7.5 Netzwerk ist langsam

Ein langsames Netzwerk liegt vor, wenn benötigte Daten oder Anwendungen zwar grundsätzlich erreichbar sind, die tatsächliche Leistung jedoch deutlich unter dem vorgesehenen oder bisher üblichen Niveau liegt.

„Langsam“ ist zunächst nur eine subjektive Wahrnehmung. Für eine belastbare Diagnose muss das Verhalten durch Messwerte wie Antwortzeit, Paketverlust, Jitter, Durchsatz, Fehlerzähler oder Serverauslastung beschrieben werden.

Kurzbeschreibung

Die Ursache kann auf unterschiedlichen Ebenen liegen:

- Client oder Netzwerkkarte,
- Kabel, Switchport oder Transceiver,
- WLAN-Verbindung,
- überlasteter Uplink,
- Routingpfad,
- Firewall, VPN oder Proxy,
- WAN- beziehungsweise Internetanbindung,
- fehlerhafte MTU,
- TCP-Wiederholungen,
- Server, Anwendung oder Datenspeicher,
- allgemeine Überlastung zu bestimmten Zeiten.

Ein erfolgreicher Ping beweist lediglich eine grundsätzliche IP-Erreichbarkeit. Er beweist weder einen ausreichenden Datendurchsatz noch eine fehlerfreie Anwendung oder einen leistungsfähigen Server.

Typische Symptome

- Webseiten oder Anwendungen öffnen sich verzögert.
- Dateiübertragungen erreichen nur einen geringen Durchsatz.
- Netzlaufwerke reagieren langsam.
- Remote-Sitzungen stocken.
- Sprache oder Video weisen Aussetzer auf.
- Downloads sind schnell, Uploads jedoch langsam.
- Kleine Dateien funktionieren, große Übertragungen brechen ein.
- Nur WLAN-Clients sind betroffen.
- Nur ein bestimmter Client ist betroffen.
- Mehrere Benutzer sind gleichzeitig betroffen.
- Nur ein Server oder Dienst reagiert langsam.
- Die Störung tritt nur während bestimmter Uhrzeiten auf.

- Die Verbindung beginnt schnell und wird anschließend langsamer.
- Ping funktioniert, die Anwendung benötigt trotzdem lange.
- Über VPN ist die Verbindung langsamer als im lokalen Netzwerk.
- Die Leistung schwankt stark.

Mögliche Auswirkungen

- verlängerte Arbeitsabläufe,
- Abbrüche bei Dateiübertragungen,
- schlechte Sprach- und Videoqualität,
- Zeitüberschreitungen in Anwendungen,
- verzögerte Datenbankabfragen,
- Probleme bei Backups und Synchronisationen,
- unvollständige Softwareverteilung,
- sinkende Produktivität,
- erhöhte Belastung durch wiederholte Übertragungen,
- Ausfall zeitkritischer Dienste.

Sicherheits- und Betriebswarnung

Leistungsprüfungen können selbst erhebliche Netzlast verursachen. Insbesondere `iperf3`, große Dateiübertragungen, parallele Verbindungen und UDP-Tests dürfen nur kontrolliert und autorisiert eingesetzt werden.

Vor Veränderungen müssen dokumentiert werden:

- Ausgangszustand,
- Messzeitpunkt,
- betroffene Systeme,
- aktuelle Konfiguration,
- aktuelle Fehlerzähler,
- bestehende Auslastung,
- verwendeter Testpfad,
- erwarteter Sollwert.

Nicht mehrere Einstellungen gleichzeitig verändern. Sonst lässt sich nicht mehr eindeutig feststellen, welche Änderung das Ergebnis beeinflusst hat.

---

1. Die Aussage „langsam“ messbar machen

Zuerst muss das genaue Verhalten beschrieben werden.

Zu klären sind:

- Welche Anwendung oder Übertragung ist langsam?
- Seit wann besteht die Störung?
- Ist sie dauerhaft oder zeitabhängig?
- Welche Leistung wird erwartet?
- Welche Leistung wird tatsächlich erreicht?
- Betrifft es Upload, Download oder beide Richtungen?
- Sind kleine und große Dateien gleichermaßen betroffen?
- Tritt die Störung lokal, über VPN oder über das Internet auf?
- Besteht das Problem über Ethernet, WLAN oder beide Zugangsarten?
- Funktionierte der gleiche Vorgang früher schneller?
- Existieren ältere Messwerte als Vergleich?

Ungeeignete Beschreibung

```
Das Netzwerk ist langsam.
```

Geeignete Beschreibung

```
Dateiübertragungen vom Client 192.0.2.45 zum Server 192.0.2.80
erreichen seit 14:00 Uhr nur noch etwa 35 Mbit/s.

Bisheriger Vergleichswert: ungefähr 850 Mbit/s
Clientanschluss: 1 Gbit/s Ethernet
Andere Clients: nicht betroffen
Ping zum Server: durchschnittlich 1 ms
```

Erst die zweite Beschreibung ermöglicht eine gezielte Eingrenzung.

---

2. Umfang der Störung bestimmen

Beobachtung	Wahrscheinlicher Prüfbereich
nur ein Client betroffen	Client, Netzwerkkarte, Kabel, Switchport oder lokale Software
alle Clients eines Switches betroffen	Uplink, Switch, VLAN, Spanning Tree oder Überlastung
nur WLAN-Clients betroffen	Funkversorgung, Kanalbelegung, SNR, Access Point oder WLAN-Uplink
alle Clients eines Standorts betroffen	Standort-Uplink, Firewall, Router oder WAN
nur ein Zielserver betroffen	Server, Anwendung, Storage oder Serveranschluss
nur externe Ziele betroffen	Internetanschluss, WAN, Firewall, Proxy oder Provider

Beobachtung	Wahrscheinlicher Prüfbereich
nur VPN-Verkehr betroffen	VPN-Gateway, Verschlüsselungsleistung, MTU oder Tunnelpfad
nur zu bestimmten Uhrzeiten	Backup, Synchronisation, Scan, Update oder planmäßige Last
nur Upload langsam	asymmetrische Auslastung, Rückweg, Duplex, Provider oder Traffic Shaping
nur große Übertragungen langsam	Paketverlust, TCP, MTU, Storage oder Überlastung

Zum Vergleich möglichst denselben Vorgang durchführen:

- auf einem zweiten Client,
- am gleichen Switch,
- an einem anderen Switch,
- über Ethernet statt WLAN,
- innerhalb desselben VLANs,
- zu einem anderen Server,
- ohne VPN, sofern der vorgesehene Test dies erlaubt.

Dabei darf keine Sicherheitskontrolle umgangen werden.

---

3. Sollleistung richtig bestimmen

Die angezeigte Verbindungsgeschwindigkeit ist nicht mit dem nutzbaren Anwendungsdurchsatz gleichzusetzen.

```
Linkgeschwindigkeit ≠ tatsächlicher Datendurchsatz
```

Bei einer Ethernet-Verbindung mit `1 Gbit/s` ist der nutzbare Durchsatz aufgrund von Protokoll- und Verwaltungsdaten geringer. Zusätzlich können beteiligt sein:

- Ethernet-Header,
- IP-Header,
- TCP- oder UDP-Header,
- Verschlüsselung,
- Anwendungsoverhead,
- Dateisystem,
- Storage,
- Latenz,
- Paketverlust,
- konkurrierender Datenverkehr.

Auch Einheiten müssen unterschieden werden:

```
1 Byte = 8 Bit
```

Beispiel:

```
100 MB/s × 8 = 800 Mbit/s
```

Eine Anwendung, die `100 MB/s` anzeigt, überträgt somit ungefähr `800 Mbit/s`, bevor zusätzlicher Protokolloverhead berücksichtigt wird.

---

4. Client und verwendeten Netzwerkadapter prüfen

Unter Windows:

```
Get-NetAdapter |
    Format-Table Name, InterfaceDescription, Status, LinkSpeed, MacAddress
```

Ausführliche IP-Konfiguration:

```
Get-NetIPConfiguration
```

Aktive IP-Adressen:

```
Get-NetIPAddress
```

Unter Linux:

```
ip link show
```

```
ip address show
```

Unter macOS:

```
ifconfig
```

Zu prüfen sind:

- richtiger Netzwerkadapter aktiv,

- erwartete Linkgeschwindigkeit,
- zusätzlicher WLAN- oder Ethernet-Adapter,
- VPN-Adapter,
- virtuelle Netzwerkkarten,
- Dockingstation,
- USB-Netzwerkadapter,
- Bridge,
- Hypervisor oder Containernetzwerk,
- Energiesparzustand,
- aktueller Netzwerkkartentreiber.

Ein Client kann gleichzeitig mehrere aktive Adapter besitzen. Der tatsächlich verwendete Pfad muss anhand von Routingtabelle, Quelladresse und Schnittstelle bestätigt werden.

Unter Windows:

```
Get-NetRoute -AddressFamily IPv4 |
    Sort-Object RouteMetric |
    Format-Table DestinationPrefix, NextHop, InterfaceAlias, RouteMetric
```

---

5. Linkgeschwindigkeit und Duplex prüfen

Unter Windows:

```
Get-NetAdapter |
    Format-Table Name, Status, LinkSpeed
```

Auf Cisco-IOS-/IOS-XE-Switches beispielsweise:

```
show interfaces status
```

Gezielter Port:

```
show interfaces GigabitEthernet1/0/12
```

Zu prüfen sind:

- ausgehandelte Geschwindigkeit,
- Duplexmodus,
- administrative Einstellungen,
- operativer Zustand,

- Übereinstimmung beider Seiten,
- unerwarteter Rückfall auf `100 Mbit/s`,
- Halbduplex statt Vollduplex,
- Link-Flapping.

Typisches Fehlerbild

```
Erwartet: 1 Gbit/s Full Duplex
Tatsächlich: 100 Mbit/s
```

Mögliche Ursachen:

- beschädigtes oder ungeeignetes Kabel,
- fehlerhafte Ader oder Steckverbindung,
- problematische Dockingstation,
- defekter Switchport,
- Transceiverproblem,
- manuell erzwungene Geschwindigkeit,
- fehlerhafte Aushandlung,
- Netzwerkkartentreiber.

Bei einem Duplex-Mismatch können extrem niedrige Leistung, Verbindungsunterbrechungen und Fehlerzähler auftreten.

Geschwindigkeit und Duplex dürfen nicht nur auf einer Seite verändert werden. Beide Seiten müssen kompatibel konfiguriert sein. Normalerweise wird die automatische Aushandlung verwendet, sofern Geräte- und Betriebsvorgaben nichts anderes verlangen.

---

6. Fehler- und Verwerfungszähler prüfen

Unter Windows:

```
Get-NetAdapterStatistics
```

Alle verfügbaren Werte eines Adapters:

```
Get-NetAdapterStatistics -Name "Ethernet" |
    Format-List *
```

Unter Linux:

```
ip -s link show
```

Alternativ, sofern vorhanden:

```
ethtool -S <interface>
```

Auf Cisco-Switches:

```
show interfaces GigabitEthernet1/0/12
```

Kurze Fehlerübersicht:

```
show interfaces counters errors
```

Zu prüfen sind:

- CRC- beziehungsweise FCS-Fehler,
- Input Errors,
- Output Errors,
- Discards,
- Drops,
- Runts,
- Giants,
- Frame Errors,
- Kollisionen,
- Late Collisions,
- Interface Resets,
- Queue Drops.

Bewertung

Zähler	Mögliche Ursache
zunehmende CRC-/FCS-Fehler	Kabel, Stecker, Transceiver oder physische Störung
Late Collisions	möglicher Duplex-Mismatch
Input Discards	Überlastung, Puffer oder Filterung
Output Drops	Ausgangswarteschlange oder überlasteter Folgelink
Interface Resets	instabiler Link, Treiber oder Hardware
Runts oder Giants	fehlerhafte Frames, MTU oder physische Störung
keine Fehler, aber geringe Leistung	Auslastung, TCP, Server, Storage oder Anwendung prüfen

Zähler zuerst dokumentieren und später erneut ablesen.

```
Ausgangswert: 12 CRC-Fehler
Nach 10 Minuten: 12 CRC-Fehler
```

Der Wert ist historisch vorhanden, steigt während des Tests jedoch nicht.

```
Ausgangswert: 12 CRC-Fehler
Nach 10 Minuten: 4.850 CRC-Fehler
```

Der Fehler besteht weiterhin und muss untersucht werden.

---

7. Latenz, Schwankung und Paketverlust messen

Windows:

```
ping <ziel-ip> -n 20
```

Mit festgelegter Paketgröße:

```
ping <ziel-ip> -n 20 -l 1400
```

Linux:

```
ping -c 20 <ziel-ip>
```

macOS:

```
ping -c 20 <ziel-ip>
```

Zu dokumentieren sind:

- Minimum,
- Maximum,
- Durchschnitt,
- Paketverlust,
- starke Abweichungen einzelner Antworten,
- Unterschiede zu einem Referenzwert.

Beispiel

```
Minimum:      1 ms
Maximum:      85 ms
Durchschnitt: 4 ms
Paketverlust: 0 %
```

Der Durchschnitt wirkt niedrig, einzelne starke Ausschläge können für Sprache, Video oder interaktive Anwendungen dennoch relevant sein.

Wichtig

Ein Ping verwendet ICMP. Netzwerkgeräte können ICMP:

- blockieren,
- begrenzen,
- verzögert beantworten,
- niedriger priorisieren.

Paketverlust oder hohe Antwortzeiten an einem einzelnen Zwischenrouter beweisen daher noch keine Störung des weitergeleiteten Nutzverkehrs.

---

8. Stufenweise unterschiedliche Ziele testen

Die Messung sollte vom nahen zum entfernten Ziel erfolgen:

1. eigenes TCP/IP-System,
2. Standardgateway,
3. Ziel im gleichen VLAN,
4. Ziel in einem anderen internen VLAN,
5. interner Server,
6. externes Ziel.

Beispiel:

```
ping <gateway-ip> -n 20
```

```
ping <lokaler-server> -n 20
```

```
ping <entfernter-server> -n 20
```

Bewertung

Gateway	Lokaler Server	Entferntes Ziel	Eingrenzung
langsam	langsam	langsam	Client, Zugang, Switchport oder lokales Netz
schnell	langsam	langsam	interner Pfad ab Gateway oder Servernetz
schnell	schnell	langsam	WAN, Internet, VPN oder entfernter Standort
überall schnell	Anwendung langsam	Anwendung oder Server genauer prüfen	

Verglichen werden müssen Messungen vom selben Client und möglichst zum selben Zeitpunkt.

---

9. Netzwerkpfad ermitteln

Unter Windows:

```
tracert -d <ziel-ip>
```

```
pathping -n <ziel-ip>
```

PowerShell:

```
Test-NetConnection -ComputerName <ziel> -TraceRoute
```

Unter Linux:

```
traceroute -n <ziel-ip>
```

Alternativ, sofern vorhanden:

```
mtr -n <ziel-ip>
```

Unter macOS:

```
traceroute -n <ziel-ip>
```

`pathping` kombiniert eine Pfadermittlung mit wiederholten ICMP-Messungen. Die Ausführung benötigt einige Zeit.

Zu prüfen sind:

- unerwartete Route,
- zusätzlicher VPN- oder Proxy-Pfad,
- ungewöhnlich viele Hops,
- Wechsel des Pfades,
- erhöhte Latenz ab einem bestimmten Segment,
- Unterschiede zwischen funktionierendem und betroffenem Client.

Vorsicht bei der Bewertung

Wenn ein Zwischenrouter ICMP nicht beantwortet, nachfolgende Ziele aber normal erreichbar sind, ist der Zwischenrouter nicht automatisch ausgefallen. Für die Eingrenzung ist entscheidend, ob sich die Verschlechterung bis zum Ziel fortsetzt.

---

10. Tatsächlichen Durchsatz mit `iperf3` messen

`iperf3` misst die erreichbare Netzwerkleistung zwischen einem Server und einem Client. Dadurch lässt sich der reine Netzwerkpfad besser von Dateiablage, Anwendung und Datenträger trennen.

Auf einem autorisierten Testsystem:

```
iperf3 -s
```

Auf dem Client:

```
iperf3 -c <server-ip>
```

Längere Messung:

```
iperf3 -c <server-ip> -t 30
```

Umgekehrte Richtung:

```
iperf3 -c <server-ip> -R
```

Mehrere parallele Datenströme:

```
iperf3 -c <server-ip> -P 4
```

Bidirektionaler Test, sofern von der verwendeten Version unterstützt:

```
iperf3 -c <server-ip> --bidir
```

UDP-Test nur mit kontrollierter Bandbreite:

```
iperf3 -c <server-ip> -u -b 100M -t 20
```

Wichtige Werte

- gemessener Durchsatz,
- Retransmissions bei TCP,
- Paketverlust bei UDP,
- Jitter bei UDP,
- Unterschied zwischen Sende- und Empfangsrichtung,
- Schwankungen zwischen den Messintervallen.

Bewertung

Ergebnis	Eingrenzung
`iperf3` schnell, Dateiübertragung langsam	Serverdienst, Protokoll oder Storage prüfen
`iperf3` ebenfalls langsam	Netzwerkpfad, Client oder Gegenstelle prüfen
normale Richtung schnell, `-R` langsam	richtungsabhängige Störung untersuchen
ein Datenstrom langsam, mehrere schnell	Latenz, TCP-Fenster oder einzelne Flussbegrenzung prüfen
UDP zeigt Verlust oder hohen Jitter	Überlastung, WLAN oder Warteschlangen untersuchen

Mehrere parallele Datenströme können Engpässe verdecken oder zusätzliche Last erzeugen. Sie ersetzen nicht den normalen Einzelstromtest.

Die ESnet-Dokumentation unterstützt `iperf3` offiziell hauptsächlich unter Linux, FreeBSD und macOS. Unter Windows verwendete Builds können von Drittanbietern stammen und müssen gesondert bewertet werden.

---

11. Messung innerhalb einzelner Segmente durchführen

Der End-to-End-Pfad sollte in Abschnitte unterteilt werden.

```
Client
  |
Access-Switch
  |
Distribution-Switch
  |
Firewall oder Router
  |
WAN oder Internet
  |
Zielserver
```

Mögliche Vergleichsmessungen:

```
Client -> lokaler Testserver
Client -> Server im anderen VLAN
Client -> Server hinter der Firewall
Client -> Server am entfernten Standort
```

Beispiel

Testpfad	Ergebnis
Client → lokaler Server	940 Mbit/s
Client → anderes VLAN	925 Mbit/s
Client → Server hinter Firewall	180 Mbit/s
Client → entfernter Standort	175 Mbit/s

Die deutliche Abweichung beginnt im Beispiel am Pfad über die Firewall. Dort sind anschließend Schnittstellen, CPU, Sicherheitsinspektion, VPN und Bandbreitenbegrenzungen zu untersuchen.

---

12. Switchports und Uplinks vergleichen

Auf Cisco-Switches beispielsweise:

```
show interfaces status
```

```
show interfaces counters errors
```

```
show interfaces GigabitEthernet1/0/12
```

Uplink prüfen:

```
show interfaces GigabitEthernet1/0/48
```

Zu prüfen sind:

- Eingangs- und Ausgangsrate,
- Fehlerzähler,
- Drops,
- Queue Drops,
- Linkgeschwindigkeit,
- Duplex,
- Auslastung,
- Zeitpunkt der letzten Statusänderung,
- Uplink mit geringerer Geschwindigkeit als erwartet,
- überbuchter gemeinsamer Uplink.

Beispiel

```
48 Clients mit jeweils 1-Gbit/s-Port
teilen sich einen einzelnen 1-Gbit/s-Uplink.
```

Nicht alle Clients übertragen dauerhaft mit voller Geschwindigkeit. Bei gleichzeitiger hoher Nutzung kann der Uplink jedoch zum Engpass werden.

Ein schneller Access-Port garantiert deshalb keine entsprechend schnelle End-to-End-Verbindung.

---

13. Auslastung und Warteschlangen prüfen

Ein ausgelasteter Link kann folgende Auswirkungen haben:

- steigende Latenz,
- Jitter,
- Paketverlust,
- Output Drops,
- TCP-Wiederholungen,
- schwankenden Durchsatz,
- schlechte Sprach- und Videoqualität.

Zu prüfen sind:

- aktuelle Auslastung,
- Durchschnitt und Spitzenwerte,
- Ein- und Ausgangsrichtung,
- Queue Drops,
- Quality-of-Service-Klassen,
- Traffic Shaping,
- Policing,
- Backups oder Synchronisationen,
- große Softwareverteilungen,
- Cloud-Uploads,
- Kamerastreams,
- replizierende Server.

Eine niedrige Durchschnittsauslastung schließt kurzzeitige Überlastung nicht aus. Sekunden- oder Minutenmittelwerte können kurze Spitzen verdecken.

---

14. Ethernet und WLAN getrennt vergleichen

Wenn ein betroffener Client WLAN verwendet, sollte – sofern vorgesehen und möglich – eine Vergleichsmessung über Ethernet durchgeführt werden.

Ethernet	WLAN	Eingrenzung
schnell	langsam	Funkstrecke, Access Point oder WLAN-Konfiguration
langsam	langsam	gemeinsamer Pfad, Client, Server oder Anwendung
nur ein WLAN-Client langsam	andere WLAN-Clients schnell	Client, Treiber, Frequenzband oder Standort
alle Clients eines Access Points langsam	andere APs schnell	Access Point, Funkkanal oder AP-Uplink

Die reine WLAN-Verbindungsrate ist nicht der tatsächlich nutzbare Durchsatz. WLAN verwendet ein gemeinsam genutztes Funkmedium und enthält zusätzlichen Verwaltungsaufwand.

---

15. WLAN-Signal und Signal-Rausch-Abstand prüfen

Unter Windows:

```
netsh wlan show interfaces
```

Unter macOS können abhängig von Version und verfügbaren Werkzeugen die WLAN-Diagnose oder Systeminformationen verwendet werden.

Zu prüfen sind:

- Signalstärke,
- Signal-Rausch-Abstand beziehungsweise SNR,
- verwendetes Frequenzband,
- Kanal,
- Kanalbreite,
- ausgehandelte Sende- und Empfangsrate,
- Anzahl der Wiederholungen,
- Entfernung zum Access Point,
- Hindernisse,
- Roaming,
- unerwarteter Access Point.

Wichtig

Ein starkes Signal allein beweist keine gute WLAN-Leistung. Auch bei guter Signalstärke können folgende Probleme bestehen:

- hoher Störpegel,
- hohe Kanalauslastung,
- Gleichkanalstörungen,
- überlappende Kanäle,
- viele gleichzeitig aktive Clients,
- langsame Clients mit hohem Airtime-Verbrauch,
- externe Störquellen,
- problematisches Roaming,
- überlasteter Access-Point-Uplink.

---

16. WLAN-Kanalauslastung und Airtime prüfen

WLAN-Clients teilen sich die verfügbare Sendezeit eines Funkkanals. Ein einzelner langsamer oder weit entfernter Client kann für die gleiche Datenmenge mehr Airtime benötigen als ein Client mit hoher Datenrate.

Zu prüfen sind:

- Channel Utilization,
- Anzahl verbundener Clients,
- Retry-Rate,
- Datenraten,
- Airtime-Nutzung,
- Co-Channel Interference,
- Adjacent-Channel Interference,
- Störpegel,
- Kanalbreite,

- Lastverteilung zwischen Access Points,
- Nutzung von 2,4 GHz, 5 GHz oder 6 GHz,
- auffällige Roaming-Ereignisse.

Ein breiterer Kanal erhöht nicht automatisch die Leistung. In einer dicht belegten Umgebung kann eine größere Kanalbreite zusätzliche Überschneidungen und Störungen verursachen.

---

17. Firewall, Router, VPN und Proxy prüfen

Wenn die Leistung erst beim Überschreiten eines bestimmten Netzsegments einbricht, sind beteiligte Netzwerkdienste zu untersuchen.

Zu prüfen sind:

- CPU- und Speicherauslastung,
- Schnittstellenauslastung,
- Paketverluste,
- Session-Anzahl,
- NAT-Tabellen,
- VPN-Verschlüsselungsleistung,
- Deep Packet Inspection,
- Intrusion Prevention,
- Malware-Scan,
- TLS-Inspection,
- Webfilter,
- Proxy-Cache,
- Traffic Shaping,
- Bandbreitenlimits,
- Quality of Service,
- Lizenz- oder Plattformgrenzen.

Vergleich

```
Interner Test ohne Firewallpfad: 930 Mbit/s
Test über Firewall:              210 Mbit/s
```

Dieses Ergebnis weist auf den zusätzlichen Pfad als Prüfbereich hin, beweist aber noch nicht, welche einzelne Funktion die Begrenzung verursacht.

Sicherheitsfunktionen dürfen nicht unkontrolliert deaktiviert werden. Stattdessen sind vorhandene Statistiken, Protokolle, Regelzähler und Herstellerdiagnosen zu verwenden.

---

18. VPN-Leistung untersuchen

Bei langsamen VPN-Verbindungen zusätzlich prüfen:

- Leistung ohne Tunnel im gleichen Ausgangsnetz,
- Round-Trip-Time zum VPN-Gateway,
- Auslastung des VPN-Gateways,
- verwendetes VPN-Protokoll,
- Verschlüsselungsleistung,
- Paketverlust auf dem äußeren Transportpfad,
- MTU und Tunnel-Overhead,
- Split-Tunneling oder Full-Tunneling,
- konkurrierender Verkehr am Client,
- Uploadgeschwindigkeit des Clientanschlusses,
- Rückweg zum Client.

Ein Full-Tunnel kann auch allgemeinen Internetverkehr durch das Unternehmensnetz führen. Dadurch können VPN-Gateway und Standortanbindung zusätzlich belastet werden.

---

19. MTU und Fragmentierung prüfen

Eine fehlerhafte MTU kann dazu führen, dass kleine Pakete funktionieren, während größere Übertragungen langsam sind oder abbrechen.

Windows-Test mit gesetztem „Don’t Fragment“-Bit:

```
ping <ziel-ip> -f -l 1472
```

Bei IPv4 entsprechen `1472 Byte` Nutzdaten zusammen mit `20 Byte` IPv4-Header und `8 Byte` ICMP-Header insgesamt `1500 Byte`.

Wenn das Paket zu groß ist, die Größe schrittweise reduzieren:

```
ping <ziel-ip> -f -l 1400
```

Linux:

```
ping -M do -s 1472 <ziel-ip>
```

Zu prüfen sind:

- MTU des Clients,
- MTU der beteiligten Tunnel,
- VPN-Overhead,
- PPPoE-Overhead,

- ICMP-Meldungen zur notwendigen Fragmentierung,
- Path MTU Discovery,
- MSS-Anpassung,
- große Pakete gegenüber kleinen Paketen.

Wichtig

Ein erfolgreicher Ping mit kleinen Paketen schließt ein MTU-Problem nicht aus.

Die maximal nutzbare Größe darf nicht aus einem einzelnen Test verallgemeinert werden. IPv4, IPv6, Tunnel und verwendete Protokolle besitzen unterschiedliche Header und Anforderungen.

---

20. TCP-Wiederholungen und Empfangsfenster analysieren

Paketverlust führt bei TCP normalerweise zu erneuten Übertragungen. Dadurch sinkt der nutzbare Durchsatz, obwohl die Verbindung nicht vollständig ausfällt.

Wireshark-Anzeigefilter:

```
tcp.analysis.retransmission
```

Weitere mögliche Wiederholungen:

```
tcp.analysis.fast_retransmission
```

```
tcp.analysis.spurious_retransmission
```

Verloren vermutete Segmente:

```
tcp.analysis.lost_segment
```

Empfangsfenster vollständig belegt:

```
tcp.analysis.window_full
```

Empfänger meldet ein Empfangsfenster von null:

```
tcp.analysis.zero_window
```

Alle TCP-Analysehinweise:

```
tcp.analysis.flags
```

Zu prüfen sind:

- Häufigkeit der Wiederholungen,
- Richtung der Wiederholungen,
- zeitlicher Zusammenhang mit Leistungseinbrüchen,
- TCP Zero Window,
- TCP Window Full,
- Out-of-Order-Segmente,
- Round-Trip-Time,
- Verbindungsabbrüche,
- Resets.

Bewertung

Beobachtung	Mögliche Ursache
viele Retransmissions	Paketverlust, Überlastung, WLAN oder fehlerhafter Pfad
Zero Window vom Server	Server oder Anwendung verarbeitet Daten nicht schnell genug
Zero Window vom Client	Client oder Anwendung nimmt Daten nicht schnell genug ab
Window Full	Sender erreicht das angekündigte Empfangsfenster
viele Out-of-Order-Pakete	parallele Pfade, Paketverlust oder Mitschnittposition
TCP Reset	Anwendung, Firewall oder Gegenstelle beendet Verbindung

Wireshark-Analysekennzeichnungen beruhen auf dem beobachteten Mitschnitt. Fehlende Pakete können auch durch die Mitschnittposition, Capture Drops oder Offloading entstehen.

---

21. Paketmitschnitt kontrolliert durchführen

Ein Paketmitschnitt kann zeigen:

- TCP-Verbindungsaufbau,
- Antwortzeiten,
- Wiederholungen,
- Zero Window,
- Resets,
- DNS-Verzögerungen,
- ICMP-Fehlermeldungen,

- Fragmentierung,
- lange Pausen zwischen Anfrage und Antwort.

Beispielhafte Wireshark-Filter:

```
ip.addr == <client-ip> && ip.addr == <server-ip>
```

Nur TCP-Verkehr zwischen zwei Systemen:

```
tcp && ip.addr == <client-ip> && ip.addr == <server-ip>
```

TCP-Analysehinweise:

```
tcp.analysis.flags
```

ICMP-Fehlermeldungen:

```
icmp
```

DNS:

```
dns
```

HTTP-Antwortzeiten müssen im Kontext der Anwendung bewertet werden. Bei verschlüsseltem HTTPS-Verkehr sind Anwendungsinhalte ohne vorgesehene Entschlüsselungsmöglichkeiten nicht sichtbar.

Mitschnitte dürfen nur autorisiert erfolgen. Sie können vertrauliche Inhalte, Adressen, Namen, Sitzungsinformationen oder Anmeldedaten enthalten.

---

22. Netzwerk und Anwendung voneinander trennen

Ein schneller Netzwerktest beweist nicht, dass die Anwendung schnell arbeitet.

Mögliche zusätzliche Verzögerungen:

- langsame DNS-Auflösung,
- verzögerter TLS-Verbindungsaufbau,
- langsame Authentifizierung,
- langsame Datenbankabfrage,

- überlasteter Webserver,
- blockierter Anwendungsthread,
- externer API-Aufruf,
- Virenscanner,
- Dateisperren,
- langsamer Datenträger,
- hohe CPU- oder Speicherauslastung.

Vergleich

```
Ping zum Server:          1 ms
iperf3 zum Server:        930 Mbit/s
Dateiübertragung:         35 MB/s
Anwendung reagiert:       nach 8 Sekunden
```

Das Netzwerk erreicht in diesem Beispiel grundsätzlich einen hohen Durchsatz. Deshalb müssen anschließend Dateiablage, Serverressourcen und Anwendung untersucht werden.

---

23. Serverressourcen prüfen

Unter Windows beispielsweise:

```
Get-Counter '\Processor(_Total)\% Processor Time'
```

```
Get-Counter '\Memory\Available MBytes'
```

Netzwerkadapterstatistik:

```
Get-NetAdapterStatistics
```

Aktuelle TCP-Verbindungen:

```
Get-NetTCPConnection
```

Unter Linux:

```
top
```

```
free -h
```

```
vmstat 1
```

```
iostat -xz 1
```

```
ss -s
```

Zu prüfen sind:

- CPU-Auslastung,
- Speicherdruck,
- Swap-Nutzung,
- Datenträgerlatenz,
- Warteschlangen des Storage,
- Netzwerkauslastung,
- Anzahl der Verbindungen,
- Anwendungslimits,
- Datenbankauslastung,
- Backup- oder Scanprozesse,
- Virtualisierungshost,
- gemeinsam verwendete Ressourcen.

Eine niedrige CPU-Auslastung schließt einen Serverengpass nicht aus. Eine Anwendung kann durch einen einzelnen Thread, Storage, Sperren, Datenbankabfragen oder externe Abhängigkeiten begrenzt sein.

---

24. Storage-Leistung von Netzwerkleistung unterscheiden

Dateiübertragungen werden mindestens durch folgende Komponenten begrenzt:

```
Clientdatenträger
   ↓
Clientnetzwerk
   ↓
Netzwerkpfad
   ↓
Servernetzwerk
   ↓
```

```
Serverdatenträger
```

Der langsamste beteiligte Abschnitt bestimmt die erreichbare Gesamtleistung.

Vergleichsmöglichkeiten

- `iperf3` für den Netzwerkpfad,
- lokale Lese- und Schreibtests nach Betriebsvorgaben,
- Dateiübertragung aus dem Arbeitsspeicher,
- Vergleich mit einem anderen Datenträger,
- Server-Monitoring für Storage-Latenz und Warteschlangen.

Ein schneller `iperf3`-Test und eine langsame Dateiübertragung sprechen dafür, dass nicht allein der Netzwerkpfad begrenzt.

Unkontrollierte Datenträger-Benchmarks dürfen auf Produktivsystemen nicht durchgeführt werden. Sie können erhebliche Last erzeugen und verfügbare Speicherkapazität beeinflussen.

---

25. Zeitabhängige Last untersuchen

Wenn die Störung nur zu bestimmten Zeiten auftritt, prüfen:

- Backups,
- Replikationen,
- Cloud-Synchronisation,
- Softwareverteilung,
- Virenscans,
- Datenbankwartung,
- Patchmanagement,
- Videoüberwachung,
- geplante Exporte,
- Benutzeranmeldungen am Arbeitsbeginn,
- große Downloads oder Uploads,
- Storage-Snapshots,
- WAN-Auslastung,
- Provider- oder Standortauslastung.

Erforderlich ist eine zeitliche Korrelation:

```
14:00 Uhr: Backup startet
14:02 Uhr: Uplink erreicht 98 % Auslastung
14:03 Uhr: Output Drops steigen
14:04 Uhr: Benutzer melden langsame Dateiübertragungen
15:00 Uhr: Backup endet
```

15:02 Uhr: Durchsatz normalisiert sich

Eine zeitliche Übereinstimmung ist ein starker Hinweis, aber noch kein vollständiger Ursachennachweis. Die beteiligten Messwerte müssen gemeinsam bewertet werden.

---

26. Baseline und Vergleichswerte verwenden

Eine Baseline beschreibt den normalen Zustand eines Systems.

Sinnvolle Vergleichswerte:

- Ping-Latenz,
- Jitter,
- Paketverlust,
- `iperf3`-Durchsatz,
- Linkauslastung,
- Fehlerzähler,
- WLAN-SNR,
- WLAN-Kanalauslastung,
- CPU-Auslastung,
- Storage-Latenz,
- Anwendungsantwortzeit,
- Anzahl aktiver Sitzungen.

Beispiel

Messwert	Normalzustand	Störungszeit
RTT zum Server	1–2 ms	25–180 ms
Paketverlust	0 %	3 %
TCP-Durchsatz	920 Mbit/s	85 Mbit/s
Uplink-Auslastung	20–40 %	98 %
Output Drops	0/s	2.500/s

Ohne Vergleichswert ist schwer zu beurteilen, ob ein Messwert tatsächlich ungewöhnlich ist.

---

27. Beispiel für eine systematische Diagnose

Symptom

Mehrere Benutzer melden langsame Zugriffe auf einen Dateiserver.

Sollzustand

```
Clientanschlüsse: 1 Gbit/s
Switch-Uplink:    10 Gbit/s
Serveranschluss:  10 Gbit/s
Normaler TCP-Test: ungefähr 900 Mbit/s je Client
```

Clienttest

```
ping 192.0.2.80 -n 20
```

Ergebnis:

```
Durchschnitt: 2 ms
Paketverlust: 0 %
```

Durchsatztest

```
iperf3 -c 192.0.2.80 -t 30
```

Ergebnis:

```
Durchschnittlicher Durchsatz: 92 Mbit/s
Retransmissions: erhöht
```

Clientport

```
show interfaces GigabitEthernet1/0/12
```

Ergebnis:

```
Full-duplex, 1000 Mb/s
Keine zunehmenden CRC-Fehler
```

Uplinkprüfung

```
show interfaces TenGigabitEthernet1/1/1
```

Ergebnis:

```
Auslastung: 99 %
Output Drops steigen
```

Zeitlicher Vergleich

```
Auslastungsbeginn:  14:00 Uhr
Backupbeginn:       14:00 Uhr
Benutzermeldungen:  ab 14:05 Uhr
```

Festgestellte Ursache

Ein neu eingerichteter Backupauftrag belegte während der Geschäftszeit nahezu die gesamte verfügbare Uplinkkapazität. Dadurch entstanden Warteschlangen, Drops und TCP-Wiederholungen.

Kontrollierte Maßnahme

Der Backupzeitplan und die vorgesehene Bandbreitensteuerung wurden nach betrieblicher Freigabe angepasst.

Rollback

Falls die Änderung unerwartete Auswirkungen verursacht:

- ursprünglichen Zeitplan wiederherstellen,
- ursprüngliche Bandbreitenrichtlinie wiederherstellen,
- Konfiguration erneut prüfen,
- Änderung dokumentieren.

Verifikation

```
iperf3 -c 192.0.2.80 -t 30
```

Ergebnis:

```
Durchschnittlicher Durchsatz: 928 Mbit/s
Retransmissions: keine auffällige Zunahme
```

Zusätzlich:

- Uplink unterhalb der vorgesehenen Auslastungsgrenze,
- keine neuen Output Drops,
- Dateiübertragung wieder im normalen Bereich,

- Anwendungen reagieren normal,
- Benutzer bestätigen die Wiederherstellung.

---

28. Beispiel „Netzwerk schnell, Server langsam“

Symptom

Der Zugriff auf eine Datenbankanwendung benötigt mehrere Sekunden.

Netzwerkprüfung

```
Ping:              1 ms
Paketverlust:      0 %
iperf3:            935 Mbit/s
Interfacefehler:   keine Zunahme
```

Serverprüfung

```
Storage-Latenz: stark erhöht
Datenträgerwarteschlange: stark erhöht
Start eines Sicherungsauftrags: gleicher Zeitpunkt wie Störung
```

Festgestellte Ursache

Der Netzwerkpfad funktionierte normal. Die Anwendung wartete auf den stark ausgelasteten Serverdatenträger.

Lehre

Eine langsame Netzwerkanwendung ist nicht automatisch ein langsames Netzwerk. Netzwerk, Anwendung und Serverressourcen müssen getrennt gemessen werden.

---

29. Ungeeignete Sofortmaßnahmen

Nicht als erste Maßnahme verwenden:

- Switch oder Router ohne Diagnose neu starten,
- Geschwindigkeit oder Duplex nur auf einer Seite erzwingen,
- WLAN-Kanäle wahllos verändern,
- Access Points unkontrolliert neu starten,
- Firewall- oder Sicherheitsprüfung deaktivieren,
- VPN umgehen,

- Quality of Service vollständig entfernen,
- alle Traffic-Limits pauschal aufheben,
- MTU ohne Messung verändern,
- TCP-Einstellungen ohne Baseline ändern,
- Netzwerkkartentreiber ungeprüft ersetzen,
- Fehlerzähler vor der Dokumentation löschen,
- produktive Links mit unkontrolliertem `iperf3` auslasten,
- UDP-Tests ohne Bandbreitenlimit starten,
- ausschließlich einen öffentlichen Speedtest verwenden,
- aus einem einzelnen Ping auf die Gesamtleistung schließen,
- mehrere Änderungen gleichzeitig durchführen.

Solche Maßnahmen können Diagnoseinformationen beseitigen, Sicherheitsgrenzen verändern oder zusätzliche Störungen erzeugen.

---

30. Vollständige Schnellprüfreihenfolge

1. genaue Anwendung und Benutzeraktion ermitteln.
2. erwartete und tatsächliche Leistung dokumentieren.
3. Beginn, Dauer und zeitliches Muster bestimmen.
4. feststellen, ob ein oder mehrere Benutzer betroffen sind.
5. WLAN und Ethernet getrennt betrachten.
6. lokales und entferntes Ziel vergleichen.
7. Upload und Download getrennt prüfen.
8. tatsächlich verwendeten Netzwerkadapter feststellen.
9. Linkgeschwindigkeit und Duplex prüfen.
10. Fehler- und Verwerfungszähler dokumentieren.
11. Gateway, lokales Ziel und entferntes Ziel anpingen.
12. Latenz, Schwankung und Paketverlust vergleichen.
13. tatsächlichen Netzwerkpfad ermitteln.
14. Durchsatz mit einem autorisierten Testsystem messen.
15. beide Übertragungsrichtungen prüfen.
16. Netzwerkpfad in einzelne Segmente unterteilen.
17. Access-Port, Uplink und Serverport prüfen.
18. Auslastung und Warteschlangen untersuchen.
19. WLAN-Signal, SNR, Kanal und Airtime prüfen.
20. Firewall, Router, Proxy und VPN untersuchen.
21. MTU und mögliche Fragmentierungsprobleme prüfen.
22. TCP-Wiederholungen und Empfangsfenster untersuchen.
23. Anwendung und Netzwerk getrennt testen.
24. CPU, Arbeitsspeicher und Storage des Servers prüfen.
25. geplante Backups, Scans und Synchronisationen berücksichtigen.
26. Messwerte mit einer Baseline vergleichen.
27. genau eine Hypothese formulieren.
28. genau eine kontrollierte Änderung durchführen.

29. ursprüngliche Messungen wiederholen.
30. Nebenwirkungen und Sicherheitsfunktionen prüfen.
31. temporäre Diagnoseänderungen entfernen.
32. Ursache, Maßnahme, Rollback und Nachweis dokumentieren.

---

31. Checkliste „Netzwerk ist langsam“

- [ ] subjektive Aussage wurde in Messwerte übersetzt.
- [ ] erwarteter Sollwert ist bekannt.
- [ ] tatsächlicher Istwert wurde dokumentiert.
- [ ] Beginn und zeitliches Muster sind bekannt.
- [ ] Anzahl betroffener Benutzer wurde bestimmt.
- [ ] betroffene Anwendungen wurden bestimmt.
- [ ] Upload und Download wurden getrennt geprüft.
- [ ] WLAN und Ethernet wurden verglichen.
- [ ] lokales und entferntes Ziel wurden verglichen.
- [ ] verwendeter Netzwerkadapter wurde bestätigt.
- [ ] zusätzliche Adapter und VPN-Verbindungen wurden berücksichtigt.
- [ ] Linkgeschwindigkeit wurde geprüft.
- [ ] Duplexmodus wurde geprüft.
- [ ] Clientfehlerzähler wurden dokumentiert.
- [ ] Switchportfehler wurden dokumentiert.
- [ ] CRC-/FCS-Fehler wurden geprüft.
- [ ] Discards und Drops wurden geprüft.
- [ ] Gateway-Latenz wurde gemessen.
- [ ] Latenz zum Ziel wurde gemessen.
- [ ] Paketverlust wurde gemessen.
- [ ] Schwankungen beziehungsweise Jitter wurden berücksichtigt.
- [ ] Netzwerkpfad wurde ermittelt.
- [ ] Durchsatz wurde kontrolliert gemessen.
- [ ] beide Übertragungsrichtungen wurden geprüft.
- [ ] einzelne Netzwerksegmente wurden verglichen.
- [ ] Access-Port wurde geprüft.
- [ ] Uplink wurde geprüft.
- [ ] Serverport wurde geprüft.
- [ ] Auslastung und Warteschlangen wurden geprüft.

- [ ] WLAN-Signal und SNR wurden geprüft.
- [ ] WLAN-Kanalauslastung wurde geprüft.
- [ ] WLAN-Airtime und Retry-Rate wurden berücksichtigt.
- [ ] Firewall und Router wurden geprüft.
- [ ] VPN und Proxy wurden berücksichtigt.
- [ ] Traffic Shaping und Policing wurden geprüft.
- [ ] Quality of Service wurde berücksichtigt.
- [ ] MTU und Fragmentierung wurden geprüft.
- [ ] TCP-Retransmissions wurden berücksichtigt.
- [ ] TCP Window Full und Zero Window wurden berücksichtigt.
- [ ] Server-CPU wurde geprüft.
- [ ] Serverarbeitsspeicher wurde geprüft.
- [ ] Storage-Latenz wurde geprüft.
- [ ] Anwendung wurde getrennt vom Netzwerk getestet.
- [ ] zeitabhängige Prozesse wurden untersucht.
- [ ] Baseline oder Vergleichsmessung wurde verwendet.
- [ ] vor Änderungen wurde der Ausgangszustand gesichert.
- [ ] nur eine kontrollierte Änderung wurde durchgeführt.
- [ ] Rollback wurde festgelegt.
- [ ] ursprüngliche Messungen wurden wiederholt.
- [ ] temporäre Diagnoseänderungen wurden entfernt.
- [ ] Ursache, Maßnahme und Nachweis wurden dokumentiert.

---

32. Schnellreferenz

Ergebnis	Nächster Schritt
nur ein Client langsam	Client, Kabel, Treiber und Switchport prüfen
alle Clients langsam	gemeinsamen Uplink, Firewall, WAN oder Server prüfen
Ethernet schnell, WLAN langsam	Funkstrecke, SNR, Kanal und Airtime prüfen
Gateway bereits langsam	lokalen Zugang und Clientpfad prüfen
Gateway schnell, entferntes Ziel langsam	Routing-, WAN-, VPN- oder Internetpfad prüfen
Link nur mit 100 Mbit/s aktiv	Kabel, Aushandlung, Dock und Port prüfen
zunehmende CRC-Fehler	physischen Übertragungsweg prüfen
Output Drops steigen	nachgelagerten Engpass oder Warteschlange prüfen

Ergebnis	Nächster Schritt
hohe Latenz ohne Paketverlust	Auslastung, Warteschlangen oder entfernten Pfad prüfen
Paketverlust steigt unter Last	Überlastung, WLAN oder physische Fehler prüfen
`iperf3` schnell, Datei langsam	Anwendung, Dateidienst und Storage prüfen
`iperf3` ebenfalls langsam	Netzwerkpfad, Client und Gegenstelle prüfen
nur eine Richtung langsam	richtungsabhängige Auslastung und Rückweg prüfen
viele TCP-Retransmissions	Verlustursache entlang des Pfades suchen
TCP Zero Window vom Server	Server oder Anwendung verarbeitet Daten zu langsam
kleine Pakete funktionieren, große nicht	MTU und Fragmentierung prüfen
nur VPN langsam	Tunnelpfad, MTU und VPN-Gateway prüfen
nur zu bestimmten Zeiten langsam	geplante Last und historische Messwerte vergleichen
Server-Storage stark ausgelastet	Server- und Speicherproblem statt Netzwerkfehler prüfen
öffentlicher Speedtest langsam	Ergebnis durch internen Referenztest eingrenzen
Zwischenhop antwortet nicht	prüfen, ob nachfolgende Hops und Ziel betroffen sind
WLAN-Signal stark, Leistung schlecht	SNR, Störungen, Airtime und Kanalauslastung prüfen

---

Merksatz

> Ein langsames Netzwerk wird nicht durch Gefühl diagnostiziert. Zuerst werden Umfang, Richtung, Latenz, Paketverlust und Durchsatz gemessen. Danach wird der Pfad segmentweise untersucht und eindeutig zwischen Client, WLAN, Netzwerk, Firewall, VPN, Server, Storage und Anwendung getrennt.

Quellen und weiterführende Dokumentation

- Microsoft Learn – Get-NetAdapterStatistics
- Microsoft Learn – Test-NetConnection
- Microsoft Learn – ping
- Microsoft Learn – tracert
- Microsoft Learn – pathping
- ESnet – iperf3 Documentation
- ESnet – Invoking iperf3
- ESnet – iperf3 FAQ
- Cisco – Troubleshoot Switch Port and Interface Problems

- Cisco – Troubleshoot Interface CRC Errors
- Cisco – RF Health and Wireless Troubleshooting
- Cisco – RF Analysis Tools
- Wireshark – TCP Analysis
- Wireshark – TCP Display Filter Reference
- Wireshark – User’s Guide
