

Fehlersuche in konvergenten Netzen

von

**Oliver Flüs
Dietlind Hübner
Hartmut Kell
Joachim Wetzlar**

6.3 IP-Routing und Fehlersuche

6.3.1 Dynamisches IP-Routing ist „robust“

Generell sind Routingprotokolle für IP ausgereift und daher in der Praxis sehr stabil. Von daher sollte man erwarten, dass hier keine „Baustelle“ für die Fehlersuche besteht, sofern nicht Routingkomponenten ausfallen und dadurch sofortiger Handlungsbedarf entsteht, bzw. Erst-Konfigurationen oder Konfigurationsänderungen fehlerhaft sind und sich entsprechend zeigen.

Genau hier ist aber ein erstes Thema, dass die eigentlich etablierte Routingthematik in der letzten Zeit wieder stärker zum Gegenstand der Fehlersuche werden lässt: In der Vergangenheit wurden mindestens im LAN gerne „einfache“ dynamische Routingverfahren, v.a. RIP, eingesetzt, und es wurde auf Eingriffe über statisches Routing verzichtet, schon um sich unnötige Konfigurationsarbeit zu ersparen. Die mit RIP und einer einfachen redundanten Wegführung erzielbaren automatischen Redundanzen erschienen ausreichend und wurden schon als Fortschritt empfunden gegenüber der Notwendigkeit, bei Ausfall einer Strecke oder Routingkomponente „von Hand“ eine Ersatzschaltung zu schaffen.

Diese Situation hat sich in den letzten Jahren grundlegend verändert:

- Statisches Routing wird zum Teil gezielt eingesetzt, um Security-Belange so wenig wie möglich dynamischen Entscheidungen durch die Komponenten anzuvertrauen.

Z.B.: jeglicher Verkehr „nach außen“ wird über eine Sicherheitsbarriere mit Firewall u.ä. geführt, dabei wird dieser Weg über statische Routen an bestimmten Stellen erzwungen.

- Die Anforderungen an Redundanz im LAN sind so hoch, dass die Konvergenznachteile eines vector distance-Protokolls wie RIP nicht akzeptabel erscheinen, und Layer-2-Redundanzlösungen auf standardisierter, Hersteller-unabhängiger Basis waren lange Zeit auf Spanning Tree-Verfahren mit nicht mehr als akzeptabel angesehenen Umschaltzeiten reduziert.

RIP als „vector distance“-Protokoll stellt für „schnelles Umschalten“ keine gute Alternative dar: Hier werden in regelmäßigen Abständen die Routingtabellen unter benachbarten Routern ausgetauscht und „zusammengemischt“. Dabei bleibt ein längst ausgefallener Weg noch so lange registriert, bis auch „der Letzte“ die Sinnlosigkeit bemerkt hat, in Richtung eines gestörten Router-Anschlusses noch Pakete weiterzuleiten, und dies kann eine Weile dauern. Der Grund für diese langsame Verbreitung der Erkenntnis des Wegfalls von bislang verfügbaren Wegen besteht in der Tatsache, dass nicht alle Router gleichzeitig dieselben Informationen über verfügbare Wege haben, sondern nur „Next-Hop“-Einzelninformationen über ein „Schneeball-Prinzip“ austauschen. Einzelheiten zu den hiermit verbunde-

nen typischen Effekten wie „count to infinity“ können in jedem Grundlagenbuch zu TCP/IP nachgelesen werden (Routinginformationen, die in Konsequenz vermeintliche Nutzbarkeit von Wegen über den gestörten Router bedeuten, „kreisen“ zwischen den Routern und müssen zunächst mühsam durch schrittweises Neu-Registrieren in den Routingtabellen mit erhöhten Kosten entwertet werden.)

Damit geht der Trend zum Einsatz von komplizierteren Routingprotokollen, v.a. OSPF, das als Link-State-Protokoll deutlich bessere „Konvergenzeigenschaften“ hat. Bessere Konvergenz bedeutet, dass alle Router sich früher auf die neue Situation eingestellt haben und Ersatzwege tatsächlich auf allen durchlaufenen Routern „richtig“ gewählt werden.

Eine Vielzahl von LAN-Backbones wird heutzutage mit Layer-3-Switches und auf Basis von OSPF-Routing aufgebaut, um genau die gute Konvergenz von OSPF zu nutzen und damit eine „schnell schaltende“ Redundanz zu haben. Auf Grund dieser Entwicklung kann man sich für die Fehlersuche nicht auf den Standpunkt stellen, mit einer korrekten Konfiguration durch kundige Spezialisten in der Installationsphase kann man das Thema „abhaken“ und braucht sich nicht weiter mit den Einzelheiten zu beschäftigen. Allerdings muss wegen der Komplexität der Mechanismen eine gezielte Auswahl getroffen werden, was in der Fehlersuche-Praxis angesichts des Zeitdrucks lohnt, ohne gezielten Verdacht systematisch untersucht zu werden. Dies und typische Aspekte der Diagnose im Routingbereich sollen im Weiteren diskutiert und vorgeführt werden.

Man muss spätestens nach Durchführung entsprechender systematischer Tests (etwa: Kabel Ziehen oder ähnliche Problemprovokation im Bereich von OSPF-Router-links), die zum erwarteten Umschalten führen, von einer prinzipiell fehlerfrei arbeitenden OSPF-Software ausgehen. Der Versuch, auf Grund der zwischen den Routern ausgetauschten Informationen das „Funktionieren“ des Routing Schritt für Schritt nachzuvollziehen, mag also vielleicht interessant und lehrreich sein, für die zu schnellen Ergebnissen „verdammte“ Fehlersuche ist dies aber zu aufwändig.

Typische Fehlersuche-Ansätze in heutigen Netzen sind vielmehr:

- Prüfen von Routingtabellen auf „Stimmigkeit“ zur Situation und Netzwerkstruktur
- Beobachten des Informationsaustauschs zwischen den Routern, Prüfen auf Auffälligkeiten in Paketen bzw. deren Versendezeitpunkten und Abfolge
- Überprüfen der an Paketflüssen ablesbaren Routingentscheidungen gegen die kontrollierten Routingtabellen:

Arbeitet der Router die Routingtabelle „richtig ab“? Wenn nicht, besteht bei wie angenommen korrektem Verhalten der Software ein Problem der Komponente in dem Sinne, dass diese die angezeigten Inhalte der Routingta-

belle nicht wirklich genau wie angezeigt ihrer Transportentscheidung zugrunde legt. Eine typische Erklärung ist etwa ein Ressourcenproblem auf dem Router. Dieser Verdacht kann etwa dadurch erhärtet werden, dass ein Neustart zumindest kurzfristig wieder zu korrektem Verhalten führt. (Stellt sich nach einer zeitweilig höheren Belastung das Problem wieder ein, kann und sollte etwa nach der Ursache der Belastung gesucht werden.)

Um hier mögliche Ursachen zu ermitteln, ist es wichtig, die im Moment einer Änderung im Sinne von Wegfall oder (Wieder-)Hinzukommen von funktionsfähigen Router-Links ausgetauschten Pakete zu inspizieren und auf korrekte Inhalte, Abläufe und Abfolge zu überprüfen. Dies setzt voraus, dass wesentliche „Felder“ in solchen Paketen verstanden und den entsprechenden Routern / Router-Interfaces zugeordnet werden können:

Redundanzmechanismen helfen einerseits, die Verfügbarkeit des Netzwerks aus Sicht der Anwender zu erhöhen, sie erhöhen aber andererseits auch die Komplexität der insgesamt vom Betreiber / Fehlersucher zu beherrschenden Mechanismen. Eine nicht wie vorgesehen funktionierende Redundanz kann ihrerseits zur Problemursache werden oder zumindest beitragen. Komplexere Mechanismen beinhalten in der Regel auch aufwändigere Konfigurationsmöglichkeiten und damit mehr Möglichkeiten, bei der Konfiguration Fehler zu machen und damit Probleme heraufzubeschwören, so auch bei OSPF. Zwar ist prinzipiell eine Router-Konfiguration eine Planungsaufgabe und damit ein diesbezüglicher Fehler ein Planungsfehler. Gerade bei redundanzspezifischen Mechanismen werden solche Fehler aber möglicherweise erst bei bestimmten Konstellationen spürbar, die durch Ausfälle entstehen, und damit das eigentliche Planungsthema zum Aspekt der Fehlersuche in einem produktiven Netzwerk.

Durch diese Entwicklungen und Erkenntnisse ist das Thema „Routing“ zu einer neuen Brisanz auch im LAN gekommen und rückt im Vergleich zu früher stärker in den Aufgabenbereich der Fehlersuche.

Im Weiteren soll daher auf Aspekte eingegangen bzw. hingewiesen werden, die im Rahmen der Fehlersuche mögliche Ansatzpunkte darstellen können.

6.3.2 Die Routingentscheidungen überprüfen

6.3.2.1 Ein Routingentscheidungsweg für alle Fälle

Unabhängig davon, wie die Routingtabelle zustande kommt (d.h., woher die dort verwalteten Informationen stammen und wann / in welcher Form die Update-Informationen zwischen den Routern verschickt werden), ist bei gegebener Routingtabelle der Weg zur Entscheidung für den Next Hop immer der gleiche.

Es werden bestimmte Schritte durchlaufen, durch die nacheinander der „beste“ bekannte Weg zum Ziel, nämlich der IP Destination Address eines zu transportierenden Pakets, aus der Routingtabelle ermittelt wird.

Jeder Eintrag in einer Routingtabelle umfasst drei maßgebliche Informationen:

- eine Zielangabe;
Dies kann ein Netzwerk/ Subnetz (in der Regel unter Angabe einer Maske, die den Umfang des Adressbereichs festlegt) oder eine einzelne IP-Adresse (Fall: Host-Route) sein, bzw. (Defaultroute) die Angabe 0.0.0.0 .
- eine Metrik;
Hiermit wird in Form einer Kennzahl der Next Hop zum Ziel bewertet.
- eine Next-Hop-Adresse.
Dies ist die IP-Adresse des Routinginterfaces, an das ein Paket weiterzugeben ist, sofern die zugehörige Route entsprechend der vorgeschriebenen Routingentscheidung die günstigste ist. Diese Adresse selbst wird in die Entscheidungsfindung nicht einbezogen, sondern nur die ersten beiden Informationen.

6.3.2.2 Warum Routingentscheidungen nachvollziehen?

Wozu ist es nun aus Sicht der Fehlersuche interessant, sich mit den Schritten der Entscheidungsfindung zu beschäftigen?

Zwar sind prinzipiell die etablierten dynamischen Routingprotokolle wie erwähnt so lange „im Einsatz“, dass grundlegende Schnitzer in der Implementierung kaum noch zu erwarten sind. Allerdings können bestimmte Situationen entstehen, in denen eine Routingkomponente „Fehler“ macht, indem sie die bei Kontrolle gezeigten Routing-Table-Inhalte nicht mehr vollständig verwendet (dieser Effekt ist auch von Layer-2-Switches / Bridging bekannt: wenn Komponenten an den Rand ihrer Leistungsfähigkeit kommen, wird die Verwaltung dynamischer Informationen fehlerhaft). Noch wichtiger ist aber der Fall, in dem statische Routen, also manuell festgelegte, mit dynamisch gelernten kombiniert auftreten. Dies hat spätestens mit der Bedeutung des Securityaspekts zugenommen. Auch Maßnahmen zur Reduzierung der Inhalte von Routingtabellen führen zu manuellen Eingriffen derart, dass Routen gezielt „zusammengefasst“ werden. Bei derartigen „Festkonfigurationen“ von Routen kann es geschehen, dass je nach Problemsituation (teilweiser Ausfall der „normalerweise“ vorgesehenen Wege) Konstellationen entstehen, die zu nicht sinnvollen Ergebnissen der Routingentscheidung führen.

In der abgebildeten Routingtabelle sind sowohl dynamisch „erzeugte“ („originated“) Einträge enthalten (Spalte „Ori“, Kennung „d“ für direct, d.h. direkt angeschlossene Netze bzw. „oa“ für von anderem OSPF-Router gelernt) als auch eine statische Route (erste Zeile, „Ori“-Kennung „s“).

Ori	Destination	Gateway	Mtr
*s	149.224.129.160/32	149.224.5.13	1
*d	149.224.1.0/24	149.224.1.14	1
*d	149.224.5.0/24	149.224.5.14	1
*d	149.224.6.0/24	149.224.6.14	1
*d	149.224.14.0/24	149.224.14.14	1
*oa	149.224.128.0/23	149.224.14.1	11
*d	127.0.0.1/8	127.0.0.1	0

Origin (Ori):
b - Black hole, be - EBGp, bi - IBGP, bo - BOOTP, ct - CBT, d - Direct
df - DownIF, dv - DVMP, h - Hardcoded, i - ICMP, mo - MOSPF, o - OSPF
oa - OSPFIntra, or - OSPFInter, oe - OSPFAsExt, o1 - OSPFExt1, o2 - OSPFExt2
pd - PIM-DM, ps - PIM-SM, r - RIP, ra - RtAdvrt, s - Static,
sv - SLB_VIP, un - UnKnown

Abbildung 6.28: Beispiel für eine Routingtabelle

In solchen Momenten muss der Diagnosespezialist in der Lage sein, für ein betrachtetes Ziel und eine zur Überprüfung abgerufene aktuelle Routingtabelle

- zu prüfen, ob die mit einer Protokoll-Analysator-Messung bestimmbare Transportentscheidung der Routingkomponente auf Basis der abgefragten Routingtabelle korrekt ist, bzw.
- ob die so zustande kommende Kette von Entscheidungen auf dem Weg vom Sender eines Pakets zum Empfänger womöglich in der konkreten Problemsituation dazu führt, dass der Empfänger nicht erreicht werden kann, obwohl physikalisch gesehen ein funktionsfähiger Weg zu ihm zur Verfügung steht.

Je nach Ergebnis der Prüfung können unterschiedliche Maßnahmen notwendig sein. Entscheidet der Router „falsch“ bei korrekt aussehender abgefragter Routingtabelle, so liegt ein Verdacht auf die eben erwähnte „Überlastung“ nahe. Man kann hier entweder mit Hilfe eines entsprechenden Befehls versuchsweise die Routing-Table löschen und einen Neuaufbau erzwingen, oder den Router neu starten und so auch ein „Aufräumen“ des Speichers erzwingen.

Entscheidet der Router nachvollziehbar, die Entscheidung führt jedoch zu einem Umweg oder gar nicht zum Ziel, so ist zu überprüfen, warum die zur Entscheidung gehörige Route zustande kam. Oft ist es eine von Hand konfigurierte, und die konkrete Konstellation von verfügbaren Next Hops bzw. Next-Hop-Abfolgen wurde nicht vorausgesehen. Bei der Planung manueller Routen-Einträge hat man im Wesentlichen die Situation vor Augen, in der alle Routing-interfaces funktionieren; alle möglichen, durch Ausfälle vielleicht einmal zustande kommenden Konstellationen werden selten systematisch durchgespielt, schon gar nicht bei größeren Netzen. Möglicherweise lässt sich durch eine Änderung der Metrik, d.h. der „Kosten“ der Route eine solche manuell definierte Route so abwandeln, dass sie nur noch dann zum Zuge kommt, wenn sie die einzige Alternative darstellt, zum Ziel zu gelangen. Eventuell muss auf die stati-

sche Route in der bisherigen Form auch verzichtet werden, um zukünftig die erlebte Fehlersituation zu vermeiden.

6.3.2.3 Routingtabellen bei Servern und Endgeräten und der Redirect

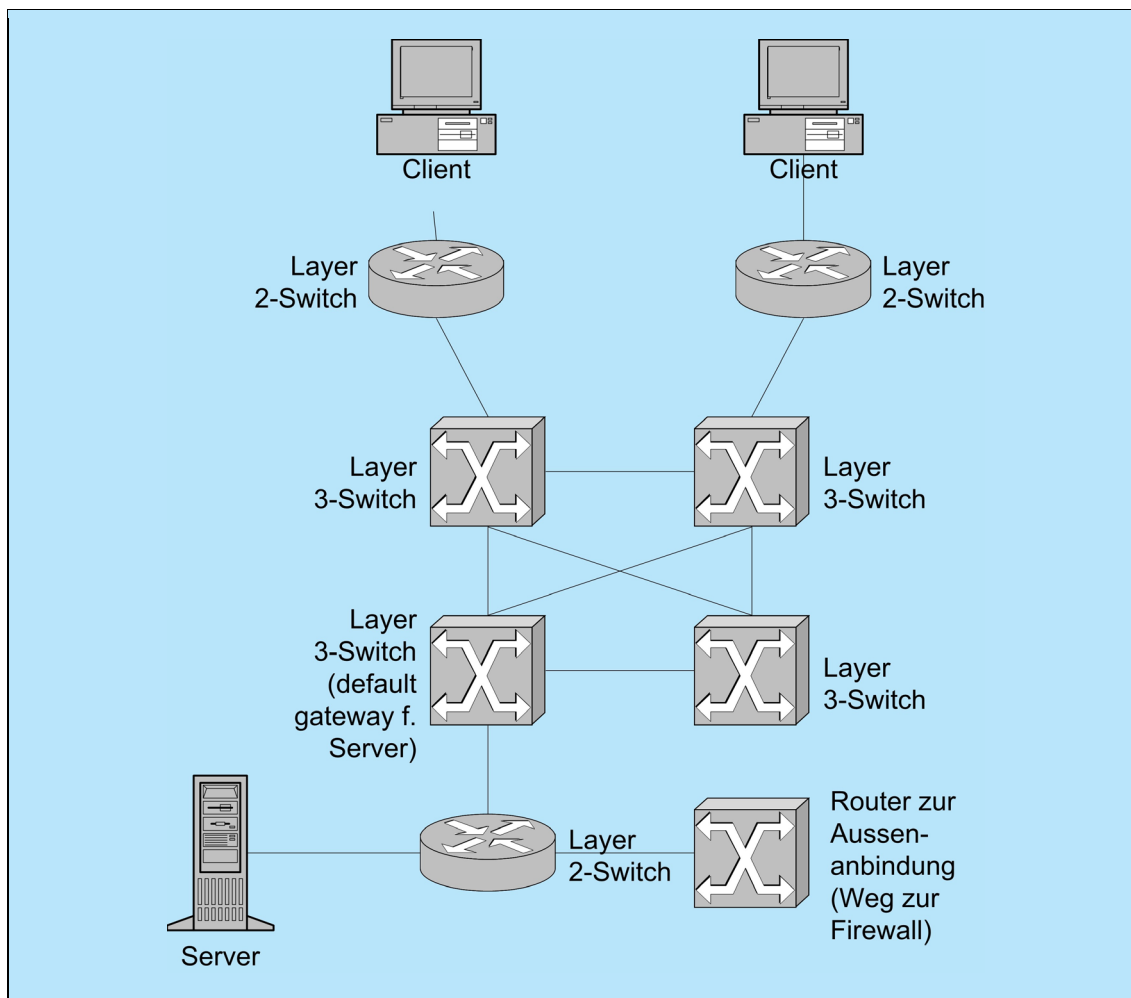


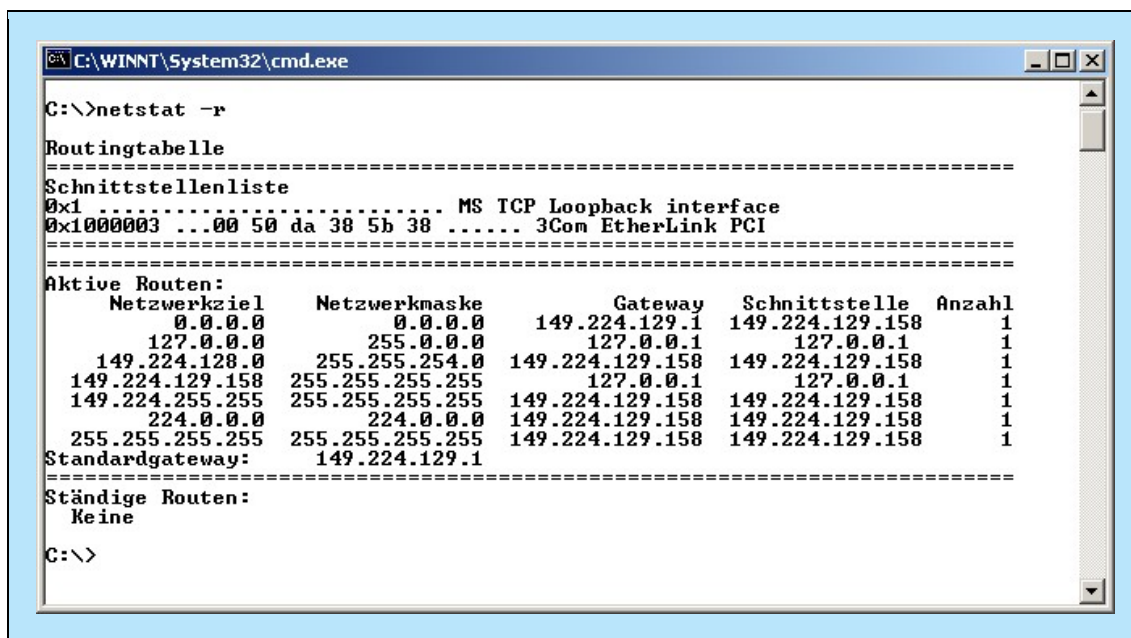
Abbildung 6.29: Beispiel für Bedarf zu punktueller Korrektur der Defaultroute

Wichtig ist dabei, dass nicht nur Routingkomponenten Routingtabellen führen. Auch IP-„Hosts“, d.h. etwa Endgeräte und Server tun dies zur „First-Hop“-Bestimmung beim Sendevorgang. Nicht immer ist eine Defaultroute allein ausreichend, um die Routingschnittstelle optimal auszuwählen, der ein zu sendendes Paket übergeben wird.

Solange der exemplarisch eingetragene Server Rückantworten zu Clients im abgebildeten LAN schickt, ist das Default-Gateway der optimale First Hop. Wird der Server aber auch via WAN-Verbindung, etwa von einem Nachbarstandort, mitgenutzt, so führt das Beharren auf dem Default-Gateway als First Hop zu einem vermeidbaren Umweg: ein Paket vom Server „nach draußen“ geht dann

erst an sein Default-Gateway, dieses leitet dann an den Router zur Außenanbindung weiter. Diesen hätte der Server aber gleich selbst ansprechen können!

Führt nun ein IP-Teilnehmer wie der Server eine dynamische Routingtabelle, so kann er für Ziele, die über den Router zur Außenanbindung zu erreichen sind, den besseren Next Hop „lernen“ und in diese Tabelle eintragen.



```

C:\WINNT\System32\cmd.exe

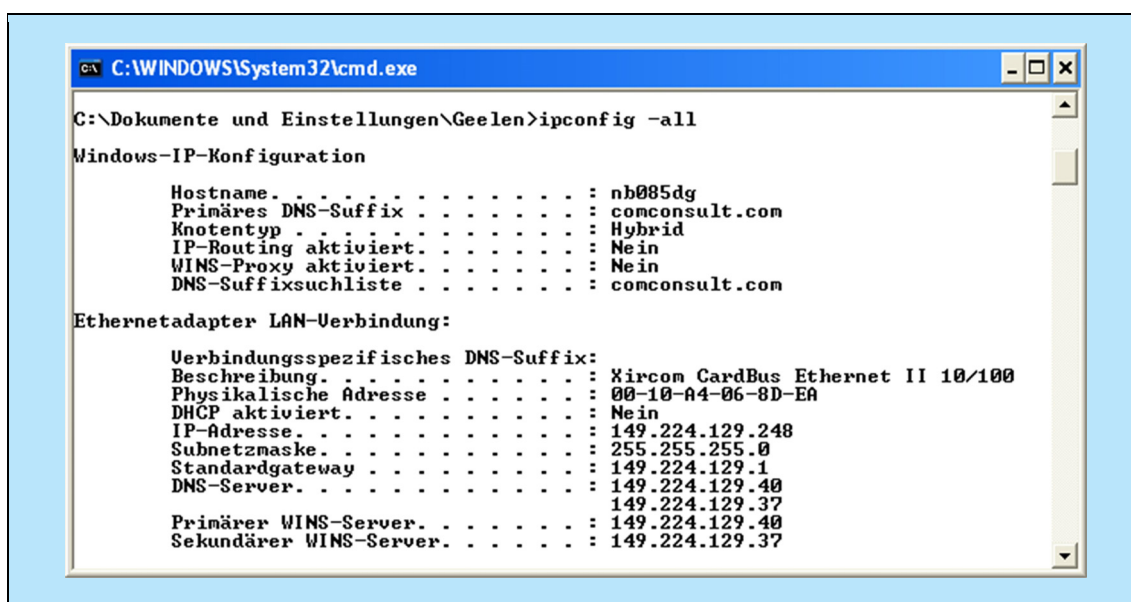
C:\>netstat -r

Routingtabelle
=====
Schnittstellenliste
0x1 ..... MS TCP Loopback interface
0x1000003 ...00 50 da 38 5b 38 ..... 3Com EtherLink PCI
=====
Aktive Routen:
Netzwerkziel   Netzwerkmaske   Gateway   Schnittstelle   Anzahl
0.0.0.0        0.0.0.0         149.224.129.1  149.224.129.158  1
127.0.0.0      255.0.0.0       127.0.0.1     127.0.0.1        1
149.224.128.0  255.255.254.0   149.224.129.158  149.224.129.158  1
149.224.129.158  255.255.255.255  127.0.0.1     127.0.0.1        1
149.224.255.255  255.255.255.255  149.224.129.158  149.224.129.158  1
224.0.0.0      224.0.0.0       149.224.129.158  149.224.129.158  1
255.255.255.255  255.255.255.255  149.224.129.158  149.224.129.158  1
Standardgateway: 149.224.129.1
=====
Ständige Routen:
Keine

C:\>

```

Abbildung 6.30: Beispiel für (Abruf) eine(r) Routingtabelle auf einem Windows-Rechner



```

C:\WINDOWS\System32\cmd.exe

C:\Dokumente und Einstellungen\Geelen>ipconfig -all

Windows-IP-Konfiguration

    Hostname. . . . . : nb085dg
    Primäres DNS-Suffix . . . . . : comconsult.com
    Knotentyp . . . . . : Hybrid
    IP-Routing aktiviert. . . . . : Nein
    WINS-Proxy aktiviert. . . . . : Nein
    DNS-Suffixsuchliste . . . . . : comconsult.com

Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : Xircom CardBus Ethernet II 10/100
    Physikalische Adresse . . . . . : 00-10-A4-06-8D-EA
    DHCP aktiviert. . . . . : Nein
    IP-Adresse. . . . . : 149.224.129.248
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . : 149.224.129.1
    DNS-Server. . . . . : 149.224.129.40
                          149.224.129.37

    Primärer WINS-Server. . . . . : 149.224.129.40
    Sekundärer WINS-Server. . . . . : 149.224.129.37

```

Abbildung 6.31: Konfiguration mit falscher (zu scharfer) Subnetzmaske