutschland.de [31.16.0.254]
 3  14 ms    12 ms    10 ms    83-169-172-222-isp.superkabel.de [83.169.172.222]
 4  12 ms     9 ms    11 ms    ip5886c385.static.kabel-deutschland.de [88.134.195.133]
 5  13 ms    12 ms    12 ms    145.254.3.88
 6  10 ms    10 ms     8 ms    145.254.2.217
 7  13 ms    10 ms    10 ms    72.14.194.138
 8  14 ms    12 ms    11 ms    216.239.63.21
 9  14 ms    11 ms    11 ms    216.239.49.249
10  10 ms    13 ms     9 ms    dns.google [8.8.8.8]

Ablaufverfolgung beendet.
```

- Im Inter- und häufig auch im Intranet bekommen Computer symbolische Namen
- Damit Computer über diese symbolischen Namen erreichbar sind, muss das DNS funktionieren
- Wie kann überprüft werden, ob dies der Fall ist, oder wo sich der Fehler befindet?



3.6.2 Namensauflösung prüfen

3.6.2 Namensauflösung prüfen

NSLookup

- Kann verwendet werden, um Namen in IP-Adressen und IP-Adressen in Namen aufzulösen
- Zeigt außerdem an, welcher DNS-Server für die Namensauflösung kontaktiert wird und ob dieser erreichbar ist

```
C:\Users\CTaus>nslookup 8.8.8.8
Server:  fritz.box
Address: 192.168.10.1

Name:    dns.google
Address: 8.8.8.8
```

Wo sucht ein Client, nach IP-Adressen?



1. Im eigenen DNS-Cache



2. In der Hosts-Datei

(unter Windows:
C:\Windows\System32\drivers\etc\)



3. Auf dem eingetragenen
DNS-Server



Sollte sich im DNS-Cache ein falscher/veralteter Eintrag befinden, so wird dieser weiterhin genutzt. Mit: **ipconfig /flushdns** leeren Sie den Cache.

- Ein Netzwerk soll natürlich nicht nur nach der Einrichtung funktionieren
- Es soll langfristig und performant seinen Dienst verrichten!
- Das geht nicht ohne Wartung und Management



3.6.3 Management und vorbeugende Wartung

3.6.3 Management und vorbeugende Wartung

Reaktives Management

- Es wird auf auftretende Probleme und Fehler reagiert.
- Beispiel:
 - Jeden Tag wird eine Menge Daten produziert und auf dem Server gespeichert. Plötzlich ist der Festplattenplatz eines Servers voll. Man kann nichts mehr auf dem Server speichern. Eventuell stürzt dabei sogar der Server ab. Schnellstmöglich muss eine weitere Platte eingebaut werden und das System wieder zum Laufen gebracht werden. Das Ganze während der Hauptgeschäftszeit. Wie steht es dann um Datenverlust und Datensicherung?

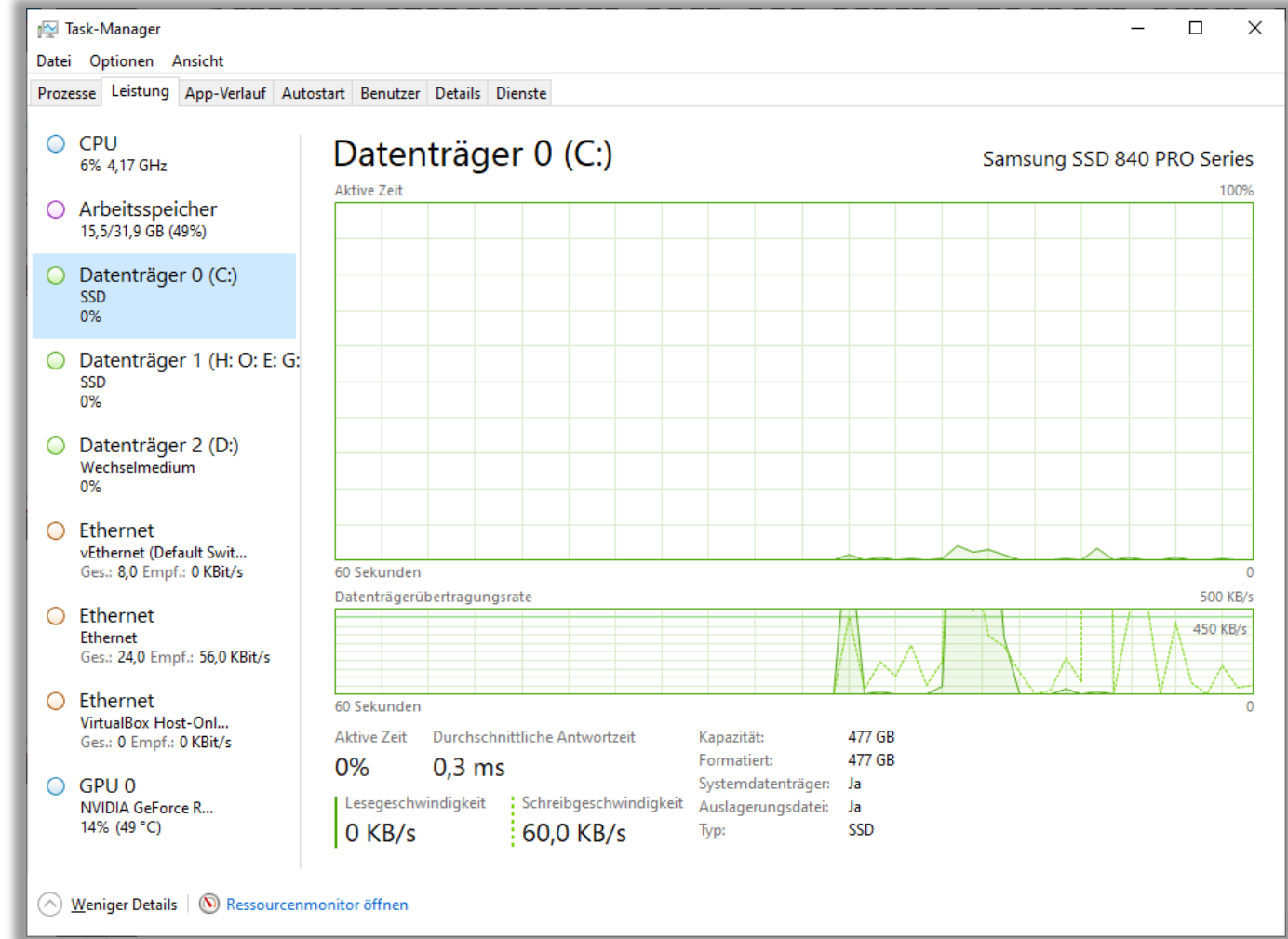
Proaktives Management

- Es wird schon im Vorfeld überwacht und agiert, so das Probleme und Fehler möglichst gar nicht auftreten
- Beispiel:
 - Jeden Tag wird eine bestimmte Menge Daten produziert und auf dem Server gespeichert. Der freie Plattenplatz wird laufend beobachtet. Rechtzeitig, bevor der freie Platz zu Ende geht, wird eine neue Platte beschafft und ins System eingebaut. Die IT-Nutzer bemerken von der Sache gar nichts.

3.6.3 Management und vorbeugende Wartung

Systemüberwachung mit Bordmitteln

- Computersysteme lassen sich mit speziellen Management-Tools überwachen
- Aber auch mit integrierten Systemwerkzeugen
 - z. B. Task-Manager oder Ressourcenmonitor
 - Damit kann man sich schnell einen Überblick über die Auslastung von Clients und Servern verschaffen
 - Wichtig ist es, die Normalwerte zu kennen: **Die Baselines**



**Das Modul ist
geschafft,
das nächste ist nicht
sehr lang!**