



7 Switching und Routing



7.1 Switching

Switches arbeiten auf dem OSI-Layer 2, dem Data Link Layer, bzw. auf dem TCP/IP-Layer 1, dem Network-Access-Layer. Sie treffen ihre Entscheidung, wohin ein Datagramm weitergeleitet werden muss, anhand der MAC-Adresse. Switches verbinden Netzwerksegmente *eines* Netzwerkes miteinander. Jeder Switchport bildet ein eigenes Netzwerksegment.

Es wird nun zuerst die Arbeitsweise eines Switches betrachtet. Was macht ein Switch, wenn er einen Datenrahmen empfängt?

L7	Application
L6	Presentation
L5	Session
L4	Transport
L3	Network
L2	Data Link
L1	Physical



Bild 7.1: Entscheidungspunkt

7.1.1 Fast-Forward-Switch

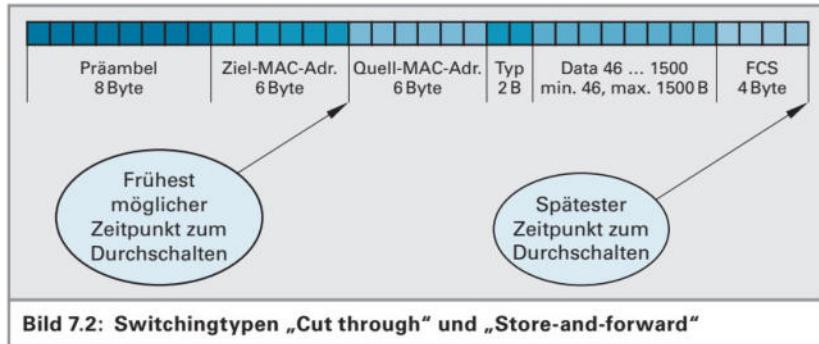
Bild 7.2 zeigt den Layer-2-Datenrahmen, einen Ethernetframe. Dabei erhält ein Empfänger zuerst eine 8 Byte lange Präambel.

Fast-Forward-Switch:
schnell, aber fehlerbehaftet

Danach folgt die Zieladresse des adressierten Rechners. Nachdem die Zieladresse beim Switch angekommen ist, kann der Switch schon die Entscheidung treffen, an welchem Switchport er diesen Rahmen wieder

7 Switching und Routing

ausgibt. Die maximale Verzögerungszeit beträgt somit 14 Byte-Zeiten. Ein großer Nachteil dieser schnellen Switching-Technik ist allerdings, dass Rahmen, die weiter hinten abgebrochen oder durch irgendwelche Störungen unbrauchbar geworden sind, trotzdem weitergeleitet werden, da sie zu diesem frühen Zeitpunkt ja noch völlig in Ordnung sind. Treten häufig Kollisionen oder Störungen in einem Netzwerk auf, so werden die defekten Frames mit dieser Switching-Technologie trotzdem weitergeleitet.



7.1.2 Store-and-Forward-Switch

Store-and-Forward-Switch: langsam, aber sicher

Eine sehr sichere Switching-Technologie ist die **Store-and-Forward**-Technologie. Hierbei wird ein Frame komplett vom Switch empfangen, inklusive Prüfsumme am Frameende. Diese Rahmenprüfsumme wird beim Empfangen laufend mit kalkuliert und am Ende mit der empfangenen Prüfsumme FCS verglichen. Ist das Datagramm unverfälscht, stimmt die Prüfsumme überein. In diesem Fall wird der Frame an dem entsprechenden Port in Richtung Zielrechner ausgegeben. Defekte Rahmen werden nicht weitergeleitet und im Switch verworfen. Dasselbe gilt für zu kurze und auch für zu lange Frames. Sie werden ebenfalls im Switch verworfen. Es erfolgt keine Fehlermeldung an den Sender. Die Überwachung auf korrektes Zustellen der Daten muss eine übergeordnete Schicht leisten.

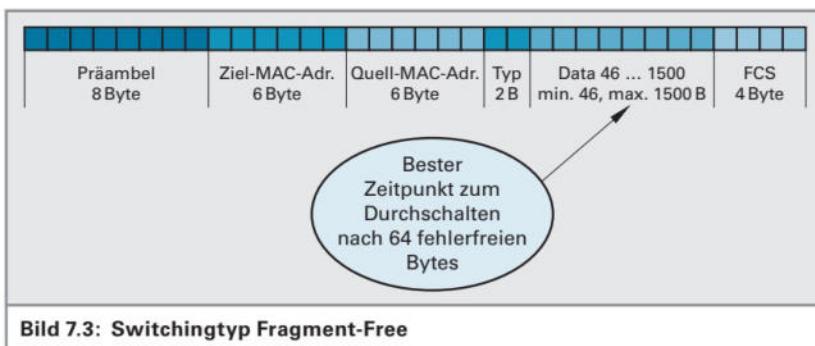
Der Nachteil dieser Technologie ist, dass der ganze Rahmen im Switch gespeichert werden muss und erst dann weitergeleitet werden kann. Die Verweilzeit im Switch ist also maximal. Weiterhin benötigt der Switch mehr RAM-Speicher als ein Fast-Forward-Switch um die Messages zu puffern.

7.1.3 Fragment-Free-Switch

Fragment-Free-Switch: schnell und sicher

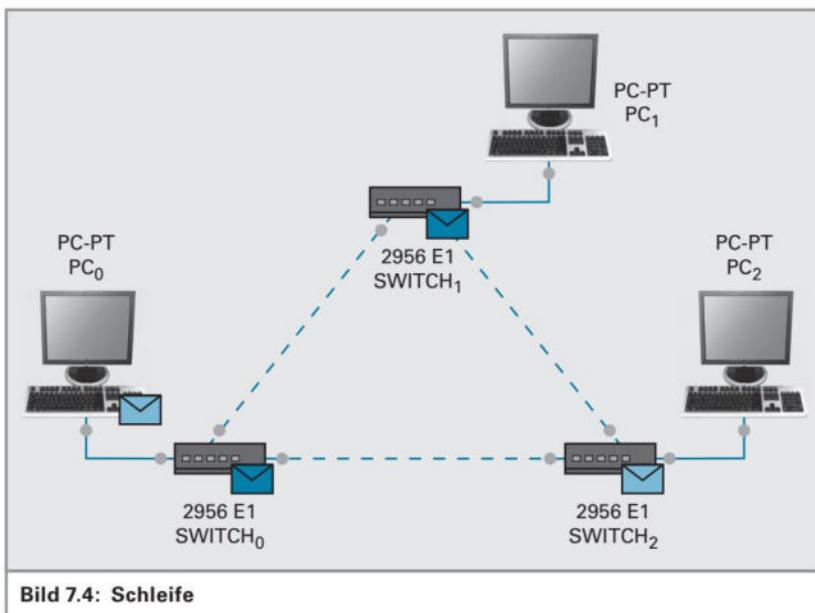
Die Erfahrung zeigt, dass die allermeisten defekten Frames innerhalb der ersten Bytes zerstört werden. Wenn man also die ersten Bytes fehlerfrei empfangen hat, so ist der Rest des Rahmens mit großer Wahrscheinlichkeit auch in Ordnung.

Diese Erkenntnis macht man sich zunutze um einen weiteren Switchtyp zu kreieren, den Fragment-Free-Switch. Dieser schaltet den eingehenden Datenstrom nach 64 korrekt empfangenen Bytes in Richtung Zielrechner weiter. Er ist fast so sicher wie ein Store-and-Forward-Switch und fast so schnell wie ein Fast-Forward-Switch. Fast-Forward-Switch und Fragment-Free-Switch nennt man auch „Cut-Through-Switches“.



7.1.4 Spanning Tree

In Kapitel 2.3 wurden strukturierte Gebäudeverkabelungen vorgestellt. Es wurde gezeigt, dass man eine erweiterte Sterntopologie verkabelt und aus Sicherheitsgründen Querverbindungen installiert. Nun wird betrachtet, was passiert, wenn man in die Verteiler Switches installiert und die Sicherheitsleitungen an die Switches anschließt: Es entstehen Schleifen (siehe Bild 7.4).



Sendet nun ein Rechner eine Broadcast-MESSAGE, beispielsweise eine ARP-Anfrage zur Adressauflösung, dann schickt der Switch diese Message an alle Ports weiter, natürlich auch an die benachbarten Switches. Diese schicken sie wiederum an alle Anschlüsse weiter usw. Dieses einzelne Broadcast-Datagramm kursiert nun im Netz auf allen Leitungen und wird nie mehr gestoppt. Es entsteht ein Broadcast-Sturm, der das komplette Netzwerk lahmlegt.

Eine Schleife in der Verkabelung erzeugt einen Broadcast-Sturm.

Schleifen müssen also unbedingt vermieden werden. Aus Sicherheitsgründen möchte man aber Schleifen haben.

7 Switching und Routing

Die Lösung sieht ganz einfach aus:

Querverbindungen werden zwar gesteckt, die Switchports werden allerdings nicht aktiviert. Fällt nun eine aktive Leitung aus, so muss nur die Querverbindung aktiviert werden, und der Betrieb kann weiter gehen.

Dieses Auftrennen von Schleifen durch Deaktivieren von gesteckten Leitungen, sowie das Aktivieren von Leitungen im Fehlerfall, muss der Switch selbständig übernehmen.

Spanning tree, Spanning tree protocol, STP (auch Spannbaum oder gespannter Baum) ist nun eine Methode in der Netzwerktechnik, um redundante geswitchte Netzwerke aufzubauen. Dabei wird jegliche Topologie auf eine einzige Baumstruktur reduziert, die in der Rootbridge (Wurzelbrücke) ihren Ursprung hat.

Jeder Switch ist durch seine BID (Bridge-Identification) eindeutig gekennzeichnet. Diese BID besteht aus 8 Byte, wobei die ersten, höchstwertigen Bytes eine vom Admin einstellbare Priorität sind. Die restlichen 6 Bytes ergeben sich aus der MAC-Adresse des Switches. Somit ist gewährleistet, dass jeder Switch eine eindeutige Kennung und somit auch eine eindeutige Priorität hat.

Tabelle 7.1: BID	
Priority	MAC-Adresse
2 Byte	6 Byte

*Je kleiner die **BID**-Nummer, desto höher die Priorität.*

Die niedrigste **BID** hat die höchste Priorität. Root-Bridge wird der Switch mit der höchsten Priorität. Alle anderen Switches suchen sich nun den bestmöglichen Pfad zur Rootbridge. Diese Verbindungen werden aktiviert, die restlichen deaktiviert.

Bei mehreren Verbindungen eines Switches zur Root-Bridge hin, die dieselben Pfadkosten aufweisen, wird der Port mit der höchsten Priorität aktiviert. Dies ist der Port mit der kleinsten Portnummer.

Der Pfad mit den geringsten Kosten ist der beste.

Um den bestmöglichen Pfad zur Rootbridge zu finden, muss die Beschaffenheit der Verbindung mit berücksichtigt werden. Als Entscheidungskriterium werden hier „Pfadkosten“ definiert (dies sind keine wirklichen Kosten). Eine schnelle Verbindung ist einer langsamen Verbindung vorzuziehen. Also definiert man für die langsame Verbindung hohe Pfadkosten, für die schnelle Verbindung geringe Pfadkosten. Als Pfadkosten können vom Administrator Werte von 1 bis 65536 eingestellt werden.

Anforderungen an den Spanning Tree Algorithmus:

- ▶ Automatisches Rekonfigurieren der Baumstruktur bei Änderungen an der Topologie (bei manuellen Änderungen oder bei auftretenden Fehlern)
- ▶ Möglichst geringe Netzlast durch das eigentliche Einrichten der Baumstruktur
- ▶ Stabilisierung der Netzstruktur unabhängig von der Netzgröße
- ▶ Stabilisierung innerhalb einer bekannten (kurzen) Zeit
- ▶ Vorbestimmte, reproduzierbare Netzstruktur, die durch den Netzwerkadmin vorgegeben wird

Tabelle 7.2: Empfohlene Pfadkosten, abhängig von der Übertragungskapazität

Übertragungskapazität	empfohlene Pfadkosten	empfohlener Bereich
10 MB/s	100	50 ... 600
100 MB/s	19	10 ... 100
1000 MB/s	4	2 ... 10
10 GB/s	2	1 ... 4

Der Rootpath (Wurzelpfad) ist der Pfad von einem Switch zur Rootbridge, der die geringsten Gesamtkosten aufweist (Summe aller Einzelpfade). Jeder Switch darf nur einen Pfad zur Rootbridge haben.

Bei mehreren Pfaden mit denselben Root-Pfadkosten wird die Priorität der Switchports interessant. Je kleiner die Switch-Port-Nummer (Anschlussnummer am Switch), desto höher die Priorität. Steckt also eine Leitung auf Port 2 und eine andere auf Port 5 und beide haben gleich hohe Wurzelpfadkosten, dann wird Port 2 der Rootport und Port 5 wird deaktiviert.

Die kleinste Bridge-ID hat die höchste Priorität!

Die kleinste Port-ID hat die höchste Priorität!

Bridge Protocol Data Unit

Die Switches müssen Daten über ihren eigenen Zustand und ihre ID austauschen. Dies geschieht mit PDPUs, Bridge Protocol Data Units.

Die Rootbridge teilt den untergeordneten Switches alle 2 Sekunden mit, dass sie noch vorhanden ist. Die untergeordneten Switches geben diese Meldungen weiter. Beim Ausbleiben dieser „Hallo-Pakete“ hat sich offensichtlich das Netzwerk verändert und muss neu organisiert werden. Die Reorganisation läuft genau so ab wie die Neuorganisation beim Einschalten eines Netzwerkes. Die Reorganisation kann bis zu 30 Sekunden dauern.

Ablauf der Netz-Organisation

1. Einschalten der Switches, alle Switchports sind im „Blocked-Modus“, d.h., es werden keine Datenpakete weitergeleitet außer den Switch-Informationen (BPDUs).
2. Jeder Switch sendet Informationen über seine ID an alle Anschlüsse. Der Switch mit der **kleinsten ID** wird Root-Bridge.
3. Nachdem die Root-Bridge ermittelt wurde, bestimmt jeder Switch seinen Root-Port. Das ist der Port, der mit den geringsten Kosten zur Rootbridge führt. Bei gleichen Kosten für mehrere Ports, wird der Port mit der **kleinsten Port-Nummer** der Root-Port. Die anderen Ports, die Wege zur Rootbridge haben, werden deaktiviert (Designated Ports).
4. Danach werden die Switchports in den „Learning-Modus“ gesetzt und die Bridging-Tabellen angelegt.
5. Nach Aufbau der Bridging-Tabellen schalten die Switches ihre Ports in den „Forwarding-Modus“ und transportieren fortan ankommende Datenpakete an die richtigen Ports weiter.

7 Switching und Routing

Vorsicht! Eine Verbindung an einem einzigen Switch von einem Switch-Port zu einem anderen verursacht auch einen Broadcaststurm! Einfache Switches können keine STP und können somit diese Schleife auch nicht auftrennen.

7.1.5 Virtuelle LANs, VLANs

In einem Großraumbüro befinden sich Mitarbeiter unterschiedlicher Abteilungen. Alle Arbeitsplätze sind miteinander vernetzt und „hängen“ auf einem Etagenswitch. Aus Sicherheitsgründen sollten aber die Rechner der verschiedenen Abteilungen jeweils in getrennten Netzen stehen, nämlich jeweils auf eigener Netzwerk-Hardware.

Ein weiteres Problem ist, dass Broadcast-Messages das Netz sehr belasten. Je größer die Anzahl der Rechner, desto größer die Anzahl der Broadcasts.

Lösung: Der Etagenswitch wird in mehrere „logische Switches“ aufgeteilt, die voneinander isoliert arbeiten.

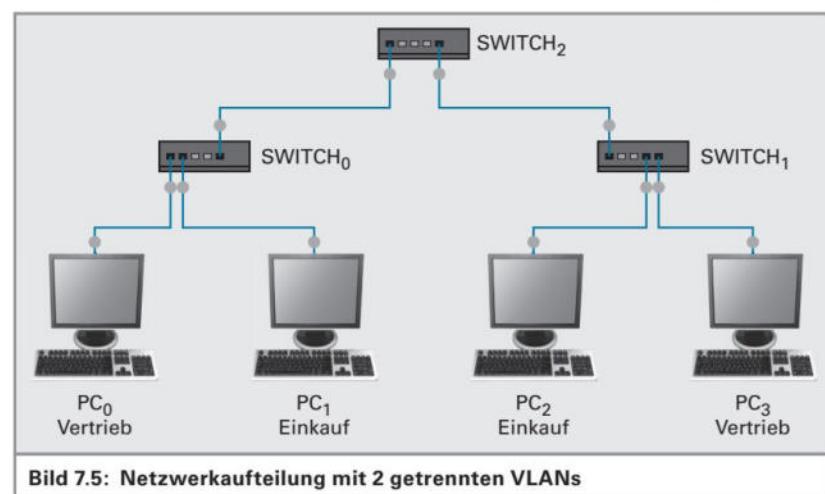
Bild 7.5 zeigt das Aufteilen in 2 getrennte virtuelle Netze, ein Netz *Vertrieb* und ein Netz *Einkauf*. Beide Netze nutzen zwar dieselben Switches, sind aber logisch völlig voneinander isoliert.

Damit zwei Rechner, die in unterschiedlichen VLANs stehen, miteinander kommunizieren können, müssen die VLANs über einen Router verbunden werden!

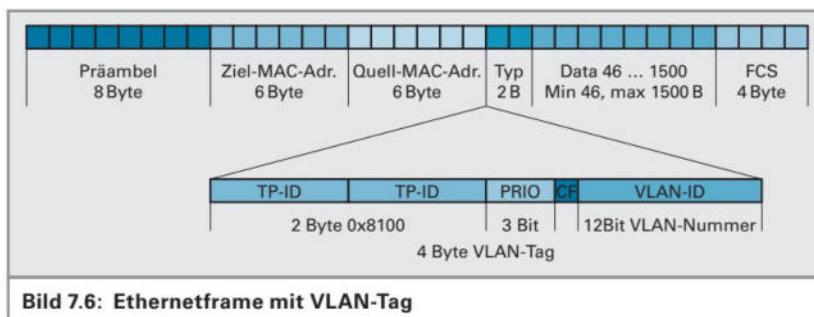
Jedes VLAN bildet ein eigenes Netz. Jedes LAN bildet eine Broadcastdomäne. Broadcasts bleiben somit im eigenen VLAN und gelangen nicht in andere VLANs.

Die Uplinks der einzelnen logischen Switches werden physikalisch zu einem Link zusammengefasst. Damit die Datenframes der einzelnen logischen virtuellen Netzwerke dem jeweiligen VLAN zugeordnet werden können, müssen die Frames modifiziert werden. Die Zugehörigkeit zum virtuellen Netzwerk muss zusätzlich im Frame transportiert werden.

Dazu wird ein VLAN-Tag eingebaut. Das VLAN-Tag ist 4 Byte groß und wird vor dem Typ-Feld im Ethernet-Frame eingefügt. Der Ethernetrahmen hat normalerweise eine maximale Größe von 1518 Bytes.



7.1 Switching



Durch den VLAN-Tag wird die Maximalgröße um 4 Byte auf 1522 Byte vergrößert (siehe Bild 7.6).

Der PC schickt einen normalen Datenrahmen heraus. Der Switch macht die Zuordnung zum virtuellen LAN und erweitert den Frame mit dem Tag. Der so gekennzeichnete Ethernetrahmen wird wie gewohnt durch das Netzwerk transportiert. Der letzte Switch entfernt diesen VLAN-Tag wieder, bevor er die Daten an den Zielrechner schickt.

Das VLAN-Tag besteht aus der Kennung **0x8100**, was anzeigt, dass hier eine VLAN-Kennung eingebaut wurde.

Dann folgen 3 Prioritätsbits. Hiermit lassen sich Datenströme innerhalb eines LANs priorisieren. So haben beispielsweise Telefonie-Daten eine höhere Priorität als Datei-Downloads oder E-Mail-Verkehr. Man nennt diese Einstellung **QoS**, Quality of Service, oder auch **CoS**, Class of Service (Tabelle 7.3).

Tabelle 7.3: Die 8 Prioritätsstufen im Einzelnen	
Priorität	Anwendung
7	reserved
6	reserved
5	voice services
4	video conferencing
3	excellent load
2	high priority data
1	medium priority data
0	best effort (so gut es geht)

Das CF-Bit steht für Canonical-Flag und gibt die Bit-Reihenfolge an, also ob das höchstwertige Bit (MSB) oder das niederwertigste Bit (LSB) zuerst übertragen wird. Token-Ring und Ethernet handhaben dies genau umgekehrt.

Im VLAN-Tag bleiben dann noch 12 Bit für die Kennung der virtuellen Netze. Somit sind 2^{12} VLANs realisierbar.

7 Switching und Routing

VLAN-Zuordnung

Es gibt verschiedene Möglichkeiten, wie ein PC oder auch ein einzelner Datenframe zu einem VLAN zugeordnet wird.

► **Switchport-Zuordnung (OSI-Layer 1)**

Ein Port, ein Steckplatz eines Switches, wird einem VLAN zugeordnet. Jeder PC, der an diesem Port eingesteckt wird, gehört zu diesem VLAN.

► **MAC-Adress-Zuordnung (OSI-Layer 2)**

Ein Datenframe wird anhand seiner Absender-MAC-Adresse einem VLAN zugeordnet. Jeder PC, der sich eine passende MAC-Adresse gibt, gehört zu diesem VLAN.

► **IP-Adress-Zuordnung (OSI-Layer 3)**

Ein Datenframe wird anhand seiner Absender-IP-Adresse einem VLAN zugeordnet. Jeder PC, der sich eine passende IP-Adresse gibt, gehört zu diesem VLAN.

► **Port-Zuordnung/Applikations-Zuordnung (OSI-Layer 4)**

Ein Datenframe wird anhand seiner Absender-Port-Nummer, also einer bestimmten Applikation, einem VLAN zugeordnet. Jeder PC, der über diese Ports kommuniziert, gehört zu diesem VLAN.

► **802.1x-User-Zuordnung**

Der Benutzer muss sich am Netzwerk anmelden. Abhängig von seinem Benutzerprofil wird der Switch konfiguriert und der Switchport, an dem er soeben angeschlossen ist, wird für das jeweilige VLAN konfiguriert.

Als sicher kann nur angenommen werden, wenn Verfahren 1 und Verfahren 2 kombiniert werden und wenn die Leitungen, Switches, Patchfelder, Netzwerkdosen etc. verschlossen und nicht zugänglich sind.

Die sicherste Methode ist die VLAN-Zuordnung des Users über 802.1x Port-Based Network Access Control. Dieses Verfahren ist zwar das aufwendigste und benötigt viel Vorplanung, ist aber mit Abstand die beste Methode, um ein Netzwerk sicher zu machen. Der Benutzer muss sich dabei an einem Authentication Server anmelden, noch bevor eine IP-Adresse bezogen hat. Wird er authentifiziert und autorisiert, erfolgt die Zuordnung zu einem VLAN.

VLANs sind genormt in ISO 802.1Q und ISO 802.1P.

7.2 Routing

Routing-Grundlagen

Router sind Verbindungsknoten im Datennetz. An jedem Router entscheidet sich, welchen Weg ein Datenpaket weiter einschlägt analog zu einem Verkehrsknoten, an dem sich der Autofahrer entscheidet, welchen Weg er weiter einschlägt (Bild 7.7).

Router sind Netzwerkgeräte, die auf OSI-Layer 3, der Netzwerkschicht, arbeiten. Sie verbinden zwei oder mehrere Netze miteinander. Sie treffen anhand einer Routing-Tabelle ihre Entscheidung, an welchen Anschluss ein ankommendes Paket weitergeleitet wird. Die Netz-Adressen

7.2 Routing

sind Bestandteil der IP-Adressen und dienen damit als Routinginformation für den Transport der Pakete (Bild 7.8).

Die IP-Adressen von Sender und Empfänger bleiben über die gesamte Übertragungsstrecke unverändert! Die physikalischen Adressdaten werden von Teilstrecke zu Teilstrecke verändert!

Geroutet wird, wenn mit einem Host außerhalb des eigenen Netzes kommuniziert wird!

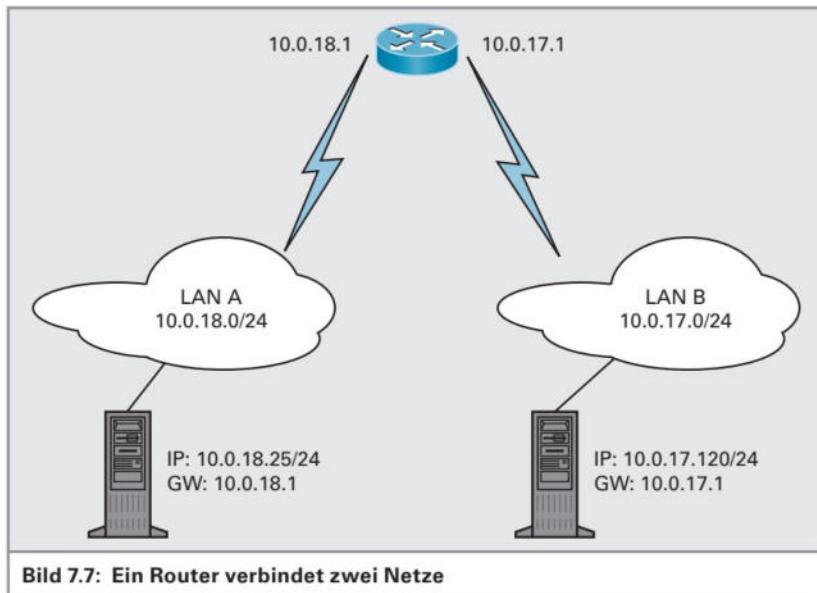


Bild 7.7: Ein Router verbindet zwei Netze

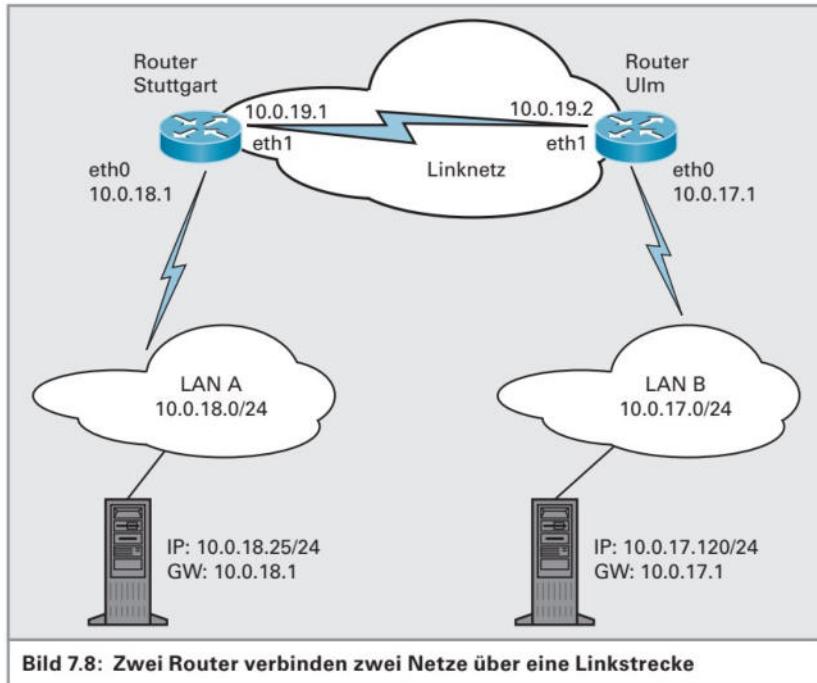


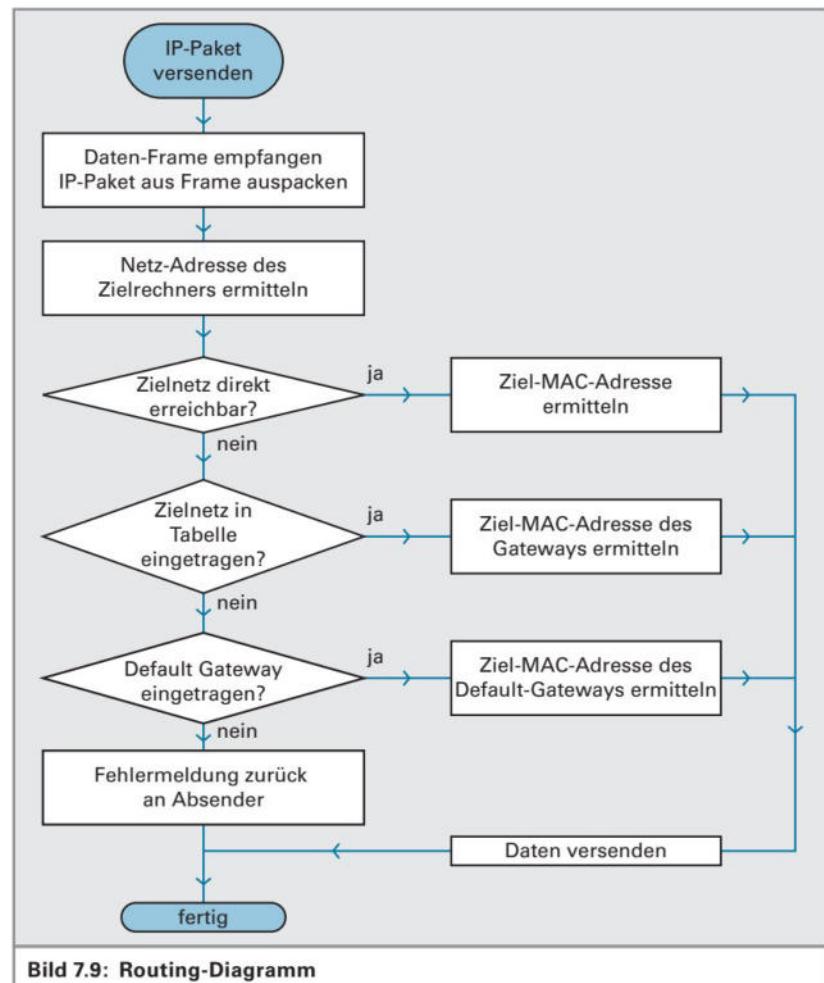
Bild 7.8: Zwei Router verbinden zwei Netze über eine Linkstrecke

7 Switching und Routing

7.2.1 Routing – Wie arbeitet ein Router?

Was geschieht im Router mit einem empfangenen Datenframe? An welchen Port leitet der Router einen empfangenen Datenframe weiter?

Bild 7.9 zeigt den Ablauf des Routing-Vorganges.



Der Router entpackt den empfangenen Datenframe bis auf OSI-Layer 3, der Netzwerkschicht.

Er liest die IP-Adresse des Zielrechners und trifft seine Entscheidung, wohin er das Paket weiterleiten soll. Ziel- und Quell-IP-Adresse bleiben dabei unverändert. Die Adressierung auf der darunter liegenden Schicht 2 wird verändert. Es wird von jedem Router der nächste Router adressiert. Der letzte Router adressiert den Zielknoten.

Eine Verbindung zwischen zwei Routern nennt man Route oder Link. Es werden statische und dynamische Routen unterschieden.

Statische Routen sind fest.

Dynamische Routen ändern sich, wenn sich die Netzstruktur ändert.

Statische Routen werden vom Administrator von Hand fest in die Routentabelle eingetragen.

Dynamische Routen werden vom Router selbst während des Betriebes in die Tabelle eingetragen und verwaltet.

Die Default-Route ist eine statische Route, die verwendet wird, wenn kein passendes Netz gefunden wird. Dies ist vergleichbar mit Default-Gateway bei jedem Rechner. Diese Route wird auch als „*Gateway of last resort*“ bezeichnet, also in etwa „der letzte Ausweg“.

Datensicherheit

Die Daten gelangen unverändert von einem Netz ins andere. Jeder, der Zugang zu den physikalischen Übertragungswegen hat, Leitungen oder Router, kann die Daten mitlesen. Dies stellt ein erhebliches Sicherheitsrisiko dar!

Abhilfe schafft hier das Verschlüsseln der Daten von Endgerät zu Endgerät, sodass auf dem Weg zwischen den beiden Rechnern die Daten zwar mitgelesen, aber nicht ausgewertet werden können.

7.2.2 Routing Protocols / Dynamisches Routing

Informationen, die den Router veranlassen, die Routingtabelle zu verändern, nennt man Routing-Protokolle. Router senden in regelmäßigen Abständen Angaben über ihren Zustand und über die angeschlossenen Netzwerke usw. an die benachbarten Router.

Beispiel 7.1: Routingprotokolle

- ▶ RIP – Router Information Protocol
- ▶ RIPv2 – RIP Version 2
- ▶ IGRP – Interior Gateway Routing Protocol
- ▶ EIGRP – Extended IGRP
- ▶ OSPF – Open Shortest Path First

7.2.3 Count-to-Infinity

Damit der Router Entscheidungen treffen kann, welche Route ein Datenpaket nehmen soll, werden die Routen mit „Metrics“ bewertet. Metrics sind Gewichtungsfaktoren wie z.B. die Distanz (RIP), Bandbreite oder die Auslastung einer Leitung.

Ältere Routingprotokolle benutzen einfache Metrics. Die einfachste Metric ist die Anzahl der Router, die bis zum Ziel übersprungen werden müssen. Man nennt dies Hops (Sprünge).

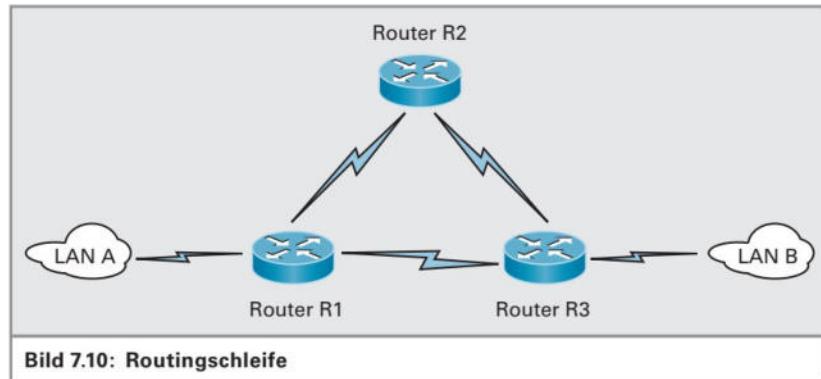
Wird nur die Anzahl der zu passierenden Router verarbeitet (Hops), so werden langsame Routen über wenige Router gegenüber längeren aber schnelleren Routen vorgezogen. Da hierbei nur die Anzahl der Router eine Rolle spielt, bezeichnet man diese Protokolle als Distance-Vector-Protokolle.

Beispiel 7.2: Distance-Vector-Protokolle

- ▶ RIP – Router Information Protocol
- ▶ RIPv2 – RIP Version 2
- ▶ IGRP – Interior Gateway Routing Protocol
- ▶ EIGRP – Extended IGRP

7 Switching und Routing

Im Beispiel aus Bild 7.10 werden zwei Netzwerke LAN A und LAN B über die Router R1, R2 und R3 mit schnellen Fast Ethernet-Leitungen verbunden. Als Ausfallsicherung wird eine langsame Wählverbindung über ISDN von Router R1 zu Router R3 eingerichtet. Die langsame Route über die ISDN-Wählleitung hat dabei eine Metrik von 2 Hops, die wesentlich schnellere Leitung hat hingegen eine Metrik von 3. Bei reinem Distance-Vector-Routing würde also immer die kürzeste, hier die langsame Leitung verwendet, was nicht erwünscht ist.



Aus diesem Grund sind reine Distance-Vector-Protokolle in größeren Netzen nicht mehr üblich. Sie kommen nur noch im LAN zum Einsatz. Komplexere Routingprotokolle berücksichtigen andere Metrics der Leitungen, wie beispielsweise die Kosten von Leitungen, deren Bandbreite und die momentane Auslastung. Man nennt diese Protokolle Link-State-Protokolle, weil die Routenauswahl von dem Zustand des Links abhängig ist.

Beispiel 7.3: Link-State-Protokolle

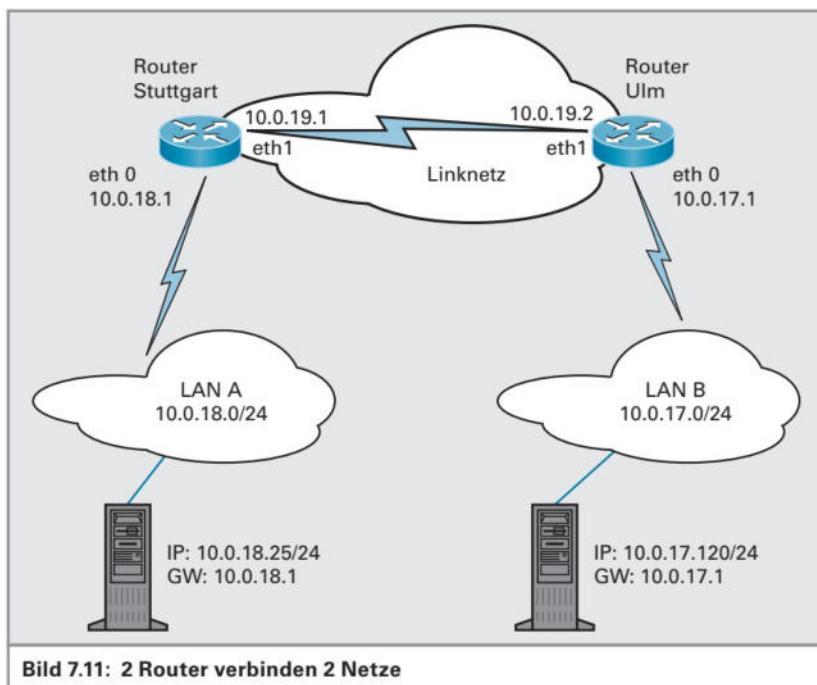
- ▶ OSPF – Open Shortest Path First
- ▶ IS-IS – Intermediate System to Intermediate System

7.2.4 Routing-Tabellen

In Bild 7.11 werden 2 Netzwerke, links 10.0.18.0 und rechts 10.0.17.0 über ein drittes Netz in der Mitte 10.0.19.0 miteinander verbunden.

Jeder PC hat als Standard-Gateway die IP-Adresse seines Routers, also des Routers in seinem Netz, eingestellt.

Der linke Router erreicht das rechte Netz über seinen Port mit der Adresse 10.0.19.1. Die Entfernung zwischen den beiden Netzen beträgt 2 Hops.

**Tabelle 7.4:** Routingtabelle zu Abbildung 7.11 – Router Stuttgart

Netz-ID	Subnetmask	Schnittstelle	Bemerkungen
10.0.18.0	255.255.255.0	eth0	das eigene Netz, direkt erreichbar ohne Router
10.0.19.0	255.255.255.0	eth1	der Weiterleitungsport des Routers
10.0.17.0	255.255.255.0	eth1	über 2 Router wird das 17er Netz erreicht

Tabelle 7.5: Routingtabelle zu Abbildung 7.11 – Router Ulm

Netz-ID	Subnetmask	Schnittstelle	Bemerkungen
10.0.17.0	255.255.255.0	eth0	das eigene Netz, direkt erreichbar ohne Router
10.0.18.0	255.255.255.0	eth1	über 2 Router wird das 18er Netz erreicht
10.0.19.0	255.255.255.0	eth1	der Weiterleitungsport des Routers verwendet

7.2.5 Routed Protocols

Routed Protocols sind die routingfähigen Protokolle. Damit sind diejenigen Protokolle gemeint, mit denen Nutzdaten über die Router weitergeleitet werden. Routingfähige Protokolle müssen neben den Rechnern auch die Netzwerke eindeutig identifizieren. Sie verfügen daher über Netz- und Rechneradresse. Beim IP-Protokoll werden IP-Adressen verwendet.

7 Switching und Routing

Beim älteren IPX/SPX aus dem Haus Novell werden IPX-Adressen eingesetzt. Protokolle ohne Netzwerkadressen, wie z.B. NetBEUI von Microsoft, können nicht geroutet werden und sind somit keine Routed Protocols.

In welchem Netz befindet sich der eigene Rechner?

Beim Versenden eines Datenpaketes von einem Rechner an einen anderen muss der Rechner entscheiden, an welchen Folge-Knoten das Paket adressiert werden muss. Dazu ist es wichtig, dass der Rechner seine eigene IP-Adresse und sein eigenes IP-Netz kennt. Die IP-Adresse wurde dem Rechner manuell oder automatisch (DHCP) zugewiesen, ebenso die Subnetzmaske (Subnetmask). Hieraus kann der Rechner seine eigene Netz-ID berechnen.

In welchem Netz befindet sich der Zielrechner?

Vor dem Verschicken eines Datenpaketes muss der Rechner nun prüfen, ob sich der Zielrechner im eigenen Netz befindet. Wenn dies der Fall ist, kann das Paket direkt zugestellt werden. Dazu wird das IP-Paket in einen Frame verpackt und an die MAC-Adresse des Zielknotens geschickt.

Befindet sich der Zielrechner in einem anderen Netz, muss das Paket über einen Router zugestellt werden. Das IP-Paket wird dazu in einen Frame verpackt, der an den Router adressiert wird.

7.2.6 Berechnen der Netz-Adresse

Die Analogie zum Telefonnetz

Wann telefoniert man mit Vorwahl, wann ohne?

Eine IP-Adresse besteht bekanntlich aus zwei Anteilen, der Netzadresse und der Rechnernummer. Telefonnummern sind ähnlich aufgebaut: Eine vollständige Telefonnummer besteht aus einer Vorwahl, der Orts-Netz-Nummer und der Rufnummer innerhalb des Ortsnetzes. Wird innerhalb des Ortsnetzes telefoniert, wird das Gespräch nicht über andere Netze geleitet. Es bleibt netzintern. Beim Telefon weiß man aus Erfahrung, wie viele Ziffern einer Telefonnummer das Ortsnetz adressieren. Die restlichen Ziffern adressieren den Telefonanschluss.

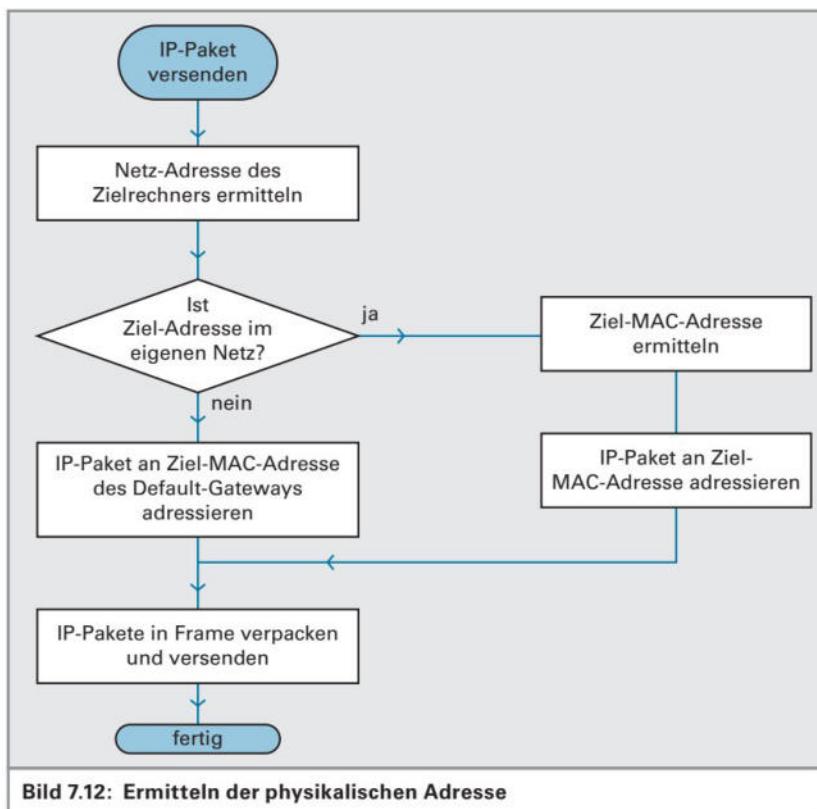
Die Vorwahl ist die Netz-Adresse.

Große Ortsnetze haben wenige Ziffern (z.B. Berlin 030 oder München 089), kleine Ortsnetze haben mehr Ziffern (z.B. Ulm 0731 oder Gomadingen 07387). Die Nummern der Telefonanschlüsse sind innerhalb eines Ortsnetzes eindeutig, d.h., jede Rufnummer gibt es nur einmal. Dieselben Rufnummern können aber in anderen Netzen auch benutzt werden. Die Telefonnummern sind trotzdem weltweit eindeutig, also nur einmal vorhanden, weil zur Anschlussnummer noch die Netznummer gehört.

Verlässt der Anruf Deutschland, wird zuerst das Netz des Ziellandes adressiert. Deutschland hat die internationale Telefon-Landesnummer 49, USA die 1 und Peru beispielsweise 511.

Dies ist also ein klassisches Netz, welches in Subnetze aufgeteilt wird, die wiederum in kleinere Subnetze aufgeteilt werden.

Bild 7.12 zeigt, in welchen Schritten die Zieladresse ermittelt wird.



IP-Netz- und IP-Rechneradressen

So wie die Telefonnummer in einen Netz- und einen Anschlusssteil aufgetrennt wird, so verhält es sich auch bei IP-Adressen. Im Gegensatz zu den Telefonnummern gibt es hier eine klare Angabe, wie viele Stellen der Adresse das Netzwerk und wie viele den Rechner adressieren. Hierzu sind 2 Verfahren gebräuchlich. Das bisherige Verfahren nutzt zusätzlich zur IP-Adresse die Subnetzmaske. Das neuere Verfahren gibt mit der IP-Adresse die Anzahl der Netz-Bits an (CIDR-Schreibweise).

Herkömmliches Verfahren – IP-Adresse mit Subnetzmaske:

Schreibweise IP: w.x.y.z und SN: s.t.u.v

Beides wird in dezimaler Schreibweise angegeben. Jede Stelle umfasst ein Oktett (≥ 8 Bit). Die Subnetzmaske wird von links nach rechts mit Einsen aufgefüllt. Die Stellen, an denen eine 1 steht, gehören zum Netzanteil, der Rest steht für die Rechneradresse.

Um nun die Netzadresse zu berechnen, gibt es mehrere Verfahren:

1. Man schreibt IP-Adresse und Subnetzmaske binär untereinander und bildet bitweise eine logische UND-Verknüpfung. Das Ergebnis ist der Netzanteil der IP-Adresse.
2. Man schreibt IP-Adresse und Subnetzmaske binär auf und zählt die Einsen der Subnetzmaske. Dieselbe Anzahl von Bits werden von links nach rechts von der IP-Adresse abgezählt. Diese Bits entsprechen dem Netzanteil. Die restlichen Bits der IP-Adresse ergeben den Hostanteil.

7 Switching und Routing

Beispiel 7.4:

	Binär	Dezimal
IP	0000'1010.0000'0001.0000'0001.0000'0111	10.1.1.7
SN	1111'1111.1111'1111.0000'0000.0000'0000	255.255.0.0
UND	0000'1010.0000'0001.0000'0000.0000'0000	10.1.0.0

Man erkennt, dass die ersten 16 SN-Bits 1 sind. Somit gehören die ersten 16 Bit der IP-Adresse zum Netzanteil, der Rest zum Hostanteil.

Es ergeben sich also die Netzadresse 10.1.0.0 und die Hostadresse 0.0.1.7.

CIDR-Schreibweise

Die CIDR-Schreibweise ist eine IP-Adresse mit Angabe der Netzbit-Anzahl: w.x.y.z/n; dabei gibt die Zahl n hinter dem Schrägstrich die Anzahl der Netzbits an.

Beispiel 7.5:

10.1.17.1/20 bedeutet, dass die ersten 20 Bits der IP-Adresse die NetzwerkkAdresse ergeben. Bitweise betrachtet ergibt sich:

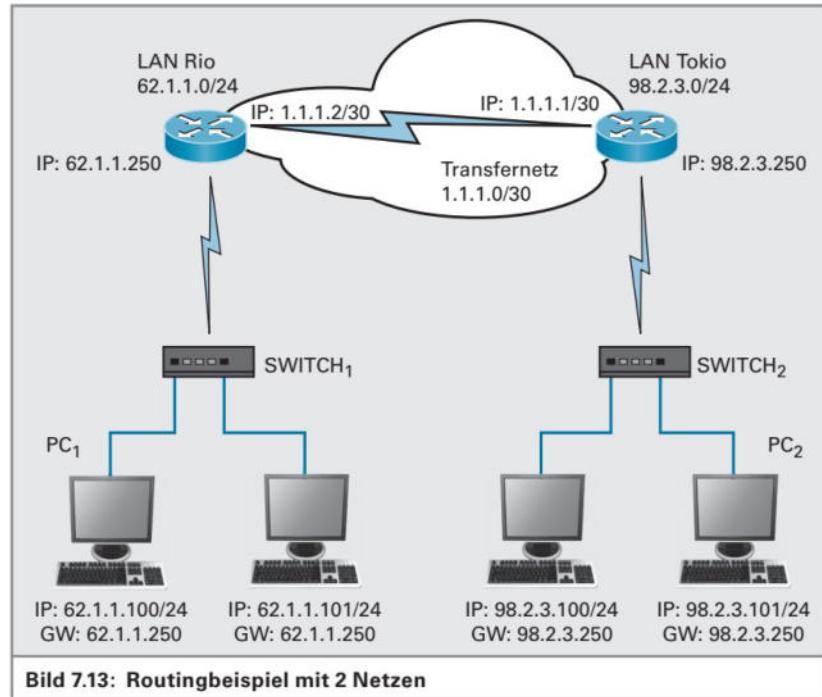
IP = 0000'1010.0000'0001.0001'0001.0000'0001.

Betrachtet man als erstes nur die ersten 20 Bits, so erhält man als Netz-Adresse:

Net-ID = 0000'1010.0000'0001.0001'0000.0000'0000 = 10.1.16.0

Betrachtet man die bisher unbeachteten Bits 21 bis 32, so erhält man die Host-Adresse:

Host-ID: 0000'0000.0000'0000.0000'0001.0000'0001 = 0.0.1.1



Beispiel 7.6: Routing (Bild 7.13)

Darstellung des Datentransportes über zwei Router: PC₁ mit der IP 62.1.1.100 schickt ein Datenpaket (OSI-Layer 3) an den Rechner PC₂ mit der IP 98.2.3.101. Das IP-Paket wird vom ersten PC mit seiner Absender-IP-Adresse und mit der Ziel-IP-Adresse des 2. Rechners versehen.

Der sendende PC reicht nun das Paket zum weiteren Versenden an die Schicht 2 weiter. Hier werden Frames erstellt und Netzwerkkarten adressiert. Bevor der Rechner nun die physikalische MAC-Adresse des Empfängers einsetzen kann, muss er prüfen, ob sich der Zielrechner im selben Netz befindet wie er. Dadurch muss er wissen, in welchem Netz er sich selbst befindet. Dies weiß der PC durch seine Netzwerkeinstellungen.

Aus der IP-Adresse 62.1.1.100 und 24 Bits Netzanteil (aus der Angabe „/24“) errechnet der PC das Netz mit der Nummer 62.1.1.0.

PC₂ liegt somit nicht im eigenen Netz. Das Paket muss also über den Router zugestellt werden. Dazu wird das Paket an den Router Rio mit der IP 62.1.1.250 adressiert. Der PC muss jetzt die MAC-Adresse des Interfaces mit dieser IP-Adresse ermitteln. Dies geschieht mithilfe des ARP. Wenn der PC die MAC-Adresse des Routerinterfaces hat, kann er das Originalpaket, weiterhin mit der Ziel-IP-Adresse von PC₂, an den Router schicken. Der Frame, in den das IP-Paket eingepackt wird, wird an den Router adressiert.

PC₁ verschickt den Datenframe, den als nächstes beim Switch₁ ankommt. Switch₁ liest die Ziel-MAC-Adresse aus dem Frame aus und vergleicht diese Adresse mit den Adressen aus seiner Switching-Tabelle. Er kennt die MAC-Adresse des Routers und leitet den Frame sofort unverändert an diesen Anschluss weiter, an dem der Router Rio angeschlossen ist.

Der Router Rio empfängt nun den Frame und packt ihn aus. Aus dem enthaltenen IP-Paket liest er die Zieladresse aus, also die IP-Adresse von PC₂. Der Router Rio kennt den Weg ins Zielnetz, in dem sich PC₂ befindet. Er weiß aus seiner Routing-Tabelle, dass er das Paket an den Router Tokio schicken muss. Er verpackt das IP-Paket wieder in einen Frame und adressiert diesen Frame an die MAC-Adresse des Routers Tokio.

Router Tokio packt den Frame aus und erhält das IP-Paket. Er liest die Ziel-IP-Adresse aus und sieht, dass sich der Zielrechner in einem Netz befindet, welches bei ihm angeschlossen ist. Er kann also den Zielrechner direkt erreichen. Er verpackt dann das IP-Paket in einen Frame, welches direkt an den PC₂ adressiert wird.

Der Switch₂ leitet den Frame sofort unverändert zum Ziel-PC.

Der Ziel-PC empfängt den Frame. Er vergleicht die empfangene Ziel-MAC-Adresse mit seiner eigenen MAC-Adresse. Da die Adressen übereinstimmen, liest er alle Daten von der Netzwerkleitung in seinen Pufferspeicher ein und übergibt den empfangenen Frame dem Betriebssystem.

Die Tabelle 7.6 zeigt, wie sich die Adressen während der Übermittlung der Daten verändern. Man sieht, dass die IP-Adressen im Datenpaket (Layer 3) unverändert bleiben. Man sieht, dass die Adressen der unteren Schicht (Layer 2) immer verändert werden.

Tabelle 7.6: Adressen während des Transportes

Strecke	Quell-IP	Ziel-IP	Quell-MAC	Ziel-MAC
PC ₁ – Switch ₁	PC ₁	PC ₂	PC ₁	R-Rio
Switch ₁ – R-Rio	PC ₁	PC ₂	PC ₁	R-Rio
R-Rio – R-Tokio	PC ₁	PC ₂	R-Rio	R-Tokio
R-Tokio – Switch ₂	PC ₁	PC ₂	R-Tokio	PC ₂
Switch ₂ – PC ₂	PC ₁	PC ₂	R-Tokio	PC ₂

7 Switching und Routing

7.2.7 Default Gateway

Der **Gateway** führt nach außen.

Ein **Gateway** (oder auf deutsch: Torweg) war im Mittelalter ein Weg, der aus einer Stadt oder einer Burg hinaus führte. Diese Wege aus dem geschützten Bereich der Mauern waren durch ein Tor geschützt und wurden streng bewacht (Bild 7.14).



Bild 7.14: Gateway

In einem Netzwerk braucht man ebenso einen „Ausweg“ aus dem eigenen Netz. Ein jeder PC in einem Netzwerk kann Daten an alle Rechner seines Netzes schicken. Hat er Daten an Rechner zu verschicken, die sich nicht in seinem Netz befinden, so schickt er diese Daten an den Gateway.

Router haben ihre Routingtabellen. Ihnen sind die Netze bekannt, die sie direkt erreichen und die direkt an ihnen angeschlossen sind. Netze hinter anderen Routern kennen die Router auch, da sie sich gegenseitig mitteilen, welche Netze sie erreichen können.

Da natürlich auch Router nicht alle Netze kennen können, haben sie für die ihnen unbekannten Netze einen Default Gateway.

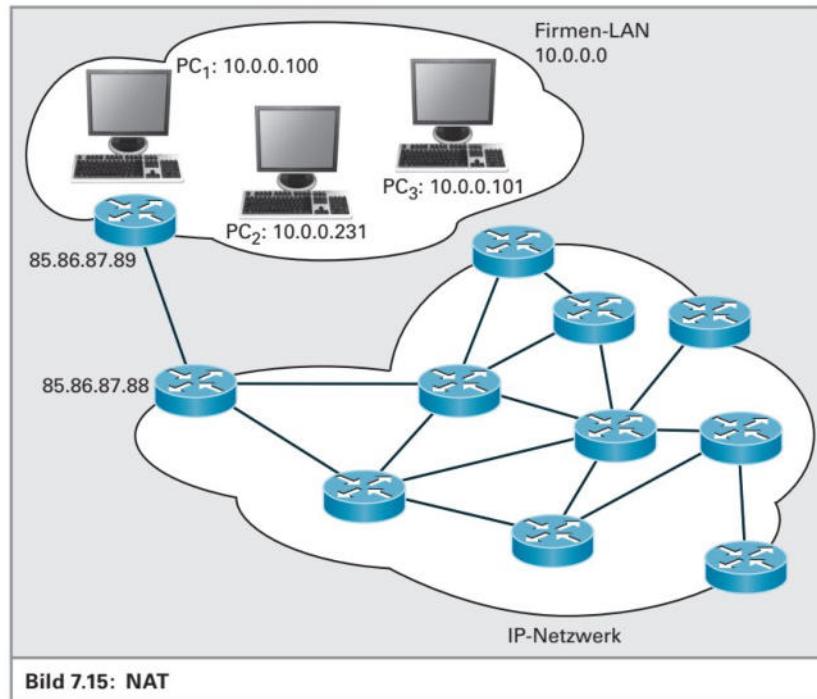
7.2.8 NAT/PAT – Network Address Translation / Port Address Translation

Würde man eine Anzahl von Rechnern in einem LAN über einen normalen Router ans Internet anschließen, so bräuchte jeder einzelne Rechner eine eigene, einmalige IP-Adresse aus dem öffentlichen Adressraum. Alle Rechner müssten dann ein Class-A, Class-B oder Class-C Netz bilden, oder zumindest ein Subnetz eines solchen öffentlichen Netzes. Dadurch könnte zwar jeder Rechner mit dem gesamten Internet kommunizieren, wäre aber auch vom gesamten Internet erreichbar und angreifbar.

Dies verursacht zwei verschiedene Probleme:

- ▶ Die öffentlichen IP-Adressen sind sehr knapp – der letzte freie Adressblock wurde im Dezember 2010 vergeben.
- ▶ Jeder Rechner wäre direkt mit dem Internet verbunden und dadurch sehr leicht angreifbar.

Abhilfe schafft hier das Einrichten eines abgeschotteten eigenen Netzes als LAN, unter Verwendung von Adressen aus einem privaten IP-Adressbereich, der nicht im Internet geroutet wird. Dieses Verfahren nennt man NAT (Bild 7.15).



Dabei werden private IP-Adressen der Klasse C für Heimnetze und kleinere Firmen verwendet, Klasse-B-Adressen für große Firmennetze und Klasse-A-Adressen für Konzerne und große Netzstrukturen.

Bei **NAT** wird nun ein ganzes Netz, mit einer Vielzahl von Rechnern mit lokalen Adressen, mit einer einzigen (oder jedenfalls sehr wenigen) öffentlichen IP-Adresse(n) verbunden. Die internen IP-Adressen werden auf die öffentliche Adresse übersetzt.

NAT verschleiert die internen Netzstrukturen.

NAT spart öffentliche IP-Adressen,

Jede Verbindung, egal von welchem internen Rechner, wird auf eine einzige externe, öffentliche IP-Adresse abgebildet. Dazu werden nicht nur die internen IP-Adressen auf eine externe IP-Adresse abgebildet, sondern auch die Ports (Sockets, IP-Adresse und TCP/UDP-Ports). Dieses PAT, Port Address Translation, wird üblicherweise nicht gesondert erwähnt, findet aber dennoch statt.

Im Gegensatz zum normalen Routing, wird bei NAT/PAT die Netzwerkadresse im Router verändert.

Jede Anfrage von einem Rechner im LAN wird nun im NAT-Router verändert. Der Router ersetzt die bisherige Quell-IP durch seine IP-Adresse.

7 Switching und Routing

Mit unterschiedlichen Portnummern werden die Anfragen der Rechner aus dem LAN unterschieden.

Da der Router dies aber mit jeder Anfrage von jedem internen Rechner machen muss, muss er als Unterscheidungskriterium für jede Anfrage eine andere Port-Nummer verwenden.

Die Antworten aus dem Internet sind an den Router adressiert. Anhand der Port-Nummer kann der Router die ankommenden Pakete wieder umadressieren und an die jeweiligen Rechner im Netz zustellen. Die Zuordnung von Rechner-IP und Port-Nummer zu der öffentlichen IP und der korrespondierenden Port-Nummer wird in einer Übersetzungstabelle, der NAT-Translation Table, gespeichert.

Ein Problem ergibt sich, wenn von außen auf einen Rechner in einem Netzwerk hinter einem NAT-Router zugegriffen werden soll.

Dies ist z.B. dann notwendig, wenn Kunden von außen auf einen Server (z.B. eines Onlineshops) in einem LAN zugreifen wollen. Dies ist auch der Fall, wenn man von seinem mobilen Rechner auf seinen Heim-PC zugreifen möchte.

Mit Einträgen in die NAT-Translation Table werden Ports geöffnet.

Ein solcher Zugriff ist im Normalfall nicht möglich, da der NAT-Router die internen Rechner und deren IP-Adressen von der Außenwelt abschottet. Hier hilft ein manueller Eintrag in die NAT-Translation Table.

Ein von außen am Router ankommendes Paket wird dieser ins LAN weiterleiten, wenn zu dem empfangenden Ziel-Port ein Eintrag in der Übersetzungstabelle vorhanden ist.

Das nächste Problem ergibt sich, wenn beispielsweise ein IP-Telefon oder ein Skype-Rechner von außen erreichbar sein muss. Man kann nicht für jedes Telefon einen Eintrag erstellen, wenn das Telefon eingeschaltet wird und wieder austragen, wenn das Telefon oder der Rechner ausgeschaltet werden.

Bei upnp können Anwendungen selbst die Ports auf dem Gateway öffnen.

Universal Plug & Play (upnp) ist eine Funktion, die es den Geräten (oder eigentlich der darin laufenden Software) erlaubt, selbst Einträge in die NAT-Tabelle einzufügen. Ist dieses Feature auf dem Router aktiviert, so wird beispielsweise ein Rechner, auf dem Skype läuft, selbstständig den entsprechenden Eintrag vornehmen und somit aus dem Internet erreichbar sein.

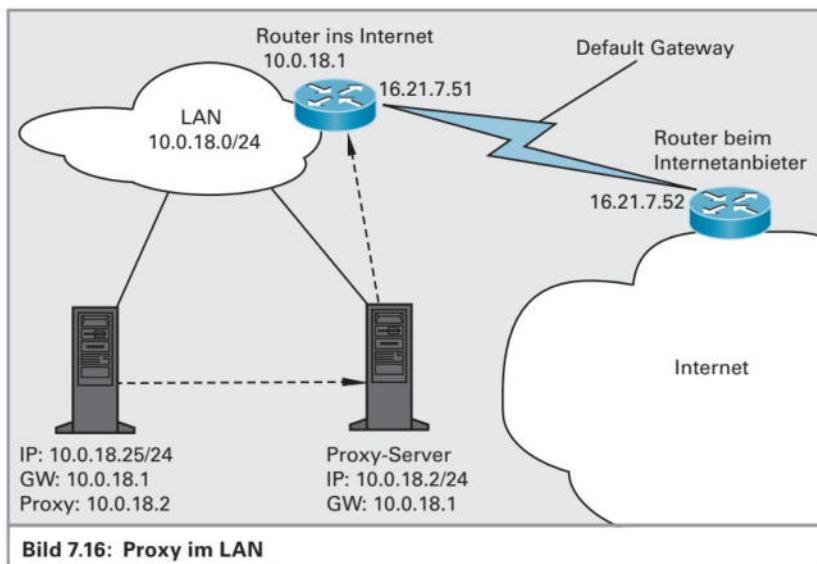
7.2.9 Proxy-Routing

Proxy: Stellvertreter

Proxy ist englisch und bedeutet „Stellvertreter“. Ein Proxy-Rechner oder Proxy-Server geht stellvertretend für alle Rechner eines LANs ins Internet. Er macht dabei NAT/PAT, genauso wie ein NAT-Router.

Der Proxy geht stellvertretend für alle lokalen Rechner ins Internet.

Der Unterschied liegt darin, dass die PCs im Netz ihre Anfragen nicht an den Gateway-Rechner adressieren, sondern an den Proxy. Bei den PCs wird in der Netzwerkeinstellung die Adresse des Proxys eingetragen. Anfragen nach außen werden dann an den Proxy adressiert, der die Anfragen dann an den Internet-Router oder das Gateway weiterschickt (Bild 7.16).



Dieser Umweg ermöglicht nun einiges, was ohne Proxy nicht möglich ist:

- ▶ Filtern von Datenverkehr
- ▶ Zwischenspeichern von Ergebnissen
- ▶ Verschleiern von Adressen

Das **Filtern** von Netzwerzkzugriffen hat ganz praktischen Nutzen. So kann in lokalen Netzen gezielt der Besuch von einzelnen Seiten im Internet geblockt werden. In vielen Firmen werden beispielsweise Seiten für Börsenkurse und Online-Börsenhandel gesperrt, da viel Arbeitszeit durch Online-Brokerage verloren ging. In Schulen werden oft Soziale Netzwerke wie Schüler-VZ, Studi-VZ, Facebook und ähnliche gesperrt, da sonst kein konzentriertes Arbeiten an Computern möglich ist.

Der Proxy filtert Datenverkehr.

Eine weitere, sehr wichtige Funktion eines Proxyservers ist das **Zwischenspeichern** der Seiten. Sehr häufig wird eine Seite, die einmal besucht wird, später erneut besucht. Der Proxy legt nun Seiteninhalte, die er vom Internet empfangen hat, auf seiner Festplatte ab. Wird nun dieselbe Seite von einem Benutzer aus dem LAN wieder angefragt, so kann der Proxy diese sofort direkt ausliefern, ohne sie über das Internet erneut zu holen.

Der Proxy speichert Seiteninhalte.

Dies verringert die Menge an Daten, die über das Internet übertragen werden müssen und dies verkürzt die Wartezeit, bis eine Seite angezeigt wird. Häufig wird mit dem Begriff Proxy diese Funktion des Zwischenspeicherns gleichgesetzt, was eigentlich nicht ganz korrekt ist.

Hier stellt sich die Frage, wie lange die Seiten im Proxy-Speicher erhalten bleiben. Da sich die Inhalte der Seiten gelegentlich ändern, ergibt es keinen Sinn, die Seiten sehr lange zu speichern. Aus diesem Grund bringen die meisten Seiten ihre „Haltbarkeit“ mit, eine Art Verfallsdatum. Statische Seiten können länger gespeichert werden, Seiten, die Änderungen unterliegen, werden früher gelöscht. Dieser Proxy-Speicher wird auch *Proxy-Cache* genannt. Ein Cache ist ein Versteck, ein verborgenes Lager, eine verdeckte Vorratskammer.

7 Switching und Routing

Das Verschleiern von Absenderdaten ist eine Funktion, die, ebenso wie NAT, Anonymität im Internet bietet.

Der Proxy spart IP-Adressen durch NAT.

Der Proxy ersetzt die IP-Adressen der PCs durch seine eigene IP-Adresse. Es ist von außen somit nur ersichtlich, dass Rechner eines bestimmten Netzes sich im Internet unterhalten. Welche Rechner des LANs dies wirklich sind, ist von außerhalb des LANs nicht ersichtlich.

7.2.10 Virtual Private Network, VPN, IP-Tunnel

Es sei folgende Situation gegeben: Ein Rechnerarbeitsplatz eines Firmennetzwerkes soll ausgelagert werden, beispielsweise als Heimarbeitsplatz. Man kann natürlich den PC mit einer langen Leitung versehen und den Arbeitsplatz an einen anderen Ort verlegen. Dies scheitert natürlich an den Kosten für das Verlegen der Leitungen.

Eine andere Lösung wäre, den ausgelagerten Rechner über eine angemietete Leitung von einem Netzwerkanbieter wie der Deutschen Telekom anzuschließen. Dies scheitert meistens an den Kosten und der Bandbreite der Mietleitung.

Das Netzwerk, welches fast überall zur Verfügung steht, ist das Internet. Es ist also naheliegend, dass das Internet für das Anbinden eines entfernten Rechners benutzt wird.

Der Rechner soll allerdings ins Firmennetzwerk eingebunden sein, so, als wäre er direkt am Firmenstandort. Er braucht dazu eine IP-Adresse aus dem LAN und der Benutzer braucht ein Anmeldekonto im Firmennetzwerk. Folgende Schwierigkeiten fallen dabei auf:

- ▶ Datenpakete mit privaten LAN-Adressen werden nicht im Internet geroutet.
- ▶ Datenpakete, die eigentlich nur firmenintern sichtbar sein sollten, sind im unsicheren Internet unterwegs. Dies ist ein großes Sicherheitsproblem.

Mit einem VPN wird ein unsicheres Netzwerk durchtunnelt – Daten werden im sicheren Tunnel transportiert.

Die Lösung heißt **VPN** – Virtual Private Network oder IP-Tunnel. Man baut sich ein großes virtuelles Netzwerk auf und nutzt dabei ein unsicheres Netzwerk als Basis. Oder anders ausgedrückt, die internen Firmendaten werden durch ein unsicheres Netzwerk getunnelt (Bild 7.17).

Der ausgelagerte Rechner erstellt ganz normale IP-Datenpakete, so als ob er sich im LAN befinden würde. Normalerweise würden nun die Datenpakete von Layer 3 auf Layer 2 weitergegeben, um dort in einen Frame eingepackt zu werden. Hier nun gibt es die entscheidende Veränderung gegenüber einem normalen Datenverkehr:

Das erzeugte Layer-3-Datenpaket wird in ein weiteres Layer-3-Paket eingepackt. Da der Rechner ans Internet angeschlossen ist, kann er nur Datenpakete mit seiner öffentlichen IP-Adresse verschicken, die er von seinem Internetprovider erhalten hat. Er packt also Pakete, die seine

öffentliche Quell-IP-Adresse als Absender enthalten und die einen speziellen Rechner/Router in seinem Firmen-LAN adressieren.

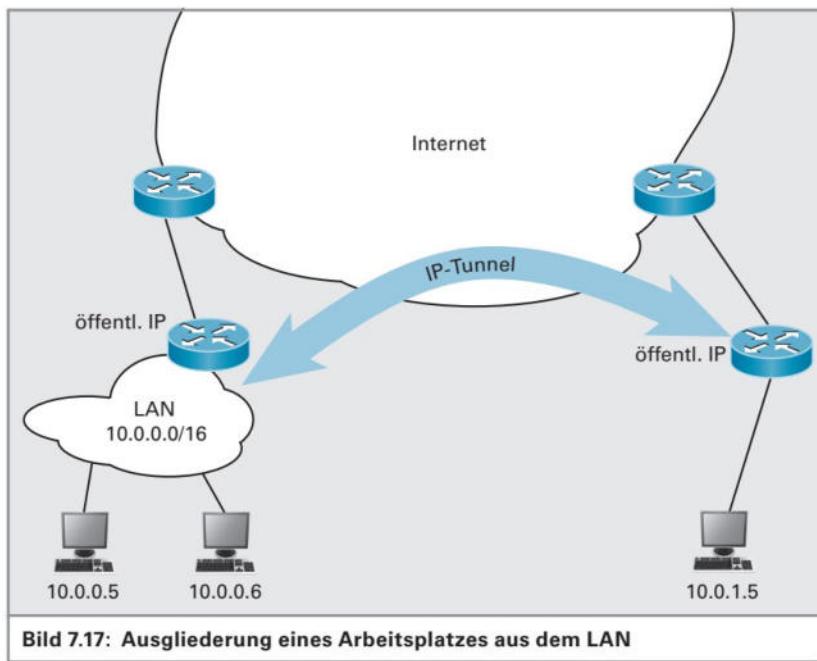


Bild 7.17: Ausgliederung eines Arbeitsplatzes aus dem LAN

Diese Datenpakete werden ganz normal im Internet transportiert. Als Inhalt eines solchen öffentlichen Paketes wird das LAN-interne IP-Paket transportiert. Der Rechner/Router im LAN, der diese Pakete empfängt, packt sie aus und erhält ein IP-Paket, welches er ganz normal ins Firmennetz weiterleiten kann.

Wenn man auf diese Weise einen einzigen Rechner an ein Firmennetzwerk anschließen kann, dann kann man ebenso auch ganze Netzwerke an andere Netzwerke anschließen. Ebenso kann man einzelne PCs mit einander verbinden.

Es sind drei Arten von VPNs möglich:

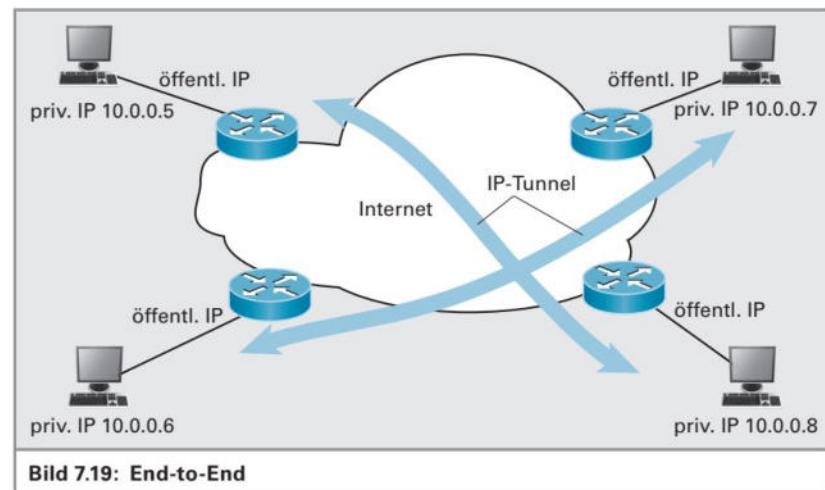
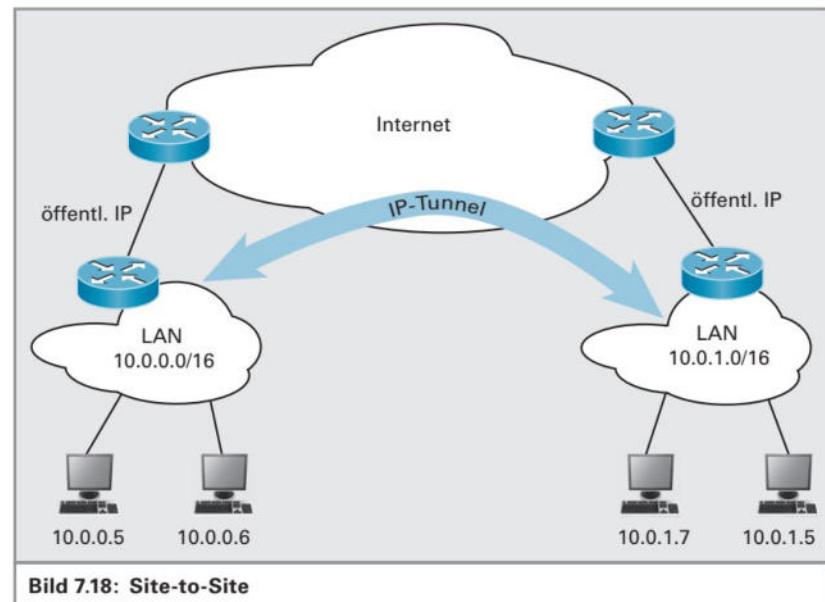
- ▶ End-to-Site-VPN
- ▶ Site-to-Site-VPN
- ▶ End-to-End-VPN

End-to-Site-VPNs werden eingesetzt, wenn von einzelnen externen Arbeitsplätzen auf das Firmennetzwerk zugegriffen werden soll. Dies ist bei Heimarbeitsplätzen der Fall oder auch bei mobilen Benutzern wie beispielsweise im Vertriebsaußendienst.

Site-to-Site-VPNs kommen zum Einsatz, wenn Außenstellen an die Firmenzentrale angebunden werden müssen (Bild 7.18).

7 Switching und Routing

End-to-End-VPNs dienen zur Kommunikation von einzelnen Rechnern. Typische Einsatzfälle sind Homebanking, Tauschbörsen und Online-Spiele (Bild 7.19).



7.3 IP-Konfiguration überprüfen

7.3 IP-Konfiguration überprüfen

Zum Überprüfen der Netzwerkkonfiguration stehen verschiedene Werkzeuge zur Verfügung. Die wichtigsten Einstellungen, die als erstes überprüft werden müssen, sind:

- ▶ IP-Adresse und Subnetzmaske des Rechners
- ▶ IP-Adresse des Standard-Gateways
- ▶ IP-Adresse des DNS-Servers

Wie bringt man in Erfahrung, welche IP-Konfiguration ein Rechner hat?

Die Tools sind bei Windows und Linux unterschiedlich.

7.3.1 IP-Konfiguration bei WINDOWS-Rechnern überprüfen

c:\> ipconfig liefert eine kurze Übersicht der wichtigsten IP-Einstellungen inclusive Standard-Gateway und DNS-Server.

c:\> ipconfig /all liefert ausführliche Angaben über die IP-Einstellungen.

Bei Windows-Rechnern liefert ipconfig die wichtigsten Informationen.

c:\> ipconfig /release gibt die IP-Adresse und alle Einstellungen frei, der Rechner hat anschließend keine IP-Verbindung mehr.

c:\> ipconfig /renew Eine neue IP-Konfiguration wird bei einem DHCP-Server angefordert.

7.3.2 IP-Konfiguration bei Linux-/Unix-Rechnern überprüfen

Das Überprüfen der Einstellungen ist bei Linux-Rechnern etwas aufwändiger. Es werden mehrere Schritte benötigt.

Rechner:~\$ ifconfig liefert die IP-Adresse und die Subnetzmaske des Rechners.

Rechner:~\$ route liefert die Routing-Tabelle des Rechners. Der Eintrag „default“ oder „0.0.0.0“ in der Spalte „Ziel“ ist der Name bzw. die Adresse des Default-Gateways.

Bei Linux benutzt man ifconfig.

Die Adresse des DNS-Servers ist bei Unix- und Linux-Rechnern in der Datei /etc/resolv.conf abgelegt. Man lässt sich zum Überprüfen der Konfiguration diese Datei auflisten.

Rechner:~\$ cat /etc/resolv.conf

Um eine neue IP-Konfiguration zu laden, vergleichbar dem

c:\> ipconfig /renew
bei Windows-Rechnern, verwendet man den Befehl

Rechner:~\$ dhclient -r

7.3.3 Verbindungen testen

Zum Testen von Verbindungen gibt es zwei Programme, die auf den meisten Rechnern verfügbar sind – das „ping“-Programm und das „traceroute“-Programm.

Der ping-Befehl ist das erste und wichtigste Werkzeug bei der Fehlersuche.

Beim *ping* wird ein Datenpaket an die angegebene Adresse geschickt. Der adressierte Rechner schickt ein Antwort-Paket zurück. So wird zum

7 Switching und Routing

Einen geprüft, ob überhaupt eine Verbindung besteht. Zum Anderen wird dabei die Antwortzeit (RTT, Round Trip Time) gemessen. Die Syntax ist bei Windows- und Linux-Rechnern dieselbe:

> ping <IP-Adresse> oder > ping <Rechnername>

Traceroute bzw. tracepath liefert die Liste der Router vom PC zum angefragten Ziel.

Traceroute schickt, ähnlich dem ping-Befehl, ein Datenpaket an den angegebenen Zielrechner. Allerdings wird beim ersten Mal die TTL (Time To Live) auf 1 gesetzt, sodass der erste Router das Paket verwirft und eine ICMP-Fehlermeldung zurückschickt. Der Rechner erhöht nun den TTL-Wert um 1 und schickt wieder ein Paket an den Zielrechner. Das Paket wird nun über zwei Router weitergeleitet. Der 2. Router verwirft das Paket und schickt eine Fehlermeldung zurück. Mit jedem weiteren Versuch erhöht der Rechner den TTL-Wert, sodass jedes Paket um jeweils einen Router weitergeleitet wird. So erhält man eine Liste der Router zwischen einem Rechner und einem Zielrechner. Je nach Betriebssystem heißt dieses Programm auch *tracert* oder *tracepath*. Beispiel eines Traceroute von einem Kabel-BW-Anschluss zum Webserver der Uni Ulm:

```
Rechner:~$ tracepath -n uni-ulm.de
1: 192.168.178.31      0.120ms pmtu 1500
1: 192.168.178.1      0.875ms
1: 192.168.178.1      0.891ms
2: 192.0.0.2            1.144ms pmtu 1460
2: 172.30.9.235         11.271ms
3: 172.30.9.234         14.571ms asymm 2
4: 78.42.40.5            12.686ms asymm 2
5: 193.138.31.16          36.045ms asymm 3
6: 129.143.57.70          27.649ms asymm 4
7: 129.143.87.114          33.441ms asymm 5
8: 134.60.112.242          34.690ms asymm 6
9: 134.60.1.25            21.338ms reached

Resume: pmtu 1460 hops 9 back 249
```

Die Path-MTU gibt die maximale Größe der Datenpakete an.

Die erste Spalte gibt den Wert des TTL-Feldes an. Die zweite Spalte zeigt die IP-Adresse (mit Parameter *-n*) oder den Namen des Knotens an, der den TTL-Wert auf null gezählt und damit eine Fehlermeldung ausgelöst hat. In der dritten Spalte steht die Antwortzeit des Knotens. Die vierte Spalte zeigt die maximale Paketgröße PMTU (Path Maximum Transmission Unit) der jeweiligen Verbindung an. Es ist zu erkennen, dass mit der maximal möglichen Größe von 1500 Bytes (dies ist die maximale Datengröße eines Ethernet-Frames) begonnen wird.

7.4 Übungsaufgaben Routing/Switching

7.3.4 DNS überprüfen

Zum Überprüfen der DNS-Einstellungen und -Funktion existieren mehrere Befehle. Der Befehl „nslookup“ schickt eine Anfrage an den nächsten DNS-Server. Im folgenden Beispiel wird der Rechner 192.168.178.1 (hier der lokale Router ins Internet) angefragt. Dieser liefert die IP-Adresse der Domäne uni-ulm.de.

```
Rechner:~$ nslookup uni-ulm.de
Server: 192.168.178.1
Address: 192.168.178.1#53
```

Werden Internetnamen richtig aufgelöst?

Welcher Rechner liefert die IP-Adressen?

nslookup und dig sind hier die richtigen Werkzeuge.

Non-authoritative answer:

```
Name: uni-ulm.de
Address: 134.60.1.25
```

Der Befehl „dig“ (domain information groper) ist ein sehr flexibles Werkzeug zur Fehlersuche bei DNS.

```
Rechner:~$ dig uni-ulm.de
; <>> DiG 9.8.1-P1 <>> uni-ulm.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5512
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;;
;; QUESTION SECTION:
;uni-ulm.de.      IN      A
;;
;; ANSWER SECTION:
uni-ulm.de.    159799   IN      A       134.60.1.25
;;
;; Query time: 1 msec
;; SERVER: 192.168.178.1#53(192.168.178.1)
```

7 Switching und Routing

7.4 Übungsaufgaben Routing/Switching

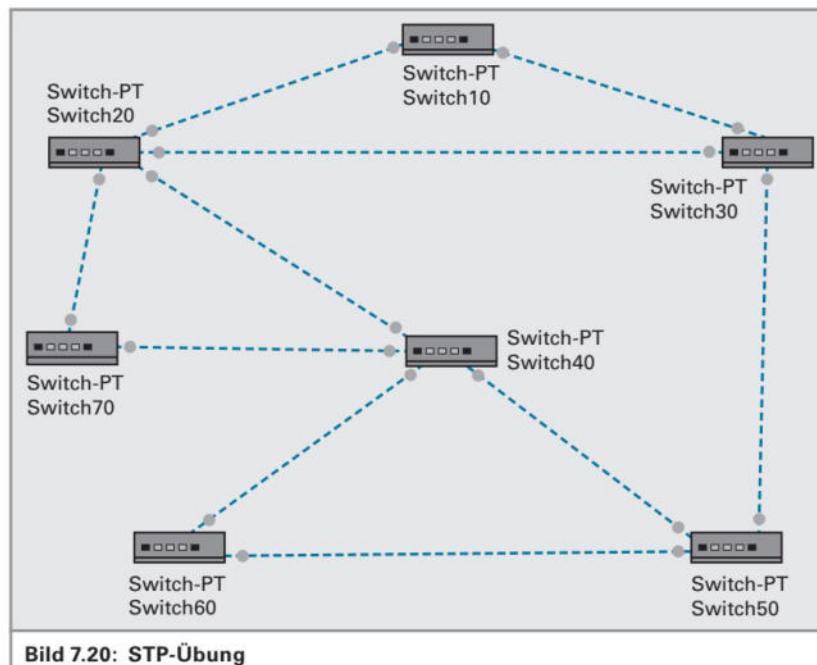
Übungsaufgabe Nr. 1

- a) Welcher Switchtyp hat die kürzeste Latenzzzeit?
- b) Welcher Switchtyp überprüft die Frames auf Richtigkeit, bevor sie weitergeschickt werden?
- c) Wie verhält sich ein Switch direkt nach dem Einschalten?

Spanning Tree Protokoll

Übungsaufgabe Nr. 2

Betrachten Sie Bild 20:



- a) Bestimmen Sie die Rootbridge und legen Sie die Links fest, die aktiviert/deaktiviert werden (alle Verbindungen sind 100 MBit/s).
- b) Angenommen, zwischen Switch40 und Switch60 existieren zwei Verbindungen, Sw40.2 auf Sw60.3 und Sw40.3 auf Sw60.1. Wie würde sich das Netzwerk verhalten?
- c) Zwischen Switch30 und Switch50 befindet sich eine Leitung mit 10 MBit/s, zwischen Switch20 und Switch70 sowie Switch70 und Switch40 befindet sich eine 1Gbit/s-Verbindung. Wie ändert sich die Topologie?
- d) Ändern Sie die Prioritäten der Switches so, dass Switch40 Wurzelbrücke wird. Zeichnen Sie farbig die geänderte Topologie ein.

7.4 Übungsaufgaben Routing/Switching

Übungen Routing

Übungsaufgabe Nr. 3

Der PC mit der Adresse 10.1.1.100 und der Subnetzmaske 255.255.0.0 schickt Daten an den Rechner 10.1.2.100.

Werden die Frames direkt zugestellt oder über einen Router? Ermitteln Sie dazu die jeweilige Netzadresse.

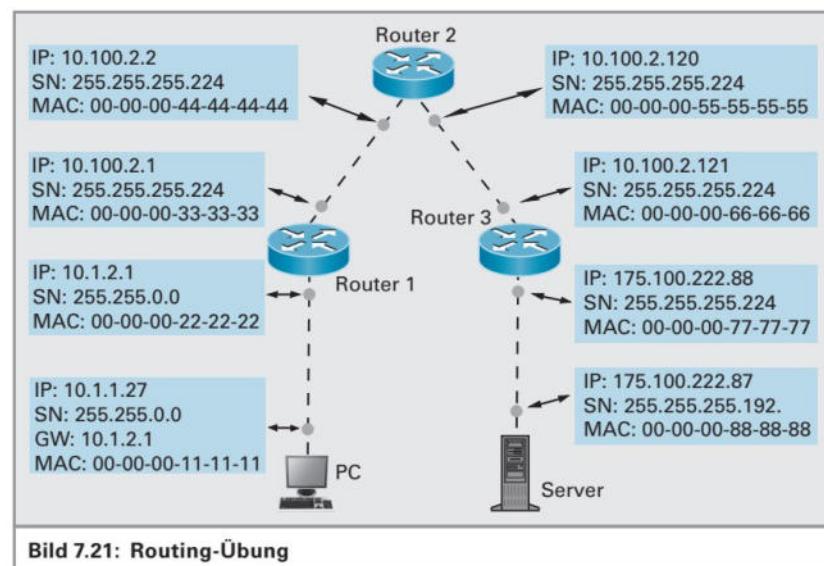
Übungsaufgabe Nr. 4

Der PC₁ mit der Adresse 10.1.1.100 und der Subnetzmaske 255.255.255.0 schickt Daten an den Rechner PC₂ mit der IP 10.1.2.100/24.

Werden die Frames direkt zugestellt oder über einen Router? Ermitteln Sie dazu die jeweilige Netzadresse.

Übungsaufgabe Nr. 5

Betrachten Sie Bild 7.21:



- In welchem Netz befindet sich der PC? Welchen Adressbereich umfasst dieses Netz?
- In welchem Netz befindet sich der Server? Welchen Adressbereich umfasst dieses Netz?
- Wie lautet die Netz-ID des Links zwischen Router 1 und Router 3 und wie lautet der Adressbereich?

7 Switching und Routing

Übungsaufgabe Nr. 6

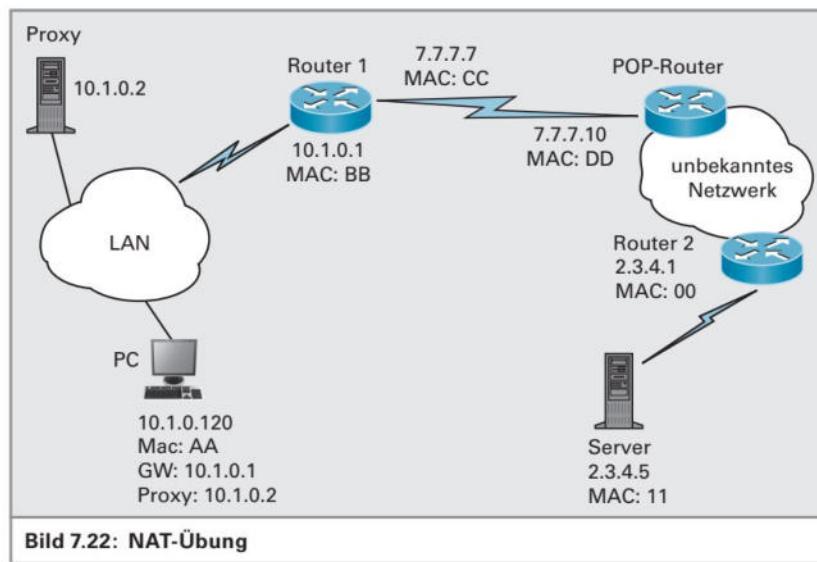
- a) Ein PC₁ mit der Adresse 10.1.1.100 und der Subnetzmaske 255.255.255.192 schickt Daten an den Rechner PC₂ mit der Adresse 10.1.2.200.

Werden die Frames direkt zugestellt oder über einen Router? Ermitteln Sie dazu die jeweilige Netzadresse.

- b) Wie lauten die Adressen der Default-Gateways, wenn als Gateway-Adresse immer die vorletzte Adresse verwendet wird?

Übungsaufgabe Nr. 7

In Bild 7.22 verschickt der PC ein Datenpaket an den Server.



- Welche Ziel-MAC-Adresse und welche Ziel-IP-Adresse verwendet er?
- Welchen Weg nimmt dieses Datenpaket vom PC bis zum Server?
- Welche Ziel-MAC-Adresse und welche Ziel-IP-Adresse verwendet Router 1?