3.7 Standardgateway und Routing analysieren

Routing bestimmt, über welchen Netzwerkpfad ein IP-Paket sein Ziel erreicht. Liegt das Ziel nicht im direkt angeschlossenen Subnetz, benötigt der Client eine passende Route zu einem Router beziehungsweise Next Hop.

Das Standardgateway wird verwendet, wenn keine spezifischere Route zum Ziel vorhanden ist. Eine vorhandene Standardroute beweist jedoch nicht, dass sie korrekt ist oder dass der vollständige Hin- und Rückweg funktioniert.

> **Grundregel:** Nicht nur prüfen, ob eine Route vorhanden ist. Es muss geprüft werden, welche Route für das konkrete Ziel tatsächlich ausgewählt wird und ob ein passender Rückweg existiert.

---

1. Welche Aufgaben erfüllt ein Router?

Ein Router verbindet unterschiedliche IP-Netze.

Beispiel

```
Clientnetz:
192.0.2.0/24

Servernetz:
198.51.100.0/24
```

Kommunikationsweg:

```
CLIENT-023
192.0.2.23/24
  │
  ├─ Standardgateway 192.0.2.1
  │
  ├─ Router oder Firewall
  │
  └─ SERVER-01
     198.51.100.20/24
```

Der Client erkennt anhand seines Präfixes, dass `198.51.100.20` nicht im lokalen Subnetz liegt. Er übergibt das Paket deshalb an einen Router.

Der Router:

1. liest die Ziel-IP-Adresse,
2. sucht die passendste Route,
3. bestimmt Ausgangsschnittstelle und nächsten Hop,
4. verringert bei IPv4 die TTL beziehungsweise bei IPv6 den Hop Limit,
5. leitet das Paket weiter oder verwirft es.

2. Wann wird das Standardgateway verwendet?

Die IPv4-Standardroute lautet:

```
0.0.0.0/0
```

Die IPv6-Standardroute lautet:

```
::/0
```

Sie passen grundsätzlich auf jedes Ziel der jeweiligen Adressfamilie. Spezifischere Routen werden jedoch bevorzugt.

Beispielroutingtabelle

Zielpräfix	Next Hop	Bedeutung
`192.0.2.0/24`	direkt verbunden	lokales Clientnetz
`198.51.100.0/24`	`192.0.2.254`	spezifische Route zum Servernetz
`0.0.0.0/0`	`192.0.2.1`	Standardroute

Für das Ziel `198.51.100.20` wird die spezifische `/24`-Route verwendet und nicht die Standardroute.

3. Was bedeutet Longest Prefix Match?

Wenn mehrere Routen zu einem Ziel passen, wird grundsätzlich die Route mit dem längsten passenden Präfix bevorzugt.

Beispiel

Route	Passt auf `198.51.100.20`?	Präfixlänge
`0.0.0.0/0`	Ja	0
`198.51.0.0/16`	Ja	16
`198.51.100.0/24`	Ja	24
`198.51.100.20/32`	Ja	32

Ausgewählt wird:

```
198.51.100.20/32
```

Reihenfolge:

```
Hostroute /32
  vor
Netzroute /24
  vor
gröberer Netzroute /16
  vor
Standardroute /0
```

Eine Route mit niedrigerer Metrik gewinnt nicht gegen eine passendere Route mit längerem Präfix. Die Metrik wird für konkurrierende, in der Auswahl gleich geeignete Routen relevant.

4. Welche Bestandteile besitzt ein Routingtabelleneintrag?

Bestandteil	Bedeutung
Zielpräfix	Netz oder Host, für den die Route gilt
Präfixlänge	Genauigkeit der Route
Next Hop	nächster Router
Ausgangsschnittstelle	verwendeter Adapter
Quelladresse	für das Ziel ausgewählte lokale Adresse
Metrik	Kosten beziehungsweise Priorität
Protokoll oder Ursprung	statisch, verbunden, DHCP oder Routingprotokoll

Bestandteil	Bedeutung
Gültigkeitsdauer	bei dynamischen Einträgen möglicherweise begrenzt
Routingtabelle	bei Policy Routing eine bestimmte Tabelle

Beispiel

```
198.51.100.0/24 via 192.0.2.254 dev eth0 metric 100
```

Feld	Wert
Ziel	`198.51.100.0/24`
Next Hop	`192.0.2.254`
Schnittstelle	`eth0`
Metrik	`100`

5. Welche Symptome sprechen für einen Routingfehler?

- lokale Ziele sind erreichbar, entfernte Ziele jedoch nicht,
- Standardgateway fehlt,
- falsches Gateway ist eingetragen,
- nur ein bestimmtes Zielnetz ist nicht erreichbar,
- VPN übernimmt unerwartet die Standardroute,
- Zugriff funktioniert nur ohne VPN,
- Hinweg funktioniert, Rückweg fehlt,
- Traceroute zeigt eine Schleife,
- Pakete erreichen die falsche Firewall,
- Verbindung funktioniert nur in eine Richtung,
- mehrere Standardrouten konkurrieren,
- Route zeigt auf eine falsche Schnittstelle,
- falsche Quelladresse wird ausgewählt,
- ein neues Subnetz ist noch nicht überall bekannt,
- Route wurde zusammengefasst und enthält ein nicht erreichbares Teilnetz,
- dynamische Route wurde zurückgezogen,
- Routingtabelle unterscheidet sich zwischen redundanten Routern,
- IPv4 funktioniert, IPv6 jedoch nicht.

6. Wie wird die Routingtabelle unter Windows angezeigt?

IPv4-Routen

```
[RO] Get-NetRoute -AddressFamily IPv4 |
    Sort-Object DestinationPrefix, RouteMetric |
    Format-Table ifIndex,
                 InterfaceAlias,
                 DestinationPrefix,
                 NextHop,
                 RouteMetric,
                 InterfaceMetric,
                 Protocol,
                 State
```

IPv6-Routen

```
[RO] Get-NetRoute -AddressFamily IPv6 |
    Sort-Object DestinationPrefix, RouteMetric |
    Format-Table ifIndex,
                 InterfaceAlias,
                 DestinationPrefix,
                 NextHop,
                 RouteMetric,
                 InterfaceMetric,
                 Protocol,
                 State
```

Klassische Gesamtausgabe

```
[RO] route print
```

Nur IPv4:

```
[RO] route print -4
```

Nur IPv6:

```
[RO] route print -6
```

Standardrouten

```
[RO] Get-NetRoute -DestinationPrefix '0.0.0.0/0' |
    Format-Table InterfaceAlias,
                 ifIndex,
                 NextHop,
                 RouteMetric,
                 InterfaceMetric,
                 Protocol
```

IPv6:

```
[RO] Get-NetRoute -DestinationPrefix '::/0'
```

7. Wie wird unter Windows die tatsächlich ausgewählte Route geprüft?

```
[RO] Find-NetRoute -RemoteIPAddress 198.51.100.20
```

Die Ausgabe enthält typischerweise:

- passende Route,
- Ausgangsschnittstelle,
- Next Hop,
- lokale Quelladresse.

Zusätzliche Schnittstelleninformationen

```
[RO] Get-NetIPInterface |
    Sort-Object AddressFamily, InterfaceMetric |
    Format-Table ifIndex,
                 InterfaceAlias,
                 AddressFamily,
                 ConnectionState,
                 InterfaceMetric,
                 AutomaticMetric
```

Konkrete Zielprüfung

```
[TEST] Test-NetConnection 198.51.100.20 -InformationLevel Detailed
```

Mit Traceroute:

```
[TEST] Test-NetConnection 198.51.100.20 `
    -TraceRoute `
    -InformationLevel Detailed
```

`Test-NetConnection -TraceRoute` prüft den Pfad mit den von Windows dafür vorgesehenen Diagnosemechanismen. Ein nicht antwortender Hop beweist nicht automatisch einen Weiterleitungsfehler.

8. Wie wird die Routingtabelle unter Linux angezeigt?

IPv4-Hauptroutingtabelle

```
[RO] ip -4 route show
```

IPv6-Hauptroutingtabelle

```
[RO] ip -6 route show
```

Alle Routingtabellen

```
[RO] ip route show table all
```

IPv6:

```
[RO] ip -6 route show table all
```

Standardroute

```
[RO] ip route show default
```

IPv6:

```
[RO] ip -6 route show default
```

Detaillierte Routen

```
[RO] ip -details route show
```

Routingregeln

```
[RO] ip rule show
```

Policy Routing kann dazu führen, dass eine andere Tabelle verwendet wird als die gewöhnliche `main`-Tabelle.

9. Wie wird unter Linux die tatsächlich ausgewählte Route geprüft?

```
[RO] ip route get 198.51.100.20
```

Beispiel:

```
198.51.100.20 via 192.0.2.1 dev eth0 src 192.0.2.23 uid 1000
```

Feld	Bedeutung
Ziel	`198.51.100.20`
`via`	nächster Router
`dev`	Ausgangsschnittstelle
`src`	ausgewählte Quelladresse
`uid`	bei entsprechender Ausgabe berücksichtigte Benutzer-ID

Route mit bestimmter Quelladresse prüfen

```
[RO] ip route get 198.51.100.20 from 192.0.2.23
```

IPv6

```
[RO] ip -6 route get 2001:db8:20::20
```

Bei Policy Routing kann die Routenauswahl von folgenden Merkmalen abhängen:

- Quelladresse,
- Zieladresse,
- Eingangsinterface,
- Firewallmarkierung,
- Benutzerkennung,
- Routingtabelle,
- Priorität der Regel.

10. Wie wird die Routingtabelle unter macOS angezeigt?

IPv4-Routen

```
[RO] netstat -rn -f inet
```

IPv6-Routen

```
[RO] netstat -rn -f inet6
```

IPv4-Standardroute

```
[RO] route -n get default
```

Ausgewählte Route zu einem IPv4-Ziel

```
[RO] route -n get 198.51.100.20
```

Ausgewählte Route zu einem IPv6-Ziel

```
[RO] route -n get -inet6 2001:db8:20::20
```

Typische Felder:

Feld	Bedeutung

`destination`	Ziel
`gateway`	Next Hop
`interface`	Ausgangsschnittstelle
`flags`	Routeneigenschaften
`recvpipe` `sendpipe`	interne Routinginformationen
`mtu`	routenbezogene MTU, falls vorhanden

VPN-Verbindungen erscheinen unter macOS häufig über Tunnelinterfaces wie `utun0`, `utun1` oder weitere nummerierte Varianten.

11. Wie werden mehrere Standardrouten bewertet?

Mehrere Standardrouten können beabsichtigt sein:

- LAN und WLAN gleichzeitig,
- VPN-Full-Tunnel,
- redundante Router,
- mehrere Internetanschlüsse,
- virtuelle Adapter,
- Mobilfunk-Fallback.

Windows

```
[RO] Get-NetRoute -DestinationPrefix '0.0.0.0/0' |
    Sort-Object RouteMetric, InterfaceMetric |
    Format-Table InterfaceAlias,
                 NextHop,
                 RouteMetric,
                 InterfaceMetric,
                 Protocol
```

Linux

```
[RO] ip route show default
```

```
[RO] ip rule show
```

macOS

```
[RO] netstat -rn -f inet |
    grep '^default'
```

Prüffragen

1. Welche Route gehört zur aktiven Schnittstelle?
2. Welche Route besitzt die wirksame Priorität?
3. Gibt es spezifischere VPN-Routen?
4. Welche Quelladresse wird ausgewählt?
5. Passt der Rückweg zu dieser Quelladresse?
6. Ist eine Route nur ein verbliebener Eintrag eines getrennten Adapters?
7. Wird IPv4 anders als IPv6 geroutet?

Die numerische Metrik ist nicht zwischen verschiedenen Betriebssystemen direkt vergleichbar.

12. Wie beeinflussen Schnittstellen- und Routenmetrik die Auswahl unter Windows?

Windows berücksichtigt unter anderem:

- Präfixlänge,
- Routenmetrik,
- Schnittstellenmetrik.

Vereinfacht kann bei gleich spezifischen Routen eine Kombination aus Routen- und Schnittstellenmetrik die bevorzugte Route beeinflussen.

Schnittstellenmetriken

```
[RO] Get-NetIPInterface |
    Format-Table InterfaceAlias,
                 AddressFamily,
                 AutomaticMetric,
                 InterfaceMetric,
                 ConnectionState
```

Routenmetriken

```
[RO] Get-NetRoute |
    Format-Table DestinationPrefix,
                 NextHop,
                 InterfaceAlias,
                 RouteMetric,
                 InterfaceMetric
```

Eine aktivierte automatische Metrik lässt Windows den Wert anhand der Schnittstelleneigenschaften bestimmen.

```
[CHANGE][DISRUPT] Metriken nicht verändern, nur weil eine numerische
Reihenfolge unerwartet aussieht. Zuerst die tatsächlich gewählte Route
mit Find-NetRoute prüfen.
```

13. Was ist eine Hostroute?

Eine Hostroute gilt nur für eine einzelne Zieladresse.

IPv4

```
198.51.100.20/32
```

IPv6

```
2001:db8:20::20/128
```

Beispiel:

```
198.51.100.20/32 via 192.0.2.254
0.0.0.0/0 via 192.0.2.1
```

Nur das Ziel `198.51.100.20` wird über `192.0.2.254` geleitet. Andere Ziele verwenden weiterhin die Standardroute.

Mögliche Fehler

- alte Hostroute zeigt auf nicht mehr vorhandenen Router,

- VPN legt eine Hostroute zum VPN-Gateway an,
- Sicherheitssoftware installiert spezifische Routen,
- statische Testkonfiguration wurde nicht entfernt,
- Route gilt nur für IPv4, während die Anwendung IPv6 verwendet.

14. Was ist Policy-Based Routing?

Bei gewöhnlichem Routing wird hauptsächlich die Zieladresse betrachtet. Policy-Based Routing kann zusätzliche Kriterien verwenden:

- Quellnetz,
- eingehende Schnittstelle,
- Benutzer oder Anwendung,
- DSCP beziehungsweise Traffic-Klasse,
- Firewallmarkierung,
- Dienst oder Port,
- Mandant oder VRF.

Linux-Regeln anzeigen

```
[RO] ip rule show
```

Beispielstruktur:

```
0:      from all lookup local
100:    from 192.0.2.0/24 lookup firma-a
32766:  from all lookup main
32767:  from all lookup default
```

Tabelle anzeigen:

```
[RO] ip route show table firma-a
```

Falls die Tabelle nur eine Nummer besitzt:

```
[RO] ip route show table 100
```

Eine korrekte Route in der `main`-Tabelle beweist bei Policy Routing nicht, dass sie für den konkreten Datenstrom verwendet wird.

15. Was ist eine VRF und warum ist sie für die Diagnose wichtig?

Eine Virtual Routing and Forwarding Instance stellt eine getrennte Routingdomäne bereit.

Vereinfacht:

```
Router
├─ VRF FIRMA-A
│   └─ eigene Routingtabelle
└─ VRF FIRMA-B
    └─ eigene Routingtabelle
```

Dieselben IP-Netze können in getrennten VRFs vorkommen, ohne direkt miteinander verbunden zu sein.

Mögliche Fehler

- Schnittstelle befindet sich in falscher VRF,
- Route existiert nur in einer anderen VRF,
- Firewall prüft falschen Kontext,
- Managementzugriff verwendet eine getrennte VRF,
- Ping ohne VRF-Angabe testet den falschen Pfad,
- Rückroute wurde in falscher Tabelle eingetragen.

Linux-VRFs anzeigen, falls verwendet:

```
[RO] ip -d link show type vrf
```

Routen einer Tabelle:

```
[RO] ip route show table TABELLENNAME
```

Befehle auf Routern und Firewalls sind herstellerabhängig und müssen im korrekten Routingkontext ausgeführt werden.

16. Wie wird ein fehlender Rückweg erkannt?

Für eine funktionierende Kommunikation werden Hin- und Rückweg benötigt.

```
Hinweg:
CLIENT-023 → Router A → SERVER-01

Rückweg:
SERVER-01 → Router B → CLIENT-023
```

Ein Rückweg darf anders verlaufen, muss aber:

- zur Quelladresse führen,
- von Firewalls zugelassen werden,
- bei zustandsbehafteten Komponenten zur Sitzung passen,
- notwendige NAT-Zustände berücksichtigen.

Typische Symptome eines fehlenden Rückwegs

- SYN verlässt Client, aber keine Antwort kommt zurück,
- Anfrage erreicht Server, Antwort verlässt Server,
- Antwort kommt an falscher Schnittstelle an,
- nur Verbindungen aus einer Richtung funktionieren,
- lokale Serverzugriffe funktionieren, entfernte nicht,
- Ping vom Client zum Server schlägt fehl, vom Server zum Client ebenfalls,
- Firewall meldet ungültigen oder fehlenden Sitzungszustand.

Prüfung

1. Clientroute zum Server prüfen.
2. Serverroute zur Clientadresse prüfen.
3. Zwischenrouter und Firewalls prüfen.
4. NAT-Zustände berücksichtigen.
5. Paketmitschnitt an mindestens zwei geeigneten Messpunkten vergleichen.

17. Was ist asymmetrisches Routing?

Beim asymmetrischen Routing nehmen Hin- und Rückweg unterschiedliche Pfade.

```
Hinweg:
Client → Firewall A → Server

Rückweg:
Server → Firewall B → Client
```

Asymmetrisches Routing ist nicht grundsätzlich fehlerhaft. Es kann jedoch problematisch sein für:

- zustandsbehaftete Firewalls,
- NAT,
- Intrusion-Prevention-Systeme,
- Load Balancer,
- Pfadmessungen,
- MTU-Erkennung,
- Paketmitschnitte an nur einer Stelle.

Typische Hinweise

- Firewall A sieht nur Clientpakete,
- Firewall B sieht nur Serverantworten,
- zustandslose Tests funktionieren, TCP jedoch nicht,
- einzelne Verbindungen funktionieren abhängig von Lastverteilung,
- Traceroute in Gegenrichtung zeigt anderen Pfad,
- Failover führte zu unterschiedlichen Routingtabellen.

Die ausführliche Analyse asymmetrischer Wege wird auf Seite 3.17 behandelt.

18. Wie wird der Netzwerkpfad mit tracert oder traceroute untersucht?

Windows

Ohne Namensauflösung:

```
[TEST] tracert -d 198.51.100.20
```

Mit Zielname:

```
[TEST] tracert app.example.intern
```

Linux

```
[TEST] traceroute -n 198.51.100.20
```

macOS

```
[TEST] traceroute -n 198.51.100.20
```

Prinzip

Traceroute sendet Pakete mit schrittweise erhöhtem TTL- beziehungsweise Hop-Limit-Wert.

```
TTL 1 → erster Router
TTL 2 → zweiter Router
TTL 3 → dritter Router
```

Ein Router, an dem der Wert abläuft, kann eine ICMP-Time-Exceeded-Nachricht zurücksenden.

Wichtig

- Router können Diagnosepakete nicht beantworten.
- ICMP-Antworten können prioritätsreduziert behandelt werden.
- Traceroute-Protokoll und Anwendungsprotokoll können unterschiedlich geroutet oder gefiltert werden.
- Der sichtbare Pfad zeigt nur die antwortenden Hops.
- Der Rückweg der ICMP-Antwort kann anders verlaufen.
- Ein Sternchen beweist keinen Paketverlust des eigentlichen Anwendungsverkehrs.

19. Wie werden Sternchen in einer Traceroute interpretiert?

Beispiel:

```
1  192.0.2.1      1 ms
2  203.0.113.1    5 ms
3  * * *
4  198.51.100.20  12 ms
```

Da Hop 4 antwortet, hat Hop 3 den Verkehr offenbar weitergeleitet. Hop 3 beantwortet nur die Diagnoseanfrage nicht.

Mögliche Gründe für Sternchen

- Router sendet keine TTL-Exceeded-Antwort,
- Antwort wird gefiltert,
- Rate-Limit für ICMP,
- Rückweg der Antwort fehlt,

- Gerät priorisiert Weiterleitung höher als Managementantworten,
- tatsächlicher Paketverlust.

Erst wenn alle nachfolgenden Hops ebenfalls fehlen, kann ab dieser Stelle ein Problem vermutet werden. Selbst dann muss geprüft werden, ob das Ziel oder eine Firewall Diagnoseverkehr absichtlich blockiert.

20. Wie wird eine Routing-Schleife erkannt?

Eine Routing-Schleife entsteht, wenn Router Pakete wiederholt gegenseitig weiterleiten.

Beispiel:

```
Router A → Router B → Router A → Router B
```

Mögliche Traceroute-Ausgabe:

```
5  192.0.2.1
6  192.0.2.2
7  192.0.2.1
8  192.0.2.2
9  192.0.2.1
```

Mögliche Ursachen

- widersprüchliche statische Routen,
- fehlerhafte Default Routes,
- Routingprotokollproblem,
- fehlerhafte Routenumverteilung,
- Zusammenfassungsroute ohne passende Detailroute,
- Failoverzustand,
- falsches Policy Routing,
- Tunnelrouting.

Die TTL beziehungsweise der Hop Limit verhindert, dass ein einzelnes Paket unbegrenzt zirkuliert. Die Schleife kann trotzdem fortlaufend neue Verbindungen beeinträchtigen.

21. Wie werden Paketverlust und Latenz entlang des Pfades bewertet?

Windows PathPing

```
[TEST] pathping -n 198.51.100.20
```

PathPing kombiniert eine Pfadermittlung mit längerfristigen Messungen zu den Hops. Die Ausführung kann mehrere Minuten dauern.

Linux und macOS mit MTR

Falls `mtr` installiert und freigegeben ist:

```
[TEST] mtr -n -r -c 20 198.51.100.20
```

Option	Bedeutung
`-n`	keine Namensauflösung
`-r`	Bericht erzeugen
`-c 20`	20 Messzyklen

Interpretationsregel

```
Paketverlust an einem Zwischenhop,
aber kein Verlust an nachfolgenden Hops
→ wahrscheinlich nur reduzierte Antwortpriorität dieses Hops.
```

```
Paketverlust beginnt an einem Hop
und setzt sich bis zum Ziel fort
→ möglicher Verlust ab diesem Pfadabschnitt.
```

Auch dieses Muster ist nur ein Hinweis. Das verwendete Diagnoseprotokoll kann anders behandelt werden als die eigentliche Anwendung.

22. Wie wird ein bestimmter TCP-Dienst entlang des Pfades berücksichtigt?

Ein erfolgreicher Traceroute beweist nicht, dass ein bestimmter Port zugelassen ist.

Windows

```
[TEST] Test-NetConnection 198.51.100.20 `
    -Port 443 `
    -InformationLevel Detailed
```

Linux

```
[TEST] nc -vz -w 5 198.51.100.20 443
```

macOS

```
[TEST] nc -vz -w 5 198.51.100.20 443
```

Je nach `nc`-Implementierung können Optionen und Ausgabe abweichen. Lokale Hilfe prüfen:

```
[RO] nc -h
```

Bewertung

Test	Erfolgreich	Fehlgeschlagen
Routingprüfung	IP-Pfad grundsätzlich vorhanden	Route, Filter oder Ziel offen
TCP-Porttest	TCP-Verbindungsaufbau möglich	Filter, Dienst, Rückweg oder Routing offen
Anwendungstest	Protokollantwort erhalten	Anwendung, Authentifizierung oder Backend offen

23. Wie wird eine Route mit einem Paketmitschnitt bestätigt?

Auf einem Ethernetclient zeigt die Ziel-MAC-Adresse, an welchen direkten Nachbarn das Paket übergeben wird.

Entferntes Ziel

```
IP-Ziel: 198.51.100.20
Ethernet-Ziel: MAC-Adresse des Gateways
```

Lokales Ziel

```
IP-Ziel: 192.0.2.80
Ethernet-Ziel: MAC-Adresse des Zielsystems
```

Wireshark-Filter

Bestimmtes Ziel:

```
ip.dst == 198.51.100.20
```

IPv6:

```
ipv6.dst == 2001:db8:20::20
```

TTL anzeigen beziehungsweise filtern:

```
ip.ttl
```

IPv6 Hop Limit:

```
ipv6.hlim
```

ICMP Time Exceeded:

```
icmp.type == 11
```

ICMPv6 Time Exceeded:

```
icmpv6.type == 3
```

Ein lokaler Mitschnitt zeigt nur den Verkehr am ausgewählten Interface. Er beweist nicht, wie nachfolgende Router das Paket weiterleiten.

24. Wie beeinflussen VPN-Verbindungen die Routingtabelle?

Ein VPN kann folgende Routen installieren:

- neue Standardroute,
- spezifische Routen zu internen Netzen,
- Hostroute zum VPN-Gateway,
- ausgeschlossene lokale Routen,
- IPv4- und IPv6-Routen,
- richtlinienbasierte Routen.

Full Tunnel

```
0.0.0.0/0 → VPN
```

Der gesamte IPv4-Verkehr soll durch den Tunnel geführt werden.

Split Tunnel

```
10.0.0.0/8 → VPN
0.0.0.0/0 → lokales Gateway
```

Nur bestimmte Netze werden über das VPN erreicht.

Typische Fehler

- internes Netz fehlt in der Split-Tunnel-Liste,
- lokales und entferntes Netz überschneiden sich,
- VPN-Route ist spezifischer als lokale Route,
- IPv6 wird nicht durch den Tunnel geführt,
- Rückroute zum VPN-Adresspool fehlt,
- Tunnelinterface bleibt nach Trennung bestehen,
- Metriken und Policies wählen falschen Weg.

Vergleich

```
Routingtabelle vor VPN-Verbindung
Routingtabelle nach VPN-Verbindung
```

Dabei dürfen sensible interne Routen nur geschützt dokumentiert werden.

25. Wie werden überlappende Netze erkannt?

Beispiel

Lokales Heimnetz:

```
192.168.1.0/24
```

Entferntes Firmennetz über VPN:

```
192.168.1.0/24
```

Der Client kann nicht allein anhand der Zieladresse unterscheiden, ob `192.168.1.50` lokal oder über das VPN erreicht werden soll.

Mögliche Auswirkungen:

- internes Ziel wird im lokalen Netz gesucht,
- ARP-Anfragen werden statt VPN-Verkehr erzeugt,
- spezifische Hostrouten sind erforderlich,
- nur einige Ziele funktionieren,
- DNS liefert eine korrekte, aber lokal überlappende Adresse.

Prüfung

Windows

```
[RO] Find-NetRoute -RemoteIPAddress 192.168.1.50
```

Linux

```
[RO] ip route get 192.168.1.50
```

macOS

```
[RO] route -n get 192.168.1.50
```

Die nachhaltige Lösung erfordert eine abgestimmte Adressplanung oder ein vorgesehenes VPN-/NAT-Konzept. Willkürliche Hostrouten sind häufig nur eine begrenzte Übergangslösung.

26. Wie werden dynamische Routingprotokolle berücksichtigt?

Router können Routen dynamisch austauschen, beispielsweise über:

- OSPF,
- IS-IS,
- BGP,
- RIP,
- herstellerspezifische Verfahren.

Zu prüfen sind:

- Nachbarschaftsstatus,
- empfangene Routen,
- angekündigte Routen,
- bestes Pfadattribut,
- letzte Zustandsänderung,
- zurückgezogene Route,
- Filter und Route Maps,
- Routenumverteilung,
- Zusammenfassungen,
- gleiche Sicht auf redundanten Routern.

Typische Symptome

- Route fehlt nur auf einem Router,
- Pfad ändert sich wiederholt,
- nach Failover ist ein Netz nicht erreichbar,
- spezifische Route wurde durch Zusammenfassung ersetzt,
- Rückroute wird nicht angekündigt,
- eine Route wird durch Policy gefiltert.

Die konkreten Befehle sind router- und herstellerabhängig. Sie müssen anhand der offiziellen Dokumentation der eingesetzten Plattform ausgewählt werden.

27. Warum dürfen statische Routen nicht vorschnell hinzugefügt werden?

Eine zusätzliche statische Route kann ein Symptom kurzfristig umgehen, aber:

- dynamischen Routingfehler verdecken,
- asymmetrischen Verkehr erzeugen,
- falschen Router verwenden,
- Sicherheitskontrollen umgehen,
- nach einem Failover nicht mehr funktionieren,
- zu einer Schleife führen,
- nur auf einem einzelnen System gelten,
- später vergessen werden.

Vorher dokumentieren

- aktuelle Routingtabelle,
- vorgesehene Architektur,
- Zielpräfix,
- Next Hop,
- Schnittstelle,
- Metrik,
- Persistenz,
- Rückroute,
- Firewall- und NAT-Auswirkungen,
- Rückweg zur Entfernung der Route.

28. Welche eingreifenden Routingbefehle existieren?

Die folgenden Beispiele verändern die Routingtabelle und sind keine regulären ersten Diagnoseschritte.

Windows – temporäre Route

```
[PRIV][CHANGE][DISRUPT] New-NetRoute `
    -DestinationPrefix '198.51.100.0/24' `
    -InterfaceAlias 'Ethernet' `
    -NextHop '192.0.2.254' `
    -RouteMetric 10 `
    -PolicyStore ActiveStore
```

Route entfernen:

```
[PRIV][CHANGE][DISRUPT] Remove-NetRoute `
    -DestinationPrefix '198.51.100.0/24' `
    -InterfaceAlias 'Ethernet' `
    -NextHop '192.0.2.254'
```

Linux – Route hinzufügen

```
[PRIV][CHANGE][DISRUPT] sudo ip route add \
    198.51.100.0/24 \
    via 192.0.2.254 \
```

```
    dev eth0
```

Route entfernen:

```
[PRIV][CHANGE][DISRUPT] sudo ip route del \
    198.51.100.0/24 \
    via 192.0.2.254 \
    dev eth0
```

macOS – temporäre Route hinzufügen

```
[PRIV][CHANGE][DISRUPT] sudo route -n add \
    -net 198.51.100.0/24 \
    192.0.2.254
```

Route entfernen:

```
[PRIV][CHANGE][DISRUPT] sudo route -n delete \
    -net 198.51.100.0/24 \
    192.0.2.254
```

> Vor der Ausführung müssen Interface, Next Hop, Präfix und Rückweg geprüft werden. Eine falsche Route kann den Remotezugriff sofort unterbrechen. Temporäre Betriebssystemrouten sind außerdem nicht automatisch nach einem Neustart persistent.

29. Welche typischen Fehlinterpretationen müssen vermieden werden?

Beobachtung	Falscher Schluss	Richtige Einordnung
Standardroute vorhanden	Routing funktioniert	Next Hop und Rückweg prüfen
Gateway antwortet auf Ping	alle Ziele sind erreichbar	nur ICMP zum Gateway bestätigt
Traceroute zeigt Sterne	dort liegt der Fehler	Hop antwortet möglicherweise nur nicht
hohe Zeit an einem Hop	dieser Hop bremst den Verkehr	Antwortpriorisierung kann abweichen

Beobachtung	Falscher Schluss	Richtige Einordnung
Verlust an Zwischenhop	dort gehen Nutzdaten verloren	nachfolgende Hops vergleichen
Zielroute ist sichtbar	sie wird verwendet	konkrete Auswahl zum Ziel prüfen
niedrigste Metrik gewinnt immer	Route ist bevorzugt	längstes passendes Präfix zuerst
Hinweg funktioniert	Verbindung muss funktionieren	Rückweg kann fehlen
asymmetrischer Pfad	zwingend Fehlkonfiguration	kann beabsichtigt, aber für Stateful-Systeme problematisch sein
Route hinzufügen behebt Zugriff	Ursache ist gelöst	ursprünglicher Routingfehler kann verdeckt sein
VPN verbunden	interne Routen sind korrekt	konkrete Zielroute prüfen
Ping über IP funktioniert	DNS und Anwendung funktionieren	nur IP-/ICMP-Test bestätigt

30. Wie sieht der systematische Prüfablauf aus?

Schritt	Prüfung
1	Quell- und Zieladresse eindeutig bestimmen
2	Präfix des Clients prüfen
3	feststellen, ob das Ziel lokal oder entfernt ist
4	aktuelle Routingtabelle unverändert sichern
5	ausgewählte Route zum konkreten Ziel bestimmen
6	Ausgangsschnittstelle, Quelladresse und Next Hop prüfen
7	direkten Next Hop über ARP beziehungsweise NDP kontrollieren
8	Ziel per IP und passendem Dienst testen
9	Pfad mit Traceroute oder vergleichbarem Werkzeug untersuchen
10	Router- und Firewallrouting entlang des Pfades prüfen
11	Rückroute vom Ziel zur tatsächlichen Quelladresse kontrollieren
12	VPN, Policy Routing, VRF und NAT berücksichtigen
13	Routingtabellen redundanter Systeme vergleichen
14	Hypothese mit Mitschnitt oder gezieltem Test bestätigen
15	Änderungen nur mit Freigabe und Rückweg durchführen

Schritt	Prüfung
16	Funktion und Nebenwirkungen abschließend prüfen

Merksatz

> Ziel bestimmen → Longest Prefix Match → Quelladresse
> → Interface → Next Hop → Hinweg → Rückweg

31. Kompakte Befehlsübersicht für Windows, Linux und macOS

Aufgabe	Windows	Linux	macOS
IPv4-Routen	`[RO] Get-NetRoute -AddressFamily IPv4`	`[RO] ip -4 route`	`[RO] netstat -rn -f inet`
IPv6-Routen	`[RO] Get-NetRoute -AddressFamily IPv6`	`[RO] ip -6 route`	`[RO] netstat -rn -f inet6`
klassische Gesamtausgabe	`[RO] route print`	`[RO] ip route show table all`	`[RO] netstat -rn`
IPv4-Standardroute	`[RO] Get-NetRoute -DestinationPrefix '0.0.0.0/0'`	`[RO] ip route show default`	`[RO] route -n get default`
IPv6-Standardroute	`[RO] Get-NetRoute -DestinationPrefix '::/0'`	`[RO] ip -6 route show default`	`[RO] netstat -rn -f inet6`
Route zu IPv4-Ziel	`[RO] Find-NetRoute -RemoteIPAddress ZIEL`	`[RO] ip route get ZIEL`	`[RO] route -n get ZIEL`
Route zu IPv6-Ziel	`[RO] Find-NetRoute -RemoteIPAddress ZIEL`	`[RO] ip -6 route get ZIEL`	`[RO] route -n get -inet6 ZIEL`
Routingregeln	Windows-Routingauswahl prüfen	`[RO] ip rule show`	Systemroutingtabelle prüfen
Schnittstellenmetrik	`[RO] Get-NetIPInterface`	Routingmetriken in `ip route`	Routenflags und Dienstreihenfolge
Pfad ohne DNS	`[TEST] tracert -d ZIEL`	`[TEST] traceroute -n ZIEL`	`[TEST] traceroute -n ZIEL`
längere Pfadmessung	`[TEST] pathping -n ZIEL`	`[TEST] mtr -n -r -c 20 ZIEL`	`[TEST] mtr -n -r -c 20 ZIEL`
TCP-Port prüfen	`[TEST] Test-NetConnection ZIEL -Port 443`	`[TEST] nc -vz -w 5 ZIEL 443`	`[TEST] nc -vz -w 5 ZIEL 443`
Route hinzufügen	`[PRIV][CHANGE][DISRUPT] New-NetRoute …`	`[PRIV][CHANGE][DISRUPT] sudo ip route add …`	`[PRIV][CHANGE][DISRUPT] sudo route -n add …`
Route entfernen	`[PRIV][CHANGE][DISRUPT] Remove-NetRoute …`	`[PRIV][CHANGE][DISRUPT] sudo ip route del …`	`[PRIV][CHANGE][DISRUPT] sudo route -n delete …`

`mtr` und teilweise `traceroute` sind nicht auf jeder Linux-Installation standardmäßig vorhanden. Fehlende Werkzeuge dürfen nur aus einer freigegebenen Paketquelle installiert werden.

32. Dokumentationsvorlage

Ticketnummer:

Prüfzeitpunkt:

Zeitzone:

Betroffener Client:

Standort:

VLAN:

VPN aktiv: Ja / Nein

QUELLE

Hostname:

IPv4-Adresse/Präfix:

IPv6-Adresse/Präfix:

Schnittstelle:

Schnittstellenindex:

Schnittstellenmetrik:

MAC-Adresse:

ZIEL

Hostname:

Ziel-IPv4:

Ziel-IPv6:

Zielport:

Transportprotokoll:

Ziel laut Clientpräfix lokal: Ja / Nein

AUSGEWÄHLTE ROUTE

Adressfamilie:

Zielpräfix:

Präfixlänge:

Quelladresse:

Ausgangsschnittstelle:

Next Hop:

Routenmetrik:

Schnittstellenmetrik:

Routenursprung:

Routingtabelle/VRF:

Policy-Regel:

Direkter Nachbar aufgelöst:

Nachbar-MAC:

STANDARDROUTEN

IPv4-Standardroute:

IPv4-Next-Hop:

IPv4-Schnittstelle:

IPv4-Metrik:

IPv6-Standardroute:

IPv6-Next-Hop:

IPv6-Schnittstelle:

IPv6-Metrik:

PFAD

Hop 1:

Hop 2:

Hop 3:

Hop 4:

Letzter antwortender Hop:

Ziel erreicht:

Sternchen oder Timeouts:

Schleife erkennbar:

Pfadänderungen:

RÜCKWEG

Tatsächliche Quelladresse:

Route des Zielsystems zur Quelle:

Next Hop des Zielsystems:

Beteiligte Router:

Beteiligte Firewalls:

Asymmetrischer Weg:

NAT beteiligt:
Rückantwort am Ziel sichtbar:
Rückantwort am Client sichtbar:

VPN/POLICY ROUTING

Full Tunnel oder Split Tunnel:
Vom VPN installierte Route:
Überlappendes lokales Netz:
Policy-Regel:
Separate Routingtabelle:
Tunnelinterface:

REFERENZVERGLEICH

Referenzclient:
Ausgewählte Route:
Quelladresse:
Next Hop:
Pfad:
Relevante Abweichungen:

Arbeitshypothese:
Begründung:
Gesicherte Routingtabelle:
Geplante Änderung:
Freigabe:
Rückweg:
Tatsächliches Ergebnis:
Abschlussprüfung:
Ermittelte Ursache:

33. Offizielle Quellen und weiterführende Dokumentation

Microsoft

- Get-NetRoute
- Find-NetRoute

- Get-NetIPInterface
- New-NetRoute
- Remove-NetRoute
- Test-NetConnection
- route
- tracert
- pathping

Linux

- ip-route – Linux Manual Page
- ip-rule – Linux Manual Page
- ip-vrf – Linux Manual Page
- traceroute – Linux Manual Page

Apple

- Lokale Befehlsreferenzen: `man route`, `man netstat`, `man traceroute` und `man nc`

Wireshark

- IPv4 Display Filter Reference
- IPv6 Display Filter Reference
- ICMP Display Filter Reference
- ICMPv6 Display Filter Reference

Standards

- RFC 1812 – Requirements for IPv4 Routers
- RFC 8200 – IPv6 Specification
- RFC 792 – Internet Control Message Protocol
- RFC 4443 – ICMPv6

> Routingbefehle auf Firewalls, Routern, Layer-3-Switches und VPN-Gateways sind herstellerabhängig. Für Änderungen muss die offizielle Dokumentation der tatsächlich eingesetzten Plattform verwendet werden.