6.5 Netzwerk ist langsam – Latenz, Paketverlust und Durchsatz systematisch analysieren

Ein Netzwerk gilt nicht allein deshalb als langsam, weil eine Anwendung verzögert reagiert. Wahrgenommene Langsamkeit kann durch das Netzwerk selbst, den Client, den Server, den Datenträger, eine Anwendung, DNS, einen Proxy, ein VPN, WLAN, Paketverlust oder eine ausgelastete Zwischenkomponente entstehen.

Typische Aussagen wie:

> Das Internet ist langsam.
>
> Der Server reagiert träge.
>
> Der Download dauert zu lange.
>
> Die Verbindung hängt immer wieder.
>
> Das WLAN ist schlecht.

sind zunächst nur Symptombeschreibungen. Für eine belastbare Fehleranalyse muss bestimmt werden:

- was genau langsam ist,
- zwischen welchen Endpunkten gemessen wird,
- ob Latenz, Paketverlust, Jitter oder Durchsatz betroffen sind,
- ob der Fehler dauerhaft oder sporadisch auftritt,
- ob nur ein Client, ein Netzsegment oder alle Benutzer betroffen sind,
- ob das Netzwerk oder eine darüberliegende Anwendung begrenzt.

---

1. Die wichtigsten Messgrößen unterscheiden

Messgröße	Bedeutung	Typische Auswirkung
Latenz	Zeit für die Übertragung zwischen zwei Endpunkten	verzögerte Reaktion, langsamer Sitzungsaufbau
Round-Trip Time	Zeit für Hin- und Rückweg	messbar beispielsweise mit Ping oder TCP-Tests
Paketverlust	Pakete erreichen das Ziel nicht	Wiederholungen, Einbrüche bei TCP, Audio- und Videostörungen
Jitter	Schwankung der Laufzeit	Probleme bei Sprache, Video und Echtzeitanwendungen
Durchsatz	tatsächlich übertragene Datenmenge pro Zeit	langsame Dateiübertragung oder Downloads

Messgröße	Bedeutung	Typische Auswirkung
Bandbreite	theoretisch oder vertraglich verfügbare Kapazität	stellt nur die mögliche Obergrenze dar
Auslastung	aktuell genutzter Anteil einer Verbindung oder Ressource	Warteschlangen, Verzögerungen und Drops
Retransmission	erneute TCP-Übertragung verlorener oder nicht bestätigter Segmente	geringerer Durchsatz und zusätzliche Verzögerung
Queue	wartende Pakete oder Anfragen	steigende Latenz bei hoher Last
Fehlerrate	fehlerhafte Frames, Pakete oder Übertragungen	Paketverlust, Neuübertragungen und Verbindungsabbrüche

Ein Link mit `1 Gbit/s` garantiert keinen Anwendungsdurchsatz von `1 Gbit/s`. Protokoll-Overhead, Latenz, TCP-Verhalten, Datenträgerleistung, Verschlüsselung, Gegenstelle und weitere gleichzeitig übertragene Daten reduzieren den praktisch erreichbaren Wert.

---

2. Langsamkeit exakt beschreiben

Vor jeder technischen Änderung sind folgende Fragen zu beantworten:

- Welche Anwendung oder Übertragung ist langsam?
- Wie lange dauert der Vorgang normalerweise?
- Wie lange dauert er während der Störung?
- Seit wann besteht das Problem?
- Funktionierte es zuvor nachweislich schneller?
- Ist der Fehler dauerhaft, periodisch oder zufällig?
- Sind Download, Upload oder beide Richtungen betroffen?
- Sind kleine Anfragen oder erst große Übertragungen betroffen?
- Tritt die Verzögerung vor dem Verbindungsaufbau oder während der Datenübertragung auf?
- Ist nur ein Benutzer betroffen?
- Sind mehrere Clients im selben VLAN, WLAN oder Standort betroffen?
- Funktioniert ein Vergleichsclient normal?
- Ist die Verbindung per Kabel und WLAN gleichermaßen langsam?
- Sind interne Ziele, externe Ziele oder beide betroffen?
- Ist nur ein bestimmter Server oder sind mehrere Ziele betroffen?
- Wird ein VPN, Proxy, Load Balancer oder Sicherheitsgateway verwendet?
- Gab es unmittelbar zuvor Änderungen, Updates oder Wartungsarbeiten?
- Treten gleichzeitig CPU-, RAM-, Datenträger- oder Anwendungsprobleme auf?

Eine geeignete Ausgangsbeschreibung lautet beispielsweise:

```
Seit 02.08.2026 gegen 09:20 Uhr erreichen Clients im WLAN VLAN 30
beim Kopieren einer 2-GB-Testdatei zum internen Dateiserver nur noch
```

> etwa 8 bis 15 Mbit/s. Über kabelgebundene Clients im VLAN 20 werden zum selben Server etwa 700 Mbit/s erreicht. Kleine Webanfragen und DNS-Auflösungen funktionieren. Betroffen sind mehrere WLAN-Clients.

Diese Beschreibung ist wesentlich aussagekräftiger als:

> Das Netzwerk ist langsam.

---

3. Latenz, Durchsatz und Anwendungsdauer nicht gleichsetzen

Ein Dienst kann sich langsam anfühlen, obwohl der Netzwerkdurchsatz ausreichend ist.

Beispiele:

- eine DNS-Abfrage läuft in einen Timeout,
- ein TLS-Handshake benötigt mehrere Versuche,
- der Server wartet auf eine Datenbank,
- der Datenträger des Servers ist ausgelastet,
- eine Anwendung führt viele aufeinanderfolgende Anfragen aus,
- ein Proxy untersucht den Datenverkehr,
- eine Datei wird serverseitig auf Schadsoftware geprüft,
- eine Anwendung arbeitet nur mit einer einzelnen TCP-Verbindung,
- ein Benutzerprofil oder eine Gruppenrichtlinie verarbeitet viele Dateien,
- der Client besitzt eine hohe CPU- oder Datenträgerauslastung.

Umgekehrt kann eine Anwendung zunächst normal reagieren, während größere Übertragungen wegen Paketverlust, MTU-Problemen oder eines ausgelasteten Links einbrechen.

Deshalb sind mindestens zwei Prüfarten notwendig:

1. kontrollierte Netzwerkmessung,
2. Test der tatsächlich betroffenen Anwendung.

---

4. Umfang der Störung durch Vergleichstests eingrenzen

Vergleich	mögliche Erkenntnis
betroffener gegen funktionierenden Client	lokales Problem oder gemeinsamer Infrastrukturfehler
WLAN gegen Kabel	Funkstrecke, Access Point oder WLAN-Konfiguration
internes gegen externes Ziel	LAN, WAN, Provider oder Internetpfad
Ziel im selben VLAN gegen anderes VLAN	lokales Segment oder gerouteter Pfad
ein Server gegen mehrere Server	Zielsystem oder allgemeiner Netzwerkpfad

Vergleich	mögliche Erkenntnis
IP-Adresse gegen Hostname	DNS oder Namensauflösung
ohne VPN gegen mit VPN	Tunnel, MTU, Gateway oder VPN-Routing
ohne Proxy gegen vorgesehener Proxyweg	Proxy oder Sicherheitsprüfung
Download gegen Upload	richtungsabhängiger Engpass
einzelne gegen mehrere TCP-Verbindungen	TCP, Latenz, Lastverteilung oder Serverbegrenzung
kleine gegen große Übertragung	MTU, Paketverlust, Datenträger oder Durchsatz
aktuelle Messung gegen historische Baseline	tatsächliche Abweichung vom Normalzustand

Bei einem Vergleich sollte möglichst nur eine Variable verändert werden.

---

5. Lokale Clientressourcen ausschließen

Ein langsamer Client kann ein Netzwerkproblem vortäuschen.

Zu prüfen sind:

- CPU-Auslastung,
- Arbeitsspeicher und Paging,
- Datenträgerauslastung und Datenträgerlatenz,
- laufende Updates,
- Backups und Synchronisationsprogramme,
- Virenscanner oder EDR-Prüfungen,
- Browser-Erweiterungen,
- VPN-Client,
- Proxysoftware,
- Netzwerkfiltertreiber,
- fehlerhafter Netzwerkkartentreiber,
- Energiesparmodus,
- thermische Begrenzung,
- sehr viele parallele Verbindungen,
- lokale Anwendung oder lokaler Cache.

Windows

```
Get-Process | Sort-Object CPU -Descending
Get-Counter '\Processor(_Total)\% Processor Time'
Get-Counter '\Memory\Available MBytes'
Get-Counter '\PhysicalDisk(_Total)\Avg. Disk sec/Transfer'
Get-NetAdapter
Get-NetAdapterStatistics
```

Linux

```
top
vmstat 1
free -h
iostat -xz 1
ip -s link
```

macOS

```
top
vm_stat
iostat -w 1
netstat -ib
```

Hohe CPU-, RAM- oder Datenträgerauslastung beweist noch nicht, dass sie die Netzwerkstörung verursacht. Entscheidend ist die zeitliche Übereinstimmung mit der langsamen Übertragung.

---

6. Verbindungstyp und ausgehandelten Link prüfen

Bei Ethernet sind insbesondere zu prüfen:

- Interface aktiv,
- ausgehandelte Geschwindigkeit,
- Duplexmodus,
- automatische Aushandlung,
- Kabel und Steckverbindungen,
- Switchport,
- Dockingstation oder USB-Adapter,
- Treiber und Firmware,
- Fehlerzähler,
- Port-Security,
- VLAN-Zuweisung,
- Energiesparfunktionen.

Ein Client, der statt mit `1 Gbit/s` nur mit `100 Mbit/s` verbunden ist, kann beispielsweise durch ein ungeeignetes oder beschädigtes Kabel, eine fehlerhafte Adernpaarverbindung, einen Adapter oder den Switchport begrenzt sein.

Windows

```
Get-NetAdapter |
    Select-Object Name, InterfaceDescription, Status, LinkSpeed, MacAddress
```

Weitere Eigenschaften:

```
Get-NetAdapterAdvancedProperty -Name "<adaptername>"
Get-NetAdapterStatistics -Name "<adaptername>"
```

Linux

```
ip link show
ip -s link show
sudo ethtool <interface>
sudo ethtool -S <interface>
```

macOS

```
ifconfig <interface>
networksetup -getMedia <netzwerkdienst>
netstat -ib
```

Auf der Switchseite sind je nach Hersteller insbesondere zu prüfen:

- administrativer und operativer Portstatus,
- Geschwindigkeit und Duplex,
- CRC- oder FCS-Fehler,
- Input Errors und Output Errors,
- Drops und Discards,
- Link-Flaps,
- Pause Frames,
- Queue Drops,
- Portauslastung,
- STP-Zustand,
- LACP- oder Port-Channel-Zustand.

Geschwindigkeit, Duplex, Jumbo Frames und Offload-Einstellungen dürfen nicht wahllos verändert werden. Unterschiedliche Einstellungen an beiden Linkpartnern können neue Fehler verursachen.

---

7. Schnittstellenzähler richtig auswerten

Ein einzelner Zählerstand zeigt nicht, wann ein Fehler aufgetreten ist. Zähler müssen vor und während eines kontrollierten Tests verglichen werden.

Beispiel:

```
Zeitpunkt A:
CRC-Fehler: 12
Drops:      41

Zeitpunkt B nach Test:
CRC-Fehler: 438
Drops:      41
```

Die steigende Zahl der CRC-Fehler weist auf ein Problem der physischen Übertragung oder des Links hin. Mögliche Ursachen sind:

- beschädigtes Kabel,
- ungeeignete Verkabelung,
- defekter Stecker,
- fehlerhafter Switchport,
- defekter Netzwerkadapter,
- elektromagnetische Störung,
- Transceiver- oder Glasfaserproblem.

Steigende Drops bei gleichbleibenden CRC-Werten sprechen eher für:

- überfüllte Warteschlange,
- zu hohe Auslastung,
- Microbursts,
- unzureichende Puffer,
- QoS- oder Policing-Regel,
- überlastete CPU einer Netzwerkkomponente.

Hersteller verwenden unterschiedliche Zählerbezeichnungen. Die genaue Bedeutung muss anhand der Dokumentation des eingesetzten Geräts geprüft werden.

---

8. Latenz zunächst kontrolliert messen

Windows

```
ping <ziel>
ping <ziel> -t
```

```
Test-Connection <ziel> -Count 20
Test-NetConnection <ziel>
```

Linux

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

macOS

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

Sinnvolle Ziele für getrennte Messungen:

1. eigenes Standardgateway,
2. Ziel im eigenen VLAN,
3. Ziel in einem anderen internen VLAN,
4. interner Server,
5. VPN-Gateway,
6. externes Ziel,
7. tatsächlich betroffener Anwendungsserver.

Beispielhafte Eingrenzung:

Messung	Ergebnis	mögliche Einordnung
Gateway bereits langsam	lokaler Link, WLAN, Client oder erstes Netzsegment	
Gateway normal, interner Server langsam	Routing, Firewall, Servernetz oder Server	
interne Ziele normal, externe Ziele langsam	WAN, Provider, VPN, Proxy oder externer Pfad	
nur ein Ziel langsam	Zielserver, Zielnetz oder spezifischer Pfad	
nur unter Last langsam	Queue, Auslastung, Bufferbloat oder Ressourcenengpass	

ICMP kann durch Firewalls, Router oder Zielsysteme begrenzt oder niedriger priorisiert werden. Ein verlorenes oder verspätetes Ping-Paket beweist deshalb allein noch keinen Verlust des tatsächlichen Anwendungsverkehrs.

---

9. Paketverlust korrekt untersuchen

Paketverlust kann auftreten:

- zwischen Client und Switch,
- auf einer WLAN-Funkstrecke,
- auf einem überlasteten Uplink,
- in einer Firewall,
- an einem Router,
- in einem VPN-Tunnel,
- auf dem WAN- oder Providerpfad,
- auf dem Serverinterface,
- innerhalb eines virtualisierten Netzwerks.

Windows

```
ping <ziel> -n 100
pathping <ziel>
```

Linux

```
ping -c 100 <ziel>
mtr <ziel>
```

macOS

```
ping -c 100 <ziel>
traceroute <ziel>
```

Bei `pathping`, `mtr` und ähnlichen Werkzeugen darf ein scheinbarer Verlust an einem Zwischenhop nicht automatisch als Fehler dieses Routers bewertet werden. Ein Router kann Antworten auf Diagnosepakete begrenzen, während er Transitverkehr weiterhin normal weiterleitet.

Bedeutsamer ist ein Verlust, wenn:

- er ab einem Hop beginnt und an allen folgenden Hops bestehen bleibt,
- er gleichzeitig in Ende-zu-Ende-Messungen auftritt,
- Interfacezähler oder Paketaufzeichnungen ihn bestätigen,
- der tatsächliche Anwendungsverkehr Wiederholungen oder Abbrüche zeigt.

---

10. Pfad und Richtungsunterschiede untersuchen

Windows

```
tracert <ziel>
Test-NetConnection <ziel> -TraceRoute
Get-NetRoute
```

Linux

```
traceroute <ziel>
tracepath <ziel>
ip route
ip route get <ziel>
```

macOS

```
traceroute <ziel>
netstat -rn
route -n get <ziel>
```

Zu prüfen sind:

- Hinweg vom Client zum Ziel,
- Rückweg vom Ziel zum Client,
- unerwartete Umwege,
- VPN-Routen,
- Policy-Based Routing,
- asymmetrisches Routing,
- geänderte Gateways,
- überlappende Netze,
- unterschiedliche IPv4- und IPv6-Pfade,
- Load Balancer oder mehrere Zieladressen.

Ein klassischer Traceroute zeigt normalerweise nur den beobachteten Hinweg. Der Rückweg kann anders verlaufen und muss gegebenenfalls von der Gegenstelle aus untersucht werden.

---

11. Durchsatz mit einer kontrollierten Gegenstelle messen

Für eine kontrollierte Ende-zu-Ende-Messung kann `iperf3` verwendet werden. Dabei werden Client und Server benötigt.

Server starten

```
iperf3 -s
```

Clienttest

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

Gegenrichtung testen

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

Längerer Test

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

Mehrere parallele Datenströme

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

UDP-Test mit kontrollierter Zielrate

```
iperf3 -c <server-ip> -u -b <rate> -t 30
```

Dabei sind zu dokumentieren:

- Client und Server,
- beide IP-Adressen,
- Netzpfad,
- Datum und Uhrzeit,
- TCP oder UDP,
- Testdauer,
- Anzahl paralleler Datenströme,
- Hin- oder Rückrichtung,
- gemessener Durchsatz,
- gemeldete Wiederholungen,
- bei UDP zusätzlich Verlust und Jitter,
- gleichzeitige Auslastung anderer Verbindungen.

Wichtige Einschränkungen:

- Das Ergebnis gilt nur für den Pfad zwischen den beiden Testendpunkten.

- Der `iperf3`-Server muss autorisiert und kontrolliert betrieben werden.
- Ein Test kann produktive Links stark auslasten.
- UDP-Tests können bei ungeeigneter Zielrate erhebliche Paketverluste verursachen.
- Mehrere parallele Verbindungen können einen höheren Gesamtdurchsatz erreichen als eine einzelne Verbindung.
- Ein erfolgreicher `iperf3`-Test beweist nicht, dass DNS, TLS, Proxy oder Anwendung funktionieren.
- Das iperf3-Projekt unterstützt offiziell Linux, FreeBSD und macOS; Windows-Builds stammen häufig aus anderen Quellen und sind nicht Teil der offiziellen Plattformunterstützung des Projekts.

Tests in produktiven Netzen müssen zeitlich, räumlich und in ihrer Bandbreite begrenzt werden.

---

12. Dateitransfer nicht ungeprüft als Netzwerkbenchmark verwenden

Eine Dateiübertragung misst nicht ausschließlich das Netzwerk. Das Ergebnis kann begrenzt werden durch:

- Quelldatenträger,
- Zieldatenträger,
- Dateisystem,
- SMB, NFS, SFTP oder HTTPS,
- Verschlüsselung,
- Kompression,
- Virenscanner,
- viele kleine Dateien,
- Server-CPU,
- Client-CPU,
- Berechtigungsprüfung,
- Protokollsignierung,
- Backup oder Snapshot,
- Cache.

Sinnvolle Vergleichstests:

- große einzelne Datei gegen viele kleine Dateien,
- Speicher-zu-Speicher-Test gegen Datenträgerübertragung,
- kontrollierter Netzwerkdurchsatz gegen Anwendungsübertragung,
- derselbe Client zu einem anderen Server,
- ein anderer Client zum selben Server,
- Lesen gegen Schreiben.

Wenn `iperf3` einen normalen Netzwerkdurchsatz zeigt, die Dateiübertragung aber langsam bleibt, verschiebt sich die Untersuchung auf Protokoll, Datenträger, Server und Anwendung.

---

13. WLAN getrennt vom kabelgebundenen Netz prüfen

WLAN ist ein gemeinsam genutztes Funkmedium. Die angezeigte WLAN-Verbindungsrate entspricht nicht dem tatsächlich erreichbaren Nutzdurchsatz.

Zu prüfen sind:

- Signalstärke,
- Signal-Rausch-Verhältnis,
- verwendetes Frequenzband,
- Kanal,
- Kanalbreite,
- Kanalauslastung,
- Störungen,
- Anzahl gleichzeitig aktiver Clients,
- Airtime-Auslastung,
- Wiederholungsrate,
- Datenrate,
- Roaming,
- Access-Point-Auslastung,
- Uplink des Access Points,
- PoE-Versorgung,
- Treiber und Firmware,
- Entfernung und Hindernisse,
- Hidden-Node-Probleme,
- Band Steering,
- Mindestdatenraten,
- WLAN-Sicherheitsverfahren.

Windows

```
netsh wlan show interfaces
netsh wlan show drivers
netsh wlan show wlanreport
```

Linux

```
iw dev
iw dev <interface> link
nmcli device wifi list
```

macOS

Auf macOS können die WLAN-Diagnose, die Systeminformationen sowie je nach Systemversion verfügbare Diagnosewerkzeuge verwendet werden. Die genaue Bedienung kann sich zwischen macOS-Versionen ändern.

Wichtige Vergleichstests:

1. betroffener Client am aktuellen Standort,
2. derselbe Client näher am Access Point,
3. derselbe Client per Ethernet,
4. anderer Client am selben Standort,
5. anderer Access Point oder anderes Frequenzband,
6. Messung bei geringer und hoher Auslastung.

Wenn der kabelgebundene Test normal und der WLAN-Test langsam ist, liegt die Ursache nicht automatisch am Access Point. Auch Clienttreiber, Funkumgebung, Kanalplanung, Airtime und Roaming müssen geprüft werden.

---

14. Auslastung, Warteschlangen und Bufferbloat

Ein Link kann unter geringer Last gute Latenzwerte und unter hoher Last starke Verzögerungen zeigen.

Beispiel:

```
ohne Übertragung:
Round-Trip Time zum Gateway: 2 ms

während eines Uploads:
Round-Trip Time zum Gateway: 180 ms
```

Mögliche Ursachen:

- ausgelasteter Uplink,
- zu große Warteschlangen,
- fehlende oder ungeeignete QoS-Regeln,
- Upload begrenzt Rückverkehr und Bestätigungen,
- Firewall oder Router erreicht Leistungsgrenze,
- VPN-Gateway ist ausgelastet,
- WLAN-Airtime ist erschöpft,
- Microbursts füllen einen Puffer,
- Policer verwirft Pakete.

Zu vergleichen sind:

- Latenz ohne Last,
- Latenz während Download,
- Latenz während Upload,
- Paketverlust,
- Interfaceauslastung,
- Queue Drops,
- CPU der Netzwerkkomponente,
- Anzahl aktiver Verbindungen.

Eine hohe nominale Bandbreite verhindert solche Probleme nicht automatisch. Entscheidend sind Engpass, Warteschlangen und Lastverteilung entlang des vollständigen Pfades.

---

15. Duplex-, Speed- und Aushandlungsfehler

Ein Duplexproblem kann folgende Symptome verursachen:

- geringer Durchsatz,
- stark schwankende Übertragungsrate,
- Framefehler,
- Kollisionen oder späte Kollisionen bei älteren Ethernet-Szenarien,
- viele Wiederholungen,
- gute Werte ohne Last und schlechte Werte unter Last.

Zu prüfen sind beide Linkpartner:

```
Clientinterface ↔ Switchport
Serverinterface ↔ Switchport
Switch-Uplink ↔ Gegenstelle
Firewallinterface ↔ Switchport
```

Die Konfiguration muss zusammenpassen. Einseitiges Erzwingen von Geschwindigkeit oder Duplex kann einen Mismatch erzeugen.

Bei modernen Gigabit-Ethernet-Verbindungen wird normalerweise automatische Aushandlung verwendet. Abweichungen dürfen nur entsprechend der Hardware- und Herstelleranforderungen konfiguriert werden.

---

16. MTU und Fragmentierung prüfen

MTU-Probleme können auftreten, obwohl Ping und kleine Anfragen funktionieren.

Typische Symptome:

- kleine Webseiten funktionieren,

- größere Antworten bleiben hängen,
- Dateiübertragungen brechen ab,
- VPN-Verbindungen sind langsam,
- TLS-Handshakes scheitern oder verzögern sich,
- bestimmte Ziele funktionieren, andere nicht,
- viele TCP-Wiederholungen,
- Anwendungen warten bis zu einem Timeout.

Windows

```
ping <ziel> -f -l <paketgröße>
```

Linux

```
tracepath <ziel>
ping -M do -s <paketgröße> <ziel>
```

Die Nutzdatenlänge eines Pingpakets ist nicht mit der vollständigen IP-Paketgröße gleichzusetzen. IP- und ICMP-Header müssen berücksichtigt werden.

Zu prüfen sind:

- MTU des Clients,
- MTU des Servers,
- VLAN- und Tunnel-Overhead,
- VPN,
- PPPoE,
- VXLAN oder andere Kapselung,
- Jumbo Frames,
- Path MTU Discovery,
- blockierte ICMP-Fehlermeldungen,
- MSS-Anpassung.

Jumbo Frames dürfen nur verwendet werden, wenn der vollständige vorgesehene Pfad sie unterstützt. Eine Änderung ausschließlich an einem Endgerät ist keine geeignete Lösung.

---

17. TCP-Wiederholungen und Empfangsfenster untersuchen

TCP passt seine Übertragung an den Zustand des Datenpfades an. Paketverlust, hohe Laufzeit oder ein begrenztes Empfangsfenster können den Durchsatz stark reduzieren.

Mögliche Beobachtungen:

- Retransmissions,

- Duplicate Acknowledgements,
- Out-of-Order-Segmente,
- Zero Window,
- Window Full,
- lange Abstände zwischen Anfrage und Antwort,
- wiederholter Verbindungsaufbau,
- Reset,
- stark unterschiedlicher Durchsatz je Richtung.

Wireshark-Filter

```
tcp.analysis.retransmission
tcp.analysis.fast_retransmission
tcp.analysis.spurious_retransmission
tcp.analysis.duplicate_ack
tcp.analysis.out_of_order
tcp.analysis.lost_segment
tcp.analysis.window_full
tcp.analysis.zero_window
tcp.analysis.zero_window_probe
tcp.flags.reset == 1
```

Mögliche Einordnung:

Beobachtung	mögliche Ursache
viele Retransmissions	Paketverlust, Überlastung, physischer Fehler oder Datenpfad
Duplicate ACKs	fehlende oder verspätete Segmente
Out-of-Order	unterschiedliche Pfade, Reordering oder Aufzeichnungsartefakt
Zero Window	Empfänger verarbeitet Daten nicht schnell genug
Window Full	ausgeschöpftes angekündigtes Empfangsfenster
wiederholte RST-Pakete	Anwendung, Firewall, Proxy oder Betriebssystem
lange Zeit bis zum ersten Datenpaket	Anwendung, DNS, TLS, Proxy oder Server
schnelle Pakete, aber lange Anwendungspausen	Anwendung oder Backend statt Transport

Wireshark-Kennzeichnungen beruhen auf der im Mitschnitt sichtbaren Paketreihenfolge. Ein unvollständiger Mitschnitt, Paketverlust bei der Aufzeichnung oder NIC-Offloading kann die Interpretation beeinflussen.

---

18. Paketaufzeichnung an mehreren Punkten

Wenn die Ursache nicht eindeutig ist, kann eine autorisierte Paketaufzeichnung an mehreren Stellen helfen.

Geeignete Punkte:

- betroffener Client,
- funktionierender Vergleichsclient,
- Server,
- vor und hinter einer Firewall,
- Switch Mirror Port,
- VPN-Endpunkt,
- Reverse Proxy,
- Load Balancer.

Zu prüfen sind:

- Zeit bis zur DNS-Antwort,
- Zeit bis zum TCP-Verbindungsaufbau,
- Zeit bis zum TLS-Handshake,
- Zeit bis zur ersten Anwendungsantwort,
- Paketverlust,
- Wiederholungen,
- Fenstergrößen,
- Reset-Pakete,
- ICMP-Fehlermeldungen,
- verwendete IP-Adresse,
- IPv4 oder IPv6,
- tatsächlicher Datenpfad.

Ein Mitschnitt nur auf dem Client zeigt nicht sicher, an welcher Zwischenstelle ein Paket verloren ging. Vergleichsmitschnitte an Client und Server können zeigen:

```
Paket verlässt den Client, erreicht aber den Server nicht.
```

oder:

```
Server sendet die Antwort, Client empfängt sie nicht.
```

Paketaufzeichnungen dürfen nur mit entsprechender Berechtigung erstellt und müssen geschützt gespeichert werden.

---

19. IPv4 und IPv6 getrennt vergleichen

Ein Client kann IPv6 bevorzugen, obwohl der IPv6-Pfad langsam oder fehlerhaft ist.

Windows

```
Resolve-DnsName <zielname> -Type A
Resolve-DnsName <zielname> -Type AAAA
Test-Connection <ipv4-adresse>
Test-Connection <ipv6-adresse>
```

Linux und macOS

```
ping -4 <zielname>
ping -6 <zielname>
curl -4 -v https://<zielname>/
curl -6 -v https://<zielname>/
```

Mögliche Ursachen:

- unterschiedliche Routen,
- falscher AAAA-Record,
- IPv6-Firewallregel,
- fehlerhafte IPv6-Rückroute,
- Tunnel für eine Adressfamilie,
- unterschiedliche Proxys oder Gateways,
- Dienst antwortet nur über eine Adressfamilie zuverlässig.

IPv6 sollte nicht pauschal deaktiviert werden. Zuerst ist nachzuweisen, welche Adressfamilie betroffen ist.

---

20. DNS, Proxy, TLS und Anwendungslatenz abgrenzen

DNS-Zeit prüfen

```
dig <zielname>
```

Mit `curl` können einzelne Zeitabschnitte gemessen werden:

```
curl -sS -o /dev/null \
  -w 'DNS: %{time_namelookup}\nTCP: %{time_connect}\nTLS: %{time_appconnect}\nErstes Byte:
%{time_starttransfer}\nGesamt: %{time_total}\n' \
```

```
https://<zielname>/
```

Bedeutung:

Wert	untersuchter Bereich
`time_namelookup`	Namensauflösung
`time_connect`	Zeit bis zum TCP-Verbindungsaufbau
`time_appconnect`	Zeit bis zum Abschluss von TLS
`time_starttransfer`	Zeit bis zum ersten empfangenen Byte
`time_total`	gesamte Übertragungsdauer

Mögliche Einordnung:

- DNS langsam, TCP normal: Resolver oder DNS-Pfad,
- TCP-Verbindungsaufbau langsam: Netzwerkpfad, Paketverlust oder Ziel,
- TLS langsam: Zertifikatsprüfung, TLS-Inspection oder Server,
- erstes Byte langsam: Anwendung, Proxy, Backend oder Datenbank,
- erstes Byte schnell, Übertragung langsam: Durchsatz, Paketverlust oder Serverausgabe.

Ein einzelner Messwert reicht nicht aus. Messungen sollten wiederholt und mit einem funktionierenden Vergleich verglichen werden.

---

21. VPN und Tunnel berücksichtigen

VPN-Verbindungen erzeugen zusätzliche Netzwerkschichten.

Mögliche Ursachen:

- Tunnel-Overhead,
- ungeeignete MTU,
- fehlende MSS-Anpassung,
- VPN-Gateway ausgelastet,
- Verschlüsselung begrenzt CPU,
- Full Tunnel leitet unnötigen Datenverkehr um,
- Split-Tunnel-Regel fehlt,
- DNS wird über einen entfernten Standort geleitet,
- asymmetrisches Routing,
- Paketverlust auf dem Transportpfad,
- wechselnder Zugang zwischen WLAN und Mobilfunk,
- Sicherheitsprüfung im VPN-Gateway.

Sinnvolle Vergleichstests:

1. ohne VPN zu einem zulässigen Vergleichsziel,
2. mit VPN zum selben zulässigen Ziel,
3. internes Ziel über VPN,
4. externes Ziel bei Full Tunnel,
5. IPv4 und IPv6,
6. Download und Upload,
7. Latenz zum VPN-Gateway und zum Endziel.

Ein langsamer Test über VPN beweist nicht automatisch, dass das VPN-Gateway die Ursache ist. Auch der lokale Internetzugang und der Pfad zum Gateway müssen geprüft werden.

---

22. Firewalls, Proxys und Sicherheitskomponenten

Sicherheitskomponenten können den Datenverkehr nicht nur erlauben oder blockieren, sondern auch verarbeiten.

Mögliche Einflussfaktoren:

- TLS-Inspection,
- Virenprüfung,
- Intrusion Prevention,
- URL-Filter,
- Data Loss Prevention,
- Proxy-Caching,
- Bandbreitenbegrenzung,
- QoS- oder Policing-Regel,
- hohe Sitzungsanzahl,
- ausgelastete CPU,
- voller Arbeitsspeicher,
- überlastete Protokollierung,
- Cluster-Failover,
- fehlerhafte Lastverteilung.

Zu prüfen sind:

- Interfaceauslastung,
- CPU und Arbeitsspeicher,
- Sitzungstabelle,
- Paket- und Fehlerzähler,
- Queue Drops,
- aktive Sicherheitsprofile,
- Protokolle zum Störungszeitpunkt,
- HA-Zustand,
- Lizenz- oder Kapazitätsgrenzen,
- Unterschiede zwischen untersuchten Anwendungen.

Sicherheitsfunktionen dürfen nicht pauschal deaktiviert werden. Tests müssen genehmigt, zeitlich begrenzt und auf eine konkrete Kommunikationsbeziehung beschränkt sein.

---

23. Server und Anwendung als Engpass prüfen

Auch bei fehlerfreiem Netzwerk kann der Zielserver den Durchsatz begrenzen.

Zu prüfen sind:

- CPU pro Prozess und Thread,
- Arbeitsspeicher,
- Paging oder Swapping,
- Datenträgerlatenz,
- I/O-Wait,
- Queue Depth,
- Netzwerkinterface,
- offene Verbindungen,
- Connection Pools,
- Datenbanklocks,
- Anwendungswarteschlangen,
- parallele Backups,
- Virenscanner,
- Snapshots,
- Hypervisorauslastung,
- Storage-Netzwerk,
- Load Balancer,
- Backend-Abhängigkeiten.

Typisches Muster:

```
iperf3 zum Server: normal
Dateiübertragung: langsam
Server-Datenträger: dauerhaft ausgelastet
```

In diesem Fall ist ein Netzwerkengpass nicht nachgewiesen. Die Untersuchung muss auf Datenträger, Protokoll und Server fortgesetzt werden.

---

24. Virtualisierung und Container

Zusätzliche Ursachen bei virtuellen Systemen:

- virtuelle Netzwerkkarte begrenzt,
- vSwitch oder Bridge ausgelastet,
- falsches VLAN Tagging,

- Host-Uplink überlastet,
- NIC Teaming oder Bonding fehlerhaft,
- CPU-Steal oder CPU Ready,
- Host Memory Pressure,
- Storage-Latenz,
- Sicherheitsgruppe oder virtuelle Firewall,
- Overlay-Netzwerk,
- Container-NAT,
- Service Mesh,
- Reverse Proxy,
- Host-Portzuordnung,
- fehlerhafte MTU innerhalb des Overlays.

Die Prüfung sollte folgende Ebenen unterscheiden:

```
Anwendung
↓
Container oder virtuelle Maschine
↓
virtuelles Interface
↓
virtueller Switch oder Bridge
↓
Hostinterface
↓
physischer Switch
↓
weiterer Netzwerkpfad
```

Ein unauffälliger Zähler innerhalb der virtuellen Maschine schließt Fehler auf dem Host-Uplink nicht aus.

---

25. Sporadische Langsamkeit erfassen

Bei sporadischen Fehlern reichen manuelle Einzeltests häufig nicht aus.

PowerShell

```
1..30 | ForEach-Object {
    $time = Get-Date -Format "yyyy-MM-dd HH:mm:ss"
    $result = Test-Connection <ziel> -Count 1 -ErrorAction SilentlyContinue
```

```
    [PSCustomObject]@{
        Time   = $time
        Status = if ($result) { "Erfolg" } else { "Fehler" }
        RTTms  = if ($result) { $result.Latency } else { $null }
    }
    Start-Sleep -Seconds 10
}
```

Abhängig von der verwendeten PowerShell-Version können Eigenschaften des zurückgegebenen Objekts abweichen und müssen vor einer automatisierten Auswertung geprüft werden.

Bash

```
for i in {1..30}; do
    date '+%Y-%m-%d %H:%M:%S'
    ping -c 1 <ziel>
    sleep 10
done
```

Zusätzlich zu erfassen sind:

- Interfacezähler,
- Link-Flaps,
- Switchportstatus,
- WLAN-Roaming,
- Kanal- und Airtime-Auslastung,
- CPU und RAM,
- Datenträgerlatenz,
- Firewall-Sitzungsanzahl,
- geplante Backups,
- Updates,
- Scans,
- Cronjobs oder Timer,
- Providerereignisse,
- Temperatur und Stromversorgung.

Alle Systeme müssen möglichst einheitlich synchronisierte Zeit verwenden, damit Ereignisse auf einer gemeinsamen Zeitleiste verglichen werden können.

---

26. Praxisfall A: Nur ein Client ist langsam

Symptom

- ein Client überträgt mit etwa 90 Mbit/s,
- andere Clients am selben Switch erreichen wesentlich höhere Werte,
- Server und Anwendung sind für andere Benutzer normal,
- der betroffene Client zeigt eine Linkgeschwindigkeit von `100 Mbit/s`.

Prüfung

1. Linkgeschwindigkeit dokumentieren.
2. Netzwerkkartenstatistik prüfen.
3. Kabel und Switchport kontrollieren.
4. Client mit bekannt funktionierendem Kabel testen.
5. denselben Switchport mit einem Vergleichsclient testen.
6. Treiber und Adapter prüfen.
7. kontrollierten Durchsatztest wiederholen.

Mögliche Ursache

Das Netzwerkkabel besitzt eine fehlerhafte Adernpaarverbindung. Deshalb wird nur Fast Ethernet statt Gigabit Ethernet ausgehandelt.

Nachprüfung

- Link wird mit der vorgesehenen Geschwindigkeit ausgehandelt,
- Fehlerzähler steigen nicht,
- kontrollierter Durchsatz entspricht wieder der Baseline,
- die ursprüngliche Anwendung funktioniert,
- Kabel und Ursache sind dokumentiert.

---

27. Praxisfall B: WLAN langsam, Ethernet normal

Symptom

- mehrere WLAN-Clients sind langsam,
- kabelgebundene Clients funktionieren,
- Latenz zum Gateway steigt unter Last stark,
- Access Point und Clients verwenden denselben stark belegten Kanal.

Prüfung

1. WLAN- und Ethernettest vergleichen.
2. Signal, Kanal und Kanalauslastung erfassen.
3. Airtime und Wiederholungsrate am Access Point prüfen.
4. benachbarte Funknetze berücksichtigen.
5. Uplink und CPU des Access Points prüfen.
6. kontrollierte Messung bei geringer Last durchführen.
7. Kanalplanung entsprechend der vorhandenen Funkumgebung prüfen.

Mögliche Ursache

Der verwendete Kanal ist stark ausgelastet. Mehrere Access Points und fremde WLANs konkurrieren um dieselbe Airtime.

Nachprüfung

- vorgesehene Kanalplanung ist umgesetzt,
- Wiederholungsrate ist gesunken,
- Latenz bleibt auch unter kontrollierter Last stabiler,
- Durchsatz hat sich nachweisbar verbessert,
- benachbarte Funkzellen funktionieren weiterhin,
- Änderung und Messergebnisse sind dokumentiert.

---

28. Praxisfall C: Download schnell, Upload langsam

Symptom

- Downloads erreichen die erwartete Größenordnung,
- Uploads brechen stark ein,
- bei Uploadlast steigt die Latenz,
- andere Anwendungen reagieren währenddessen verzögert.

Prüfung

1. Download und Upload getrennt messen.
2. Gegenrichtung mit kontrollierter Messung prüfen.
3. WAN-Auslastung und Queue beobachten.
4. Firewall- und Router-CPU prüfen.
5. Drops und Policing-Zähler kontrollieren.
6. Providerprofil und vereinbarte Uploadrate prüfen.
7. VPN- und QoS-Regeln berücksichtigen.

Mögliche Ursache

Der verfügbare Upstream wird vollständig ausgelastet. Eine ungeeignete Warteschlangensteuerung verursacht zusätzliche Latenz.

Nachprüfung

- Upload bleibt innerhalb der vorgesehenen Kapazität,
- interaktive Anwendungen bleiben unter Last nutzbar,
- Queue Drops und Latenz wurden erneut gemessen,
- vorgesehene Priorisierung funktioniert,
- nicht autorisierte Bandbreitenerweiterungen wurden nicht vorgenommen.

---

29. Praxisfall D: Netzwerk normal, Anwendung langsam

Symptom

- Latenz und Paketverlust sind unauffällig,
- kontrollierter Durchsatz ist normal,
- nur eine Webanwendung antwortet langsam,
- Zeit bis zum ersten Byte ist stark erhöht.

Prüfung

1. DNS-, TCP-, TLS- und Antwortzeiten getrennt messen.
2. Anwendung mit anderem Client vergleichen.
3. Reverse-Proxy-Protokolle prüfen.
4. Backend-Verbindung testen.
5. Anwendungs- und Datenbankprotokolle auswerten.
6. Serverressourcen kontrollieren.
7. zeitgleiche Jobs oder Locks prüfen.

Mögliche Ursache

Eine Datenbankabfrage wartet auf eine Sperre. Das Netzwerk transportiert die Pakete normal, die Anwendung erzeugt die Antwort jedoch verspätet.

Nachprüfung

- Zeit bis zum ersten Byte hat sich normalisiert,
- Netzwerkwerte bleiben unverändert,
- Datenbank- und Anwendungszustand sind fehlerfrei,
- ursprünglicher Geschäftsprozess funktioniert,
- Ursache und Maßnahme sind dokumentiert.

---

30. Praxisfall E: Über VPN funktionieren kleine Anfragen, große Übertragungen brechen ein

Symptom

- Anmeldung am VPN funktioniert,
- Ping und kleine Webanfragen funktionieren,
- größere Dateiübertragungen hängen oder werden sehr langsam,
- ohne VPN tritt das Problem nicht auf.

Prüfung

1. Pfad und Tunnelart dokumentieren.
2. MTU auf Client, Tunnel und Zielpfad prüfen.

3. Paketaufzeichnung auf Wiederholungen untersuchen.
4. ICMP-Fehlermeldungen berücksichtigen.
5. MSS-Anpassung am Tunnel prüfen.
6. Upload und Download getrennt testen.
7. VPN-Gatewayauslastung kontrollieren.

Mögliche Ursache

Durch den Tunnel-Overhead ist die effektive MTU geringer. Notwendige Rückmeldungen für Path MTU Discovery werden auf dem Pfad verworfen.

Nachprüfung

- kleine und große Übertragungen funktionieren,
- TCP-Wiederholungen sind zurückgegangen,
- vorgesehene MTU- beziehungsweise MSS-Konfiguration ist dokumentiert,
- andere VPN-Verbindungen wurden kontrolliert,
- keine pauschale Deaktivierung von Sicherheitsfunktionen erfolgte.

---

31. Ungeeignete Sofortmaßnahmen

Problematisch sind insbesondere:

- Netzwerkgeräte ohne Dokumentation neu starten,
- Kabel, Switchports und Konfiguration gleichzeitig verändern,
- Geschwindigkeit oder Duplex nur auf einer Seite erzwingen,
- Jumbo Frames versuchsweise aktivieren,
- IPv6 pauschal deaktivieren,
- Firewalls oder Sicherheitsprüfung vollständig abschalten,
- QoS-Regeln ohne Messung verändern,
- produktive Links mit unkontrollierten Lasttests auslasten,
- UDP-Tests mit beliebiger hoher Zielrate durchführen,
- Provider verantwortlich machen, ohne den lokalen Pfad geprüft zu haben,
- einen einzelnen Pingverlust als eindeutigen Beweis verwenden,
- jeden Verlust an einem Traceroute-Hop als Fehler dieses Routers interpretieren,
- eine Dateiübertragung als reinen Netzwerkbenchmark behandeln,
- Paketaufzeichnungen ungeschützt speichern,
- Netzwerkkartentreiber ungeprüft ersetzen,
- Offload- und Empfangseinstellungen wahllos deaktivieren,
- Server neu starten, ohne Ressourcen und Protokolle zu sichern.

Vor Änderungen sollten mindestens dokumentiert werden:

- Symptom,
- betroffene Benutzer und Systeme,
- Quelle und Ziel,

- Verbindungstyp,
- Linkgeschwindigkeit,
- DNS-Ergebnis,
- Latenz,
- Paketverlust,
- Durchsatz,
- Interfacezähler,
- Route,
- Serverressourcen,
- Zeitpunkt,
- Vergleichssystem,
- aktuelle Konfiguration.

---

32. Vollständige Prüfreihenfolge

1. genaue langsame Funktion benennen.
2. Soll- und Istwert dokumentieren.
3. Zeitpunkt, Dauer und Häufigkeit erfassen.
4. betroffene Benutzer, Clients und Standorte bestimmen.
5. Quelle, Ziel und Datenrichtung dokumentieren.
6. funktionierenden Vergleichsclient bestimmen.
7. WLAN und Ethernet unterscheiden.
8. internes und externes Ziel vergleichen.
9. Clientressourcen prüfen.
10. Interface- und Linkstatus prüfen.
11. ausgehandelte Geschwindigkeit und Duplex kontrollieren.
12. Kabel, Adapter und Switchport berücksichtigen.
13. Interfacezähler vor dem Test erfassen.
14. Latenz zum Gateway messen.
15. Latenz zu internen und externen Zielen vergleichen.
16. Paketverlust Ende zu Ende untersuchen.
17. Pfad und Route prüfen.
18. IPv4 und IPv6 getrennt vergleichen.
19. Interfacezähler nach dem Test erneut erfassen.
20. Download und Upload getrennt messen.
21. kontrollierten Durchsatztest verwenden.
22. einzelne und parallele TCP-Verbindungen vergleichen.
23. Datenträger und Anwendung vom Netzwerk abgrenzen.
24. WLAN-Signal, Kanal, Airtime und Wiederholungen prüfen.
25. Uplinks, Port-Channels und Queue Drops kontrollieren.
26. Firewall, VPN, Proxy und Sicherheitsprüfung berücksichtigen.
27. Server-CPU, RAM und Datenträgerlatenz prüfen.
28. Virtualisierung, vSwitch und Host-Uplink untersuchen.
29. MTU, Tunnel und Fragmentierung bei passenden Symptomen prüfen.
30. TCP-Wiederholungen und Fensterverhalten analysieren.

31. bei Bedarf autorisierte Paketaufzeichnung erstellen.
32. Beobachtungen auf einer gemeinsamen Zeitleiste korrelieren.
33. konkrete Hypothese formulieren.
34. genau eine kontrollierbare Änderung durchführen.
35. Latenz erneut messen.
36. Paketverlust erneut prüfen.
37. Durchsatz erneut messen.
38. ursprüngliche Anwendung erneut testen.
39. funktionierende Vergleichssysteme kontrollieren.
40. temporäre Tests und Freigaben entfernen.
41. Ursache, Maßnahme und Nachweis dokumentieren.
42. Monitoring oder Präventionsmaßnahme festlegen.

---

33. Dokumentationsbeispiel

Ticket: INC-20718

Beginn: 02.08.2026, etwa 09:20 Uhr

Umfang: mehrere WLAN-Clients im VLAN 30

Nicht betroffen: kabelgebundene Clients im VLAN 20

Ziel: interner Dateiserver fileserver.example.test

Symptom:

Dateiübertragungen über WLAN erreichen nur etwa 8 bis 15 Mbit/s.

Kabelgebundene Vergleichsclients erreichen zum selben Server etwa

700 Mbit/s. Kleine Webanfragen und DNS-Auflösungen funktionieren.

Ausgangszustand:

- DNS-Auflösung korrekt
- Server per TCP erreichbar
- Dateiserver für Ethernet-Clients normal
- Serverressourcen unauffällig
- Access-Point-Uplink mit 1 Gbit/s aktiv
- keine steigenden CRC-Fehler am Uplink
- hohe Kanalauslastung im verwendeten Frequenzbereich
- erhöhte WLAN-Wiederholungsrate
- Latenz zum Gateway steigt unter Last deutlich

Hypothese:

Die Funkzelle besitzt zu wenig freie Airtime. Der Datenverkehr wird

wiederholt übertragen und wartet auf den Zugriff auf das Funkmedium.

Prüfung:
- Ethernet und WLAN mit demselben Ziel verglichen
- mehrere WLAN-Clients getestet
- Signalstärke und Kanal erfasst
- Uplink und Server als Engpass ausgeschlossen
- kontrollierter Durchsatztest in beide Richtungen durchgeführt
- Access-Point-Statistiken zum Störungszeitpunkt ausgewertet

Ursache:
Starke Kanalbelegung und überlappende Funkzellen führten zu einer hohen Wiederholungsrate und geringer nutzbarer Airtime.

Maßnahme:
Die Kanalplanung der betroffenen Funkzellen wurde nach einer Funkumgebungsanalyse kontrolliert angepasst.

Nachprüfung:
- Latenz zum Gateway unter Last verbessert
- Wiederholungsrate gesunken
- kontrollierter WLAN-Durchsatz deutlich erhöht
- ursprüngliche Dateiübertragung funktioniert
- Ethernet-Clients weiterhin fehlerfrei
- benachbarte Funkzellen kontrolliert

Prävention:
- Kanalauslastung und Wiederholungsrate überwachen
- WLAN-Baseline pro Standort dokumentieren
- Funkumgebung nach größeren Änderungen erneut prüfen

---

34. Checkliste „Netzwerk ist langsam“

- [ ] die langsame Funktion wurde eindeutig benannt.
- [ ] Soll- und Istzustand wurden dokumentiert.
- [ ] Beginn, Dauer und Häufigkeit wurden erfasst.
- [ ] betroffene Clients, Benutzer und Standorte wurden bestimmt.
- [ ] Quelle, Ziel und Datenrichtung wurden dokumentiert.
- [ ] ein funktionierender Vergleichsclient wurde verwendet.

- [ ] WLAN und Ethernet wurden getrennt betrachtet.
- [ ] interne und externe Ziele wurden verglichen.
- [ ] Download und Upload wurden getrennt geprüft.
- [ ] Client-CPU, RAM und Datenträger wurden berücksichtigt.
- [ ] Interface- und Linkstatus wurden geprüft.
- [ ] ausgehandelte Geschwindigkeit und Duplex wurden kontrolliert.
- [ ] Kabel, Adapter, Dockingstation und Switchport wurden berücksichtigt.
- [ ] Interfacezähler wurden vor und nach einem Test verglichen.
- [ ] Latenz zum Gateway wurde gemessen.
- [ ] Latenz zu weiteren Zielen wurde verglichen.
- [ ] Paketverlust wurde Ende zu Ende geprüft.
- [ ] Diagnoseantworten von Zwischenhops wurden nicht ungeprüft bewertet.
- [ ] Route und Rückweg wurden berücksichtigt.
- [ ] IPv4 und IPv6 wurden getrennt verglichen.
- [ ] ein kontrollierter Durchsatztest wurde durchgeführt.
- [ ] Gegenrichtung wurde geprüft.
- [ ] einzelne und mehrere TCP-Verbindungen wurden bei Bedarf verglichen.
- [ ] Dateisystem und Datenträger wurden vom Netzwerk abgegrenzt.
- [ ] WLAN-Signal, Kanal und Airtime wurden geprüft.
- [ ] Switch-Uplinks und Port-Channels wurden berücksichtigt.
- [ ] Queue Drops und Auslastung wurden geprüft.
- [ ] Firewall, Proxy, VPN und Sicherheitsprüfung wurden berücksichtigt.
- [ ] Serverressourcen wurden geprüft.
- [ ] Virtualisierung und Host-Uplink wurden berücksichtigt.
- [ ] MTU und Tunnel-Overhead wurden bei passenden Symptomen geprüft.
- [ ] TCP-Wiederholungen wurden bei Bedarf analysiert.
- [ ] DNS-, TCP-, TLS- und Anwendungszeiten wurden abgegrenzt.
- [ ] sporadische Fehler wurden zeitgestempelt erfasst.
- [ ] Paketaufzeichnungen erfolgten nur mit Berechtigung.
- [ ] eine konkrete Hypothese wurde formuliert.
- [ ] nur eine kontrollierbare Änderung wurde vorgenommen.
- [ ] Latenz, Verlust und Durchsatz wurden nach der Änderung erneut gemessen.
- [ ] die ursprüngliche Anwendung wurde erneut getestet.
- [ ] Vergleichssysteme funktionieren weiterhin.

- [ ] temporäre Testkonfigurationen wurden entfernt.
- [ ] Ursache, Maßnahme und Nachweis wurden dokumentiert.

---

35. Schnellreferenz

Fehlerbild	wahrscheinlicher Untersuchungsbereich
nur ein Client langsam	Client, Kabel, Adapter, Treiber oder Switchport
alle Clients eines Switches langsam	Uplink, Switch, VLAN oder gemeinsame Gegenstelle
nur WLAN langsam	Funkumgebung, Airtime, Kanal, AP oder Client
Ethernet und WLAN langsam	Gateway, Uplink, Firewall, WAN, Server oder Anwendung
nur ein Server langsam	Zielserver, Servernetz, Datenträger oder Anwendung
alle externen Ziele langsam	WAN, Provider, Firewall, Proxy oder VPN
nur Upload langsam	Upstream, Queue, Policing, Provider oder VPN
nur Download langsam	Downstream, Server, TCP, Proxy oder Client
Latenz steigt nur unter Last	Queue, Auslastung, Bufferbloat oder Drops
Ping normal, Dateiübertragung langsam	Durchsatz, Datenträger, Protokoll oder Anwendung
Durchsatztest normal, Anwendung langsam	DNS, TLS, Proxy, Backend, Datenbank oder Server
Link nur mit 100 Mbit/s	Kabel, Adapter, Switchport oder Aushandlung
steigende CRC-/FCS-Fehler	physischer Link, Kabel, Transceiver oder Port
steigende Drops ohne CRC-Fehler	Queue, Überlastung, Policing oder Puffer
viele TCP-Retransmissions	Paketverlust, Überlastung oder Datenpfad
TCP Zero Window	Empfänger verarbeitet Daten zu langsam
kleine Pakete funktionieren, große nicht	MTU, Tunnel oder Fragmentierung
nur über VPN langsam	Tunnel, MTU, Gateway, Verschlüsselung oder Route
nur IPv6 langsam	IPv6-Pfad, Firewall, Route oder Zieladresse
nur IPv4 langsam	IPv4-Pfad, NAT, Firewall oder Route
nur zu bestimmten Zeiten langsam	Last, Backup, Scan, Job, Provider oder Funkumgebung
ein TCP-Stream langsam, mehrere schneller	Latenz, Fenster, Verlust oder Serverbegrenzung
WLAN-Signal gut, Durchsatz schlecht	Kanalauslastung, Airtime, Störung oder Wiederholungen
erstes Byte langsam	Anwendung, Proxy, Backend oder Datenbank
erstes Byte schnell, Download langsam	Durchsatz, Verlust, Serverausgabe oder Client
lokale Ziele schnell, Internet langsam	WAN, Provider, NAT, Firewall oder Proxy
Gateway bereits langsam	lokaler Link, WLAN, Client oder erstes Netzsegment

Merksatz

> „Langsam“ ist keine eindeutige Fehlerursache. Eine belastbare Analyse trennt Latenz, Paketverlust, Jitter und Durchsatz, vergleicht funktionierende und betroffene Pfade und prüft anschließend Client, Link, WLAN, Switch, Firewall, WAN, Server und Anwendung. Erst reproduzierbare Messwerte vor und nach einer kontrollierten Änderung belegen eine Verbesserung.

Quellen und weiterführende Dokumentation

- Microsoft Learn – Guidance for troubleshooting TCP/IP performance
- Microsoft Learn – Overview of TCP/IP performance
- Microsoft Learn – TCP/IP performance known issues
- Microsoft Learn – Network Adapter Performance Tuning in Windows Server
- Microsoft Learn – Test-Connection
- Microsoft Learn – Test-NetConnection
- Microsoft Learn – Get-NetAdapterStatistics
- ESnet – iperf3 documentation
- ESnet – Invoking iperf3
- ESnet – iperf3 FAQ and supported platforms
- Wireshark User’s Guide – TCP Analysis
- Wireshark – Display Filter Reference: TCP
- Wireshark – TShark Manual
- RFC 6349 – Framework for TCP Throughput Testing
- RFC 9293 – Transmission Control Protocol
- RFC 8201 – Path MTU Discovery for IPv6
- RFC 1191 – Path MTU Discovery
