11 Routing

Im komplexen Netzwerk der Firma Lütgens soll organisiert werden, welche Rechnersysteme miteinander kommunizieren sollen. Dies gilt für die Kommunikation der Computer innerhalb eines lokalen Netzwerkes und für die Kommunikation über die Netzwerkgrenzen hinaus. Dafür sind von der Firma B@ltic Networks entsprechende Systeme einzuplanen und zu konfigurieren.

Beim Routing[1] werden für die einzelnen Kommunikationsanforderungen Wege ermittelt und zugewiesen.

Die Wegfindung, Wegauswahl und Wegzuweisung wird durch Routingverfahren ausgeführt.

Die Durchführung dieser Aufgaben wird von Routern übernommen (siehe Abschnitt: 4.3.7: Router). Routingprotokolle beschreiben die jeweils zugrunde liegenden Verfahren.

11.1 Adressbildung

Die Ermittlung von Kommunikationswegen basiert auf eindeutigen Adressinformationen routingfähiger Übertragungsprotokolle. Nicht alle Übertragungsprotokolle definieren Mechanismen für das Routing; sie sind dann nicht routingfähig (z. B. NetBEUI). Zu den routingfähigen Protokollfamilien gehören z. B. IPX/SPX und TCP/IP. Da TCP/IP in der Intranet- und Internet-Kommunikation eingesetzt wird und so zu der am weitesten verbreiteten Protokollfamilie gehört, soll es für dieses Kapitel als Anwendungsbeispiel dienen.

Das Internet-Protokoll (IP) beschreibt unter anderem die Adressierung von Netzwerksystemen. Das aktuelle Protokoll ist die Version 6 (IPv6). In lokalen Netzen wird jedoch üblicherweise auf den Grundlagen der Version 4 adressiert (IPv4). Die Unterschiede in den Protokollen werden im Abschnitt 9.3.2 „Protokolle des Transportsystems“ dargestellt. IP-Adressen der Version 4 haben eine Länge von 32 Bit. Da dieses Bitmuster relativ umständlich für Konfigurationen zu verwenden ist, wird es meist in 4 Oktette aufgeteilt, die wiederum als Dezimalzahlen oder Hexadezimalzahlen codiert sind.

IP-Adressen kennzeichnen ein Rechnersystem und seine Zugehörigkeit zu einem Netzwerk eindeutig.

Eine IP-Adresse könnte folgendermaßen dargestellt werden:

Binäre Darstellung:	11000000.10101000.01101111.01101000
Dezimale Darstellung:	192.168.111.100
Hexadezimale Darstellung:	C0.A8.6F.64

Werden IP-Adressen mehrfach verwendet, so kommt es zu Kommunikationsproblemen innerhalb des Netzwerkes, da eine Nachricht nicht mehr eindeutig einem Adressaten zugeordnet wird.

In der Adressinformation der IP-Adresse sind sowohl die Bezeichnung des Adressaten als auch seine Zugehörigkeit zu einem bestimmten Netzwerk festgelegt. Auf der Basis einer Filtermaske werden Netzzugehörigkeit und Rechneradresse voneinander getrennt. Diese Maske wird als Subnetzmaske bezeichnet. Durch die Bildung von Subnetzen wird eine Gliederung eines Gesamtnetzes in Teilnetze ermöglicht. Je nach

[1] **Route:** franz. Weg, Straße
Routing: engl. (mit franz. Wortstamm) Wegfindung

Anzahl der Rechnersysteme erreicht man damit eine bessere Gliederung der logischen Netzstruktur. Außerdem lässt sich der zur Verfügung stehende IP-Adressbereich effizienter ausnutzen. Durch die Verwendung von Subnetzen wird so eine bessere Wartung und Administration der Netze gewährleistet. Zusätzlich wird dadurch in größeren Netzen eine Reduzierung des Netzwerkverkehrs im Gesamtnetz erzielt, da nicht alle Pakete von den Routern durch das gesamte Netzwerk geleitet werden.

Die Subnetzmaske trennt Netzadresse und Rechneradresse. Subnetzmasken werden für die Einteilung der IP-Adressbereiche in Unternetze verwendet.

Eine Subnetzmaske könnte folgendermaßen aussehen: 255.255.255.0

Subnetzmasken können jedoch auch als „network prefix[1]“ an die IP-Adresse angehängt werden. Für den obigen Beispielfall würde die IP-Adresse (inkl. Subnetzmaske) dann wie folgt aussehen: 192.168.111.100/24. Mit dem Prefix werden die Anzahl der Bits angegeben, die für eine Netzwerkauswertung verwendet werden. Bei der Adressierung nach Netzklassen (siehe Abschnitt 11.1.2: Netzklassen) können die Subnetzmasken nur Längen von 8, 16 oder 24 Bit haben.

11.1.1 Adressauflösung

Durch die Verknüpfung von IP-Adresse und Subnetzmaske werden aus der IP-Adresse die Netzadresse und die Adresse des Rechners (Host-Adresse) gewonnen. Dies geschieht durch die UND-Verknüpfung der beiden Bitmuster. Mit dem Begriff Host wird allgemein jedes in einem Netzwerk angeschlossene IT-System bezeichnet, das über eine eigene IP-Adresse verfügt. Besondere Elemente, die dem Transport von Nachrichtenpaketen dienen, werden darüber hinaus als Intermediate-Systeme bezeichnet.

Um das Zusammenspiel von IP-Adresse und Subnetzmaske nachzuvollziehen, müssen sie in binärer Form betrachtet werden. Werden diese Bitmuster logisch UND-verknüpft, so gewinnt man aus der IP-Adresse zwei Adressteile. Der Teil bis zur ersten Null der Subnetzmaske ist als Netzadresse zu interpretieren. Der dann folgende Anteil an der Subnetzmaske ist als Hostadresse zu verstehen. Die Tabelle zeigt die Verknüpfung der IP-Adresse 192.168.111.100 mit der Subnetzmaske 255.255.255.000.

	Dezimal Darstellung	1. Oktett	2. Oktett	3. Oktett	4. Oktett
IP-Adresse	192.168.111.100	11000000	10101000	01101111	01101000
Subnetzmaske	255.255.255.000	11111111	11111111	11111111	00000000
UND-Verknüpfung	192.168.111.000	11000000	10101000	01101111	00000000
		Netzadresse			Hostadresse

Als Ergebnis der UND-Verknüpfung erhält man die Netzadresse 192.168.111.0. Der verbleibende Anteil bezeichnet die Hostadresse 0.0.0.100. Daraus wiederum ergibt sich, dass nur Rechner mit den IP-Adressen 192.168.111.XXX miteinander in Kontakt treten können. Es folgt daraus, dass die kleinste IP-Adresse eines möglichen Adressraumes immer die Netzadresse angibt (hier 192.168.111.000). Dies ist bei der Vergabe von IP-Adressen zwingend zu berücksichtigen. Ebenfalls zu beachten ist, dass die höchstmögliche IP-Adresse (hier: 192.168.111.255) immer als Broadcast-Adresse

[1] **Prefix:** engl. Präfix, Vorsilbe

Die niedrigste innerhalb eines Netzes zur Verfügung stehende IP-Adresse ist die Netzadresse.
Die höchste innerhalb eines Netzes zur Verfügung stehende IP-Adresse ist die Broadcast-Adresse.
Beide sind somit bereits vergeben und stehen für die Adressierung von Hosts nicht mehr zur Verfügung.

genutzt wird. Bei einer Broadcast-Nachricht werden alle in einem Netz adressierten Rechner angesprochen. Die Zusammengehörigkeit von Rechnern bezüglich der Broadcast-Adressen wird als Broadcast-Domäne bezeichnet.

11.1.2 Netzklassen

Für die Einteilung des Gesamtadressraumes in Subnetze sind durch das IP-Protokoll insgesamt 5 Netze vorgegeben und reserviert. Diese werden in die Klassen A bis E aufgeteilt. Je nach Netzklasse stehen unterschiedliche Adressräume für die Adressierung von Netzen und Hosts zur Verfügung. Die folgende Tabelle zeigt die Einteilung der Netzklassen.

	1. Oktett	2. Oktett	3. Oktett	4. Oktett
Bit-Nr.	0 … … … … 7	8 … … … … 15	16 … … … … 23	24 … … … … 31
Klasse A	0 n n n n n n n	h h h h h h h h	h h h h h h h h	h h h h h h h h
	Netzadresse	Hostadresse	Hostadresse	Hostadresse
	7 Bit nutzbar	24 Bit nutzbar		
Klasse B	1 0 n n n n n n	n n n n n n n n	h h h h h h h h	h h h h h h h h
	Netzadresse	Netzadresse	Hostadresse	Hostadresse
	14 Bit nutzbar		16 Bit nutzbar	
Klasse C	1 1 0 n n n n n	n n n n n n n n	n n n n n n n n	h h h h h h h h
	Netzadresse	Netzadresse	Netzadresse	Hostadresse
	21 Bit nutzbar			8 Bit nutzbar
Klasse D	1 1 1 0 m m m m	mmmmmmmm	mmmmmmmm	mmmmmmmm
	Multicast-Adresse	Multicast-Adresse	Multicast-Adresse	Multicast-Adresse
	28 Bit nutzbar			
Klasse E	1 1 1 1 r r r r	r r r r r r r r	r r r r r r r r	r r r r r r r r
	reserviert	reserviert	reserviert	reserviert
	27 Bit nutzbar			

Zu identifizieren sind diese Netze anhand der blau gekennzeichneten Bits. Die Adressen der Klasse D werden für die besondere Adressierung mit Multicast-Adressen genutzt. Dabei können mehrere Rechner gleichzeitig eine Nachricht empfangen. Die Adressen der Klasse E sind für experimentelle Zwecke reserviert.

Aus der obigen Einteilung der Netze lassen sich die theoretisch nutzbaren Adressräume entwickeln.

Klasse	IP-Adressraum	Maximale Anzahl von Netzen[1]	Maximale Anzahl von Rechnern pro Netz
A	0.0.0.0 – 127.255.255.255	126	16 777 214
B	128.0.0.0 – 191.255.255.255	16 382	65 534
C	192.0.0.0 – 223.255.255.255	2 097 150	254
D	224.0.0.0 – 239.255.255.255	Multicast	
E	240.0.0.0 – 255.255.255.255	Reserviert	

1. Aus welcher Netzklasse stammt die IP-Adresse 162.167.110.112?
2. Erläutern Sie, ob die IP-Adresse 192.168.123.255 nutzbar ist.
3. Welche Fehler enthält die IP-Adresse 242.224.266.200?

11.1.3 Klassenlose Netze

In der Firma Lütgens existieren mehrere kleine Netzwerke. Ihr Umfang beträgt häufig nicht mehr als 20 Rechner. Diese Rechner sollen weiterhin jeweils in eigenen Adressräumen zusammengefasst werden.

Häufig wird für die Adressierung von Netzen auf IP-Adressen eines Klasse-C-Netzwerkes zurückgegriffen. Innerhalb eines Intranets sind dies praktisch immer Adressen aus den für diese Zwecke reservierten freien Adressbereichen (siehe Abschnitt 11.2: Adressvergabe). Es stehen pro Netzwerk maximal 254 IP-Adressen für die Adressierung von Hosts zur Verfügung. Dieser Betrag berechnet sich aus 256 möglichen Adressen aus dem ersten Oktett abzüglich der Netzadresse und der Broadcastadresse. Bei der Nutzung von beispielsweise 20 Rechnern bleiben also 234 Adressen ungenutzt. Sollen jedoch im anderen Fall über 254 Rechner adressiert werden, so müsste ein Klasse B Netzwerk verwendet werden. Hier sind dann bis zu 65534 Rechner adressierbar. An diesen beiden Beispielen wird deutlich, dass die Einteilung der Netze in Klassen nur eine sehr grobe Zuordnung bezüglich der Anzahl von Rechnern zu Netzwerken zulässt.

Zur Optimierung der Adressvergabe wird deshalb zunehmend eine klassenlose Adressierung der Netze verwendet, was man als CIDR (Classless Inter Domain Routing) bezeichnet.

Zur effizienteren Ausnutzung von IP-Adressräumen wird die klassenlose Adressbildung angewandt.

Bei dieser Art der Adressbildung wird die Konvention der Netzklassenzuordnung aufgehoben. Damit steht für die Bildung der Subnetzmaske eine „beliebige Länge“ von Bits zu Verfügung, d. h. dass die Subnetzmaske eine Anzahl von 1er Bits zwischen 0 und 32 annehmen kann.

Dieser Vorgang kann auch als Aufteilung eines Netzes bzw. Verschmelzung zweier Netze betrachtet werden.

[1] Da in den einzelnen Klassen Adressen für besondere Verwendungszwecke reserviert werden, kommt es zu einer Abweichung zwischen dem theoretisch möglichen Wert und der Anzahl der tatsächlich zur Verfügung stehenden Netz- und Hostadressen.

Die Aufteilung eines Netzes in Subnetze wird als Subnetting bezeichnet.
Die Verschmelzung mehrerer Netze zu einem Netz wird als Supernetting bezeichnet.

Im Folgenden wird der Vorgang des Aufteilens eines Netzwerkes in Subnetze beispielhaft erläutert:

Das Netz mit der IP-Adresse 192.168.123.0 soll in vier Teilnetze zerlegt werden. Dazu werden zwei Bits des 4. Oktetts für die Subnetzmaske verwendet. Mit diesen zwei Bits lassen sich vier mögliche Subnetze adressieren.

	Dezimal-Darstellung	1. Oktett	2. Oktett	3. Oktett	4. Oktett
IP-Adresse	192.168.123.000	11000000	10101000	01111011	00 000000
Subnetzmaske	255.255.255.192	11111111	11111111	11111111	11000000
UND-Verknüpfung	192.168.123.000	11000000	10101000	01111011	00 000000
		Netzadresse			Host-adressen

Es ergibt sich dann folgende Adressverteilung:

Erste IP-Adresse	Letzte IP-Adresse	Kommentar
192.168.123.0		Netzadresse des Gesamtnetzes und Netzadresse des ersten Subnetzes
192.168.123.1	192.168.123.63	Adressbereich nicht nutzbar
162.168.123.64		Netzadresse des zweiten Subnetzes
162.168.123.65	192.168.123.126	62 adressierbare Hosts im zweiten Subnetz
192.168.123.127		Broadcast-Adresse im zweiten Subnetz
192.168.123.128		Netzadresse des dritten Subnetzes
192.168.123.129	192.168.123.190	62 adressierbare Hosts im dritten Subnetz
192.168.123.191		Broadcast-Adresse des dritten Subnetzes
192.168.123.192	192.168.123.254	Adressbereich nicht nutzbar
192.168.123.255		Broadcast-Adresse des vierten Subnetzes und des Gesamtnetzes

Diese Tabelle muss anschließend dahingehend interpretiert werden, welche IP-Adressen gemäß den Konventionen genutzt werden können.

- Der IP-Adressbereich des gesamten ersten Netzes ist nicht nutzbar, da hier die Netzadresse des Hauptnetzes (192.168.123.0) enthalten ist.
- Der IP-Adressbereich des gesamten vierten Netzes ist nicht nutzbar, da hier die Broadcast-Adresse des Hauptnetzes (192.168.123.255) enthalten ist.
- Im zweiten und dritten Subnetz sind jeweils die ersten (Subnetzadressen) und letzten (Broadcast-Adressen) nicht nutzbar.

Somit sind von den ursprünglich verfügbaren 254 IP-Adressen des Netzes 192.168.123.0 nur noch 124 (2×62) Adressen für die Adressierung von Hosts verfügbar.

Folgende „Faustformeln“ sind für die Berechnung der Anzahl der Subnetze und der theoretisch möglichen IP-Adressen geeignet. Die Zahlenwerte stammen aus dem obigen Beispiel.

Anzahl der IP-Adressen je Subnetz = 256 – 4. Oktett der Subnetzmaske = 256 – 192 = 64

Anzahl der Subnetze = 256 / Anzahl der Adressen je Subnetz = 256 / 64 = 4

Der Vorgang der Verschmelzung zweier Netze ist im Prinzip nach dem obigen Schema durchzuführen. Es ist nur die Subnetzmaske (z. B. 255.255.254.0) entsprechend anzupassen und ein anderes Netz (z. B. 192.168.0.0) auszuwählen. In der Praxis hat vorwiegend die Verschmelzung von ehemaligen Klasse-C-Netzwerken Bedeutung. In der Praxis lassen sich häufig auch das erste und letzte Netz nutzen. Dazu müssen jedoch die verwendeten Protokolle sicherstellen, dass auch die Subnetzmaske mit übermittelt wird. Nur so ist eine Zuordnung der Subnetze möglich.

1. Begründen Sie die oben angegebenen Faustformeln.
2. Stellen Sie beispielhaft die Verschmelzung zweier Klasse-C-Netze dar.

11.2 Adressvergabe

Die Computer in einem Subnetz der Firma Lütgens sind mit IP-Adressen zu versehen.

Im vorhergehenden Abschnitt sind die Adressräume für die Vergabe von IP-Adressen dargestellt worden. Soll eine Adressvergabe nach Netzklassen erfolgen, so stehen im Prinzip die oben aufgeführten Adressräume zur Verfügung. Sie werden weltweit einmalig durch autorisierte Stellen vergeben. Weltweit wird dies durch das ICANN[1] organisiert. In der Bundesrepublik Deutschland erfüllt diese Aufgabe die DeNIC GmbH. Anbieter von Netzwerkdiensten, so genannte Provider, kaufen Adresskontingente von den regionalen Registrierungsstellen (NIC[2]) und verkaufen diese dann an Endkunden. Im Abschnitt 12.6.1: „Domain Name System“ wird die Verbindung von IP-Adressen und Domänen-Namen erläutert.

Die Vergabe von IP-Adressen in einem lokalen Netzwerk kann nicht beliebig erfolgen.

Für die Vergabe in lokalen Netzen sind deshalb besondere Adressbereiche reserviert. Es muss von dem Einrichter sichergestellt werden, dass Anforderungen dieser IP-Adressen nicht in das Internet gelangen. Weiterhin sind die Adressreservierungen für die Netzadresse und die Broadcast-Adresse (siehe oben) zu beachten.

Die folgenden Adressen bzw. Bereiche sind ebenfalls reserviert:

0.0.0.0: Eigentlich die erste Netzadresse. Diese Adresse wird für das Routing benötigt und ist reserviert für die Standardroute eines Routers. Über diese Adresse werden alle Nachrichtenpakete geleitet, deren Empfängeradressen dem Router unbekannt sind.

127.0.0.0: Diese und die folgende Adresse sind als „loop back[3]“ dem Endgerät bzw. Netz zugeordnet. Über diese Adressen wird ein Rückkopplungstest durchgeführt. Die IP-Adresse 127.0.0.1 wird von lokalen Endgeräten genutzt.

[1] **ICANN: I**nternational **C**onference on **A**rtificial **N**eural **N**etworks; engl. Internationale Konferenz für künstliche neuronale Netze

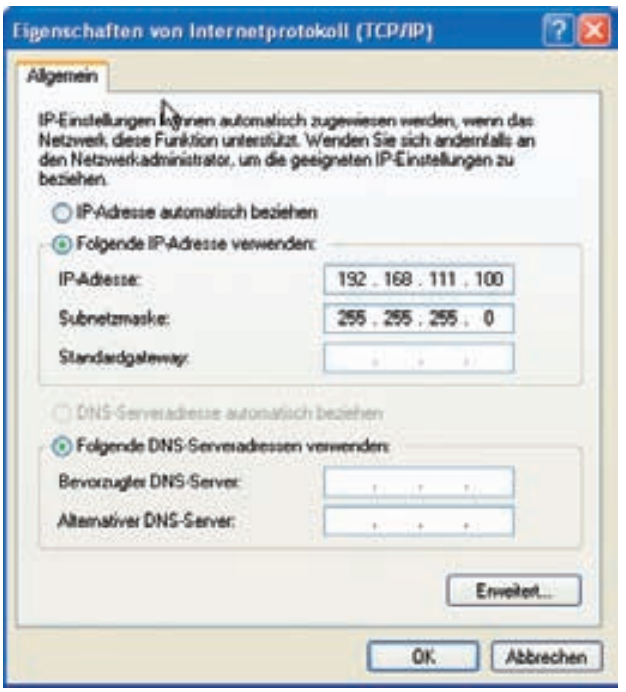
[2] **NIC: N**etwork **I**nformation **C**enter, engl. Netzwerk-Informations-Zentrum, in Deutschland DeNIC (De für Deutschland)

[3] **Loop Back:** engl. Rückschluss-Schleife

Für die freie Vergabe von IP-Adressen innerhalb eines lokalen Netzwerkes stehen also folgende Adressbereiche zur Verfügung:

Netzklasse	Anzahl der Netze	Netzadressen	Subnetzmaske	IP-Adressbereich
Klasse A	1	10.0.0.0	255.0.0.0	10.0.0.1 – 10.255.255.254
Klasse B	16	172.16.0.0 – 172.31.0.0	255.255.0.0	172.16.0.1 – 172.31.255.254
Klasse C	256	192.168.0.0 – 192.168.255.0	255.255.255.0	192.168.0.1 - 192.168.255.254

Überlegen Sie, welche Adressräume bzw. Netzklassen für die Vernetzung Ihres Betriebes/Ihrer Schule verwendet werden können. Begründen Sie Ihre Auswahl.



11.2.1-1 IP-Adresseintrag

Die temporär vergebene IP-Adresse wird als Lease[4] bezeichnet.

11.2.1 Statische IP-Adressen

IP-Adressen können bei der Einrichtung und Konfiguration eines Netzes dem jeweiligen Betriebssystem des Hosts übergeben werden. Sie werden dazu in den entsprechenden Menüs eingetragen.

In nebenstehendem Beispiel sind die Adresse 192.168.111.100 und die Subnetzmaske 255.255.255.0 dem Rechner fest zugeordnet worden. Die IP-Adresse ist damit statisch, d. h. das System wird zukünftig immer diese IP-Adresse und Subnetzmaske verwenden. Eine Kommunikation ist in diesem Fall nur mit Rechnern aus dem Adressraum 192.168.111.XXX möglich.

11.2.2 DHCP-Dienst

Anstatt eine statische IP-Adresse zu nutzen, kann der Rechner auch automatisch eine IP-Adresse von einem Server beziehen. Der Server muss den DHCP-Dienst[1] anbieten. Am Client ist einzustellen, ob er bei der Anmeldung nach einem vorhandenen DHCP-Server suchen soll oder ob er direkt von einem vorgegebenem DHCP-Server eine IP-Adresse beziehen soll. Weiterhin kann der DHCP-Client auch Informationen bezüglich anderer Netzwerkdienste abfordern. Das betrifft z. B. die Dienste WINS[2] und DNS[3], aber auch Proxy-Einstellungen können übermittelt werden.

Auf dem DHCP-Server sind umfangreichere Einstellungen vorzunehmen. Diese betreffen vor allem den zu verwaltenden Adresspool und die Dauer der Adressvergabe.

- IP-Adresspool: Mit der Einrichtung eines IP-Adresspools wird der Bereich festgelegt, aus dem der DHCP-Server IP-Adressen an die Clients vergeben soll. Dies geschieht durch die Angabe von Anfangs- und Endadresse des IP-Adressbereiches und der Subnetzmaske.

[1] **DHCP: D**ynamic **H**ost **C**onfiguration **P**rotocol, engl. Protokoll zur dynamischen Konfiguration von Hosts
[2] **WINS: W**indows **I**nternet **N**ame **S**ervice, engl. Internet-Namen Auflösungsdienst unter Windows
[3] **DNS: D**omain **N**ame **S**ervice, engl. Domänen Namen Dienst
[4] **Lease:** engl. Pacht, Miete

- Ausschlussbereiche: Sollen bestimmte IP-Adressbereiche aus dem Adresspool nicht vergeben werden, so können sie innerhalb des IP-Adresspools reserviert werden. Dies ist vor allem dann sinnvoll, wenn innerhalb des IP-Adresspools Server mit festgelegten Aufgabenstellungen oder Routern arbeiten.
- Dauer: Es kann verwaltet werden, über welchen Zeitraum eine IP-Adresse an einen Client vergeben wird. Nach Ablauf der Zeit wird dem Client eine neue IP-Adresse zugewiesen.

Die Adressvergabe erfolgt indem der Client beim Server nach einer IP-Adresse anfragt. Der Server bietet daraufhin eine IP-Adresse an. Wird diese vom Client tatsächlich angenommen, erfolgt eine Registrierung auf dem Server.
Die dynamische Vergabe von IP-Adressen ist zum Beispiel bei Funknetzen vorteilhaft, da sich die Teilnehmer überwiegend nur für begrenzte Zeiträume im Netz befinden.

Vorteile:

- **einfache Administration**
- **leichte Erweiterbarkeit**

Nachteile:

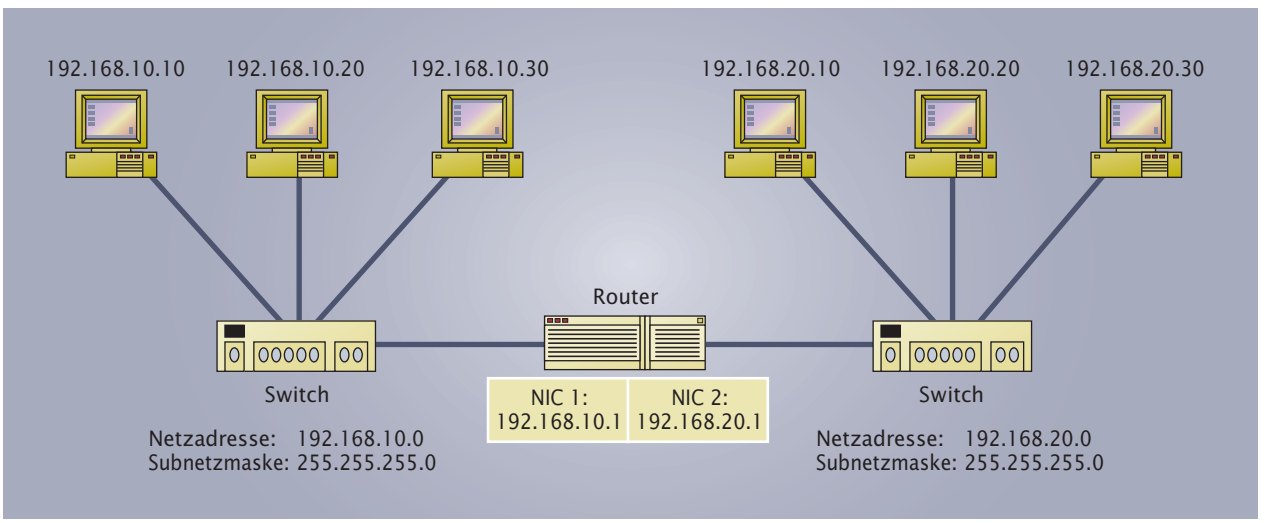
- **schwerere Nachvollziehbarkeit von Zugängen (kann als Sicherheitskriterium im Internet auch ein Vorteil sein, da die Identität verschleiert wird)**

11.3 Funktionsweise eines Routers

Innerhalb eines Intranets und im Internet sind viele Netze miteinander verknüpft. Sollen Rechner des einen Netzes mit Rechnern eines anderen Netzes kommunizieren, muss ein spezielles System diese Netze miteinander verbinden. Dieses System muss in beiden Netzen vorhanden sein (dual homed) und wird Router genannt.

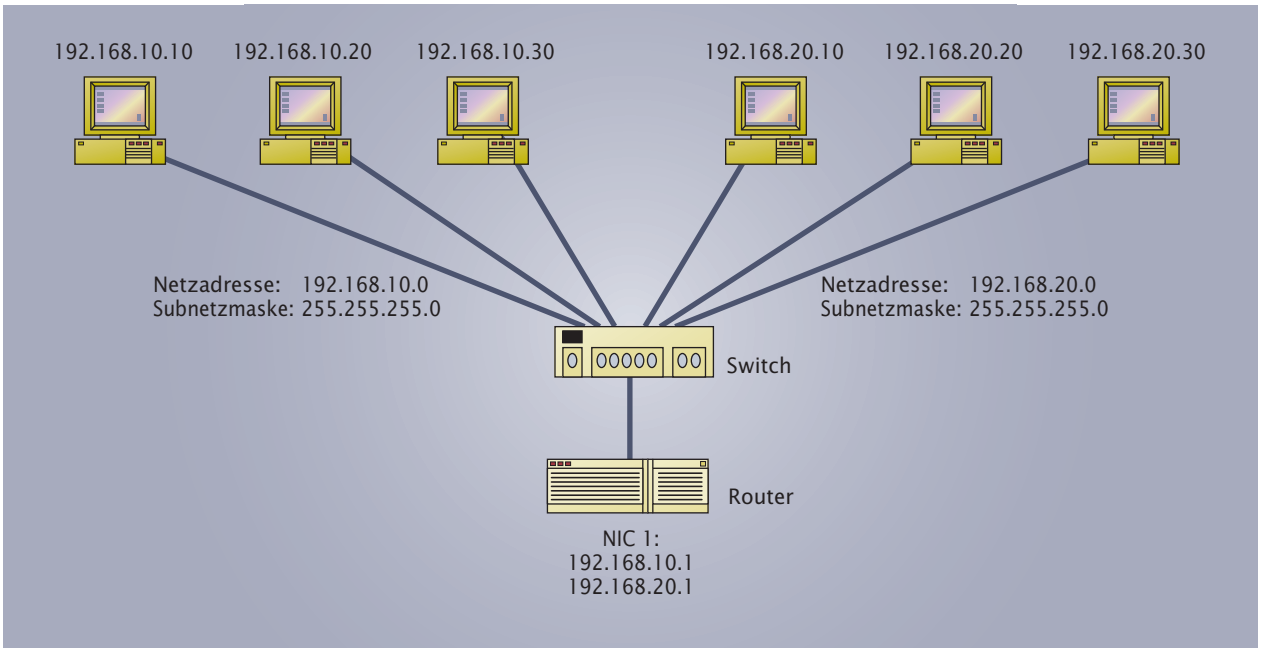
Ein Router gehört adressmäßig zu mehreren Netzen und kann einen Paketaustausch zwischen diesen Netzen organisieren.

Da ein Router für diese Arbeit Adressen routingfähiger Übertragungsprotokolle benutzt, arbeitet er auf den Schichten 1 bis 3 des ISO/OSI-Referenzmodells (siehe Abschnitt 4.3.7: Router).



11.3-1 Verbindung zweier Netze über einen Router

In der Grafik 11.3-1 verbindet der Router die Subnetze 192.168.10.0 und 192.168.20.0. Alle in den Subnetzen befindlichen Rechner können mit allen Rechnern des anderen Netzes in Kontakt treten. Der Router verfügt in diesem Fall über zwei Netzwerkadapter, die per IP-Adresse jeweils einem Netz zugeordnet sind.



11.3-2 Organisatorische Verbindung zweier Netze über einen Router

Durch die Grafik 11.3-2 wird deutlich, dass die Arbeit eines Routers nicht zwangsläufig an eine bestimmte physikalische Vorgabe gebunden ist. Im speziellen Fall wurden einer Netzwerkkarte zwei IP-Adressen zugewiesen. Die Funktionsweise ist ansonsten mit der in Grafik 11.3-1 dargestellten Arbeitsform identisch. Angewendet wird dieses Verfahren zum Beispiel:

- zur Filterung von Paketen in einer Firewall
- zur Erweiterung eines Netzes.

TIPP

Für die Arbeit des Routers ist es zwingend notwendig, dass die Funktion „IP-Forwarding[1]“ im Betriebssystem aktiviert wurde. Bei der Konfiguration eines Netzwerkes wird dies normalerweise automatisch vom Betriebssystem übernommen.

Für die Durchführung der Arbeit werden im Router Adresstabellen hinterlegt, die beschreiben, welche Netze oder Hosts miteinander kommunizieren können bzw. dürfen. Diese Tabellen werden Routingtabellen genannt. Erzeugt werden diese Tabellen entweder durch die manuelle Eingabe in die Tabellen oder durch Algorithmen, die auf speziellen Routingprotokollen basieren.

IP-Forwarding ist eine Funktion des Betriebssystems. Ist das Forwarding aktiviert, lässt das Betriebssystem es zu, dass eine IP-Adresse in ein anderes Netz weitergereicht werden darf.

1. Nennen Sie mögliche Vor- und Nachteile der in den Grafiken 11.3-1 und 11.3-2 dargestellten Verbindungsformen.
2. Wägen Sie diese Vor- und Nachteile gegeneinander ab.

[1] **Forwarding:** engl. weiterreichen

11.3.1 Statisches Routing

Beim statischen Routing werden manuell alle benötigten Routen in die Routingtabellen der Router eingetragen. Auf diese Weise wird festgelegt, welche Netze organisatorisch miteinander verbunden sind und welche Wege Nachrichtenpakete nehmen können. Das statische Routen ermöglicht eine sehr passgenaue Vorgabe der Kontaktmöglichkeiten zwischen angeschlossenen Hosts. Bei größeren Netzen bzw. bei der Verwendung mehrerer Router kann dieses Verfahren zu Problemen führen, da in den einzelnen Routern sehr viele Einträge vorgenommen werden müssen. Darüber hinaus ist bei Ausfall eines Routers trotz dem Vorhandensein alternativer Wege keine Möglichkeit zur Kommunikation mehr gegeben, da diese Wege nicht dynamisch erkannt und genutzt werden.

Beispielhaft soll die mögliche Routingtabelle für die Verwendung nach Grafik 11.3-1 aufgestellt und erläutert werden. Die Tabelle stellt die Routinginformationen des ersten Hosts (192.168.10.10/24) dar. Diese Konfiguration ist auch Bestandteil des vertiefenden Exkurses „Routing“.

Verwendung	Netzwerkadresse	Subnetzmaske	Gateway-Adresse	Schnittstelle	Anzahl
Default Route	0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	1
Loopback Network	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
Directly attached Network	192.168.10.0	255.255.255.0	192.168.10.10	192.168.10.10	1
Local Host	192.168.10.10	255.255.255.255	127.0.0.1	127.0.0.1	1
Network Broadcast	192.168.10.255	255.255.255.255	192.168.10.10	192.168.10.10	1
Multicast Address	224.0.0.0	224.0.0.0	192.168.10.10	192.168.10.10	1
Limited Broadcast	255.255.255.255	255.255.255.255	192.168.10.10	192.168.10.10	1

Die einzelnen Spalten der Tabelle haben folgende Bedeutungen:

- Die Netzwerkadresse bezeichnet das Ziel eines IP-Datenpaketes. Dies können Hosts, Netze oder Subnetze sein.
- Die Subnetzmaske ordnet das Netzwerk einer Klasse zu. Im Zusammenhang mit der Netzwerkadresse ergibt sich eine Adressierung von Host und Netzwerk.
- An die Gatewayadresse werden die Datenpakete geschickt. Hierbei kann es sich um lokale Netzwerkadapter oder auch externe Gateways handeln, die direkt erreichbar sind.
- In der Spalte Schnittstelle sind die konkreten IP-Adressen lokaler Netzwerkadapter aufgeführt.
- Der letzte Eintrag gibt die Anzahl der folgenden Router oder Vermittlungsstationen bis zum Ziel an. Diese werden auch als Sprünge (Hops) bezeichnet.

Die einzelnen Zeilen können folgendermaßen „gelesen“ werden:
„Alle IP-Pakete mit dem Ziel (Spalte Netzwerkadresse UND Spalte Subnetz-Maske) gehen über die physikalische oder logische Schnittstelle. Evtl. werden sie dann über eine spezielle Adresse weitergereicht (Spalte Gateway).“ Für die Zeile „Directly attached Network“ bedeutet das: „Alle IP-Pakete deren Adressaten zum Netz

192.168.10.0/24 gehören (192.168.10.xxx) werden an die Schnittstelle 192.168.10.10 (Netzwerkkarte) gereicht."

Für das oben dargestellte Beispiel haben die einzelnen Einträge folgende Funktion:

- Default Route:
  Die „Default Route" ist die Standardroute, die für alle Netzadressen genutzt wird, die nicht in der Routingtabelle aufzulösen sind. In einigen Betriebssystemen wird diese Route auch als Standardgateway bezeichnet. Im obigen Fall werden über die Schnittstelle 192.168.10.10 alle Anforderungen mit unbekannten IP-Adressen an das Gateway mit der Adresse 192.168.10.1 weitergeleitet. Die Adressierung 0.0.0.0 wird genutzt, wenn die IP-Adresse des Ziels nicht bekannt ist.

- Loopback Network:
  Das Netzwerk 127.0.0.0 ist ausschließlich für den Funktionstest reserviert. Der englische Begriff „loopback" bezeichnet einen Rückschluss. Mit dieser Netzwerkadresse wird die logische Funktion des Protokollstapels geprüft. Eine physikalische Verbindung ist somit nicht notwendig. Die „Local Host" Adresse steht im Zusammenhang mit dem Loopback Netzwerk.

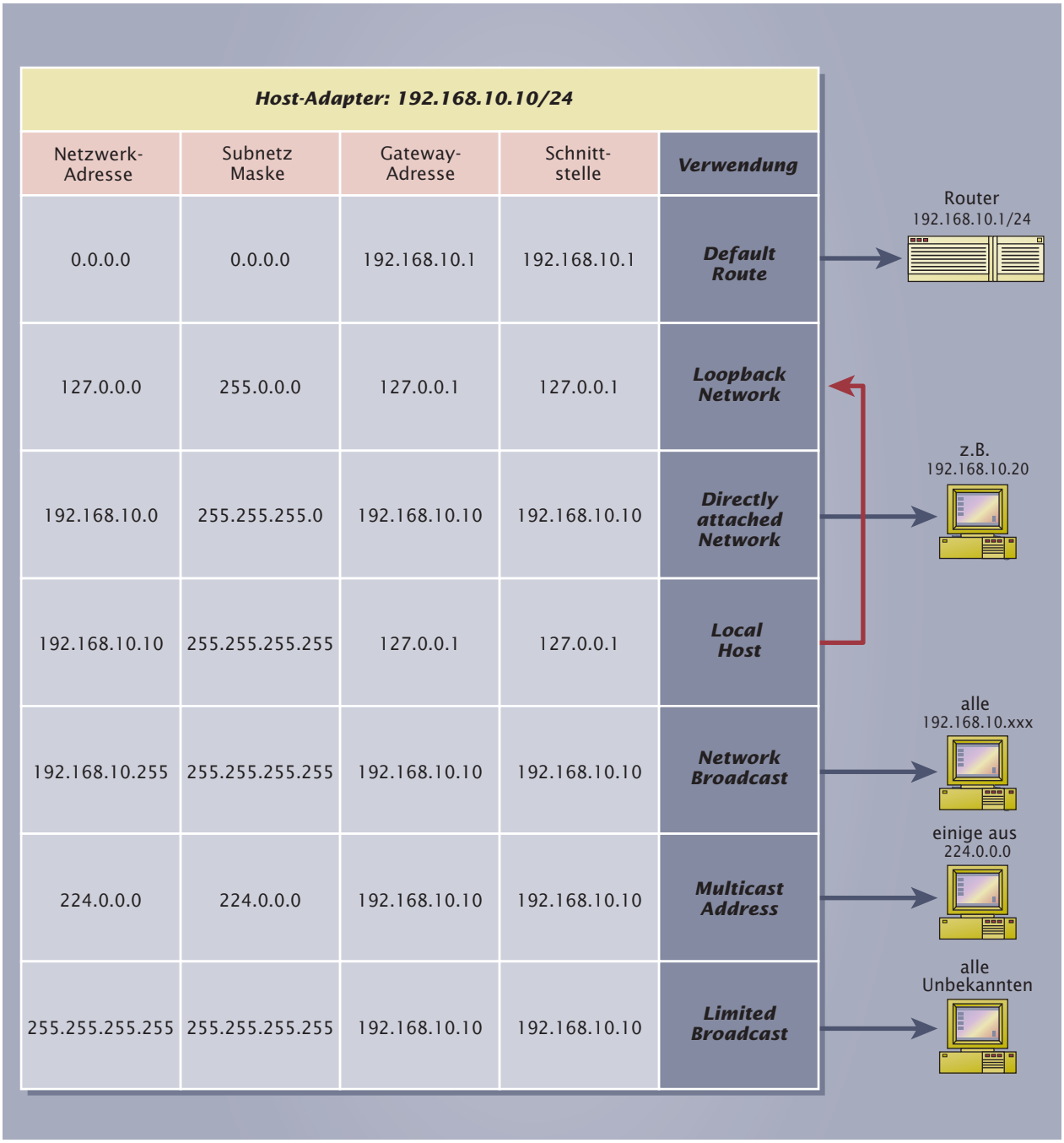
- Directly attached Network:
  Hier wird das direkt an die Netzwerkkarte (192.168.10.10) angeschlossene Netzwerk (192.168.10.0) adressiert. Alle IP-Pakete an Teilnehmer des Netzwerkes 192.168.10.0 werden über die Schnittstelle 192.168.10.10 versandt.

- Local Host:
  Über den Local Host (eigener, lokaler Host) werden IP-Pakete, die z. B. zu Testzwecken an die eigene Netzwerkkarte (192.168.10.10) übermittelt werden, der IP-Adresse 127.0.0.1 zugewiesen. Diese ist nur virtuell vorhanden. Im Zusammenhang mit dem Loopback Netzwerk werden IP-Pakete die an die Netzwerkkarte gehen, dann über den Rückschluss des Netzes 127.0.0.0 zurückgemeldet. Eine physikalische Übermittlung findet nicht statt. So ist ein Funktionstest des Protokollstapels möglich.

- Network Broadcast:
  IP-Pakete, die an alle Teilnehmer des Netzwerkes 192.168.10.0 versandt werden sollen (Broadcast), werden über die Schnittstelle 192.168.10.10 übermittelt. Die Netzwerkadresse jedes Hosts muss bekannt sein. Aus diesem Grund wird dieser Eintrag auch als Directed Broadcast Address (gerichtete Broadcast-Adresse) bezeichnet.

- Multicast Address:
  Sollen nur Gruppen von Rechnern angesprochen werden (Multicast), so ist dafür die Netzadresse 224.0.0.0 reserviert. Es werden dann Kopien der IP-Pakete über die Schnittstelle 192.168.10.10 an alle Mitglieder der Multicast-Gruppe übermittelt.

- Limited Broadcast:
  Die Limited Broadcast Address (begrenzte Broadcast-Adresse) wird genutzt, wenn allen Hosts eine Nachricht übermittelt werden soll, deren Zieladressen aber noch nicht bekannt sind. Dies ist zum Beispiel beim Systemstart der Fall. Die über die Limited Broadcast Address versendeten IP-Pakete werden nur innerhalb des physikalischen Netzes weitergeleitet.



11.3.1-1 Einfaches Routing

Unter bestimmten Voraussetzungen kann es notwendig sein, einzelne Hostadressen in den Routingtabellen zu verwalten. Dies betrifft Fälle, in denen ein Host zwar physikalisch in einem bestimmten Netz angeschlossen wurde, organisatorisch aber zu einem anderen Netz gehört. Im Exkurs „Routing“ wird ein komplexes Beispiel erläutert.

11.3.2 Dynamisches Routing

Für komplexere Netze sowie bei Netzen, die häufigen Änderungen unterworfen sind, ist es sinnvoll, die Routen berechnen zu lassen, anstatt sie vorzugeben. So kann auch besser auf gestörte Leitungsverbindungen reagiert werden. Um diese Aufgaben zu erfüllen, müssen zum einen die angeschlossenen Router ständig die aktuellen Verbindungen überprüfen und zum anderen die Router diese Informationen untereinander austauschen. Auf diese Weise ist der Weg eines Datenpaketes nicht genau vorherbestimmt und kann sich dynamisch verändern. Das hat zur Folge, dass beim Austausch von Datenpaketen unterschiedliche Hin- und Rückwege verwendet werden können.

Für die Berechnung der Routen und für den Austausch von Routinginformationen werden spezielle Algorithmen eingesetzt. Diese werden in den entsprechenden Routingprotokollen beschrieben. In die Berechnung können folgende Kriterien eingehen:

- Länge des Weges
- Kosten der Verbindung
- Bandbreite
- Auslastung
- Wegverzögerung.

Die Metrik ist eine Maßzahl für die Bewertung einer Netzwerkverbindung.

Die Bewertungen der Kriterien werden als Metriken bezeichnet.

Auch dynamisch routende Systeme arbeiten auf den Schichten 1 bis 3 des ISO/OSI-Referenzmodells. Der Austausch und die Verarbeitung von Informationen erfolgt jedoch auf höheren Schichten.

Die Ergebnisse der Berechnungen der Routen führen dann zu einer Anpassung der Routing-Tabellen. Auf der Basis der Metriken lassen sich zwei klassische Routing Verfahren ableiten.

Distance Vector Routing

Das Distance Vector Routing[1] basiert auf dem Distance Vector Algorithmus. Hier werden grundsätzlich alle Router des Netzes unabhängig von ihrer Position im Gesamtnetz als gleichwertig und gleichberechtigt betrachtet. Sie tauschen in kurzen Zeitabständen untereinander Informationen aus, die ihre aktuellen Pfade sowie die Kosten eines Kommunikationsweges betreffen. Diese Kosten basieren auf der Annahme, dass ein Zusammenhang besteht zwischen der relativen Entfernung zu einem Ziel und den Kosten. Die relative Entfernung wird angegeben in der Anzahl der Zwischenstationen bzw. der Sprünge, die eine Nachricht über Zwischenstationen durchführen muss.

Die Anzahl der Sprünge werden als Hops[2] angegeben.

Damit es nicht zu möglichen Schleifenbildungen in einer komplexen Struktur kommt, ist von vornherein die Anzahl der zulässigen Hops auf 16 begrenzt. Das Protokoll ist relativ einfach zu implementieren, benötigt jedoch eine gewisse Netzkapazität für den Austausch der Informationen. Typische Vertreter wie das klassische RIP (Routing Information Protocol) und das firmenspezifische IGRP (Interior Gateway Routing Protocol) der Firma CISCO basieren auf Implementierungen des Distance Vector Algorithmus.

[1] **Distance Vector Routing:** engl. Routing nach der Richtung und Entfernung der Stationen
[2] **Hops:** engl. Sprünge

Link State Routing

Das Link State Routing[1] basiert auf dem Link State Algorithmus. Auch beim Link State Routing werden zwischen den Routern Informationen ausgetauscht. Die Informationen enthalten Angaben darüber, ob angeschlossene Verbindungswege betriebsbereit sind und wie die bisher erkannte Struktur des Netzes aussieht. Dieser Informationsaustausch geschieht jedoch in erheblich längeren Zeitintervallen. Werden zwischen den Zeitintervallen von einem Router Änderungen z. B. bezüglich des Status benachbarter Router erkannt, so werden diese umgehend an alle Router gemeldet. Aus allen verfügbaren Informationen generiert jeder Router ein komplettes Netzabbild. Für die Berechnung des Netzabbildes müssen die Router über eine höhere lokale Rechenleistung verfügen. Dafür ist das Nachrichtenaufkommen im Netz geringer, was wiederum die Bandbreite des Netzes weniger stark belastet. Typische Vertreter sind das OSPF-Protokoll (Open Shortest Path First) und das Intermediate-System-to-Intermediate-System-Protokoll (IS-IS).

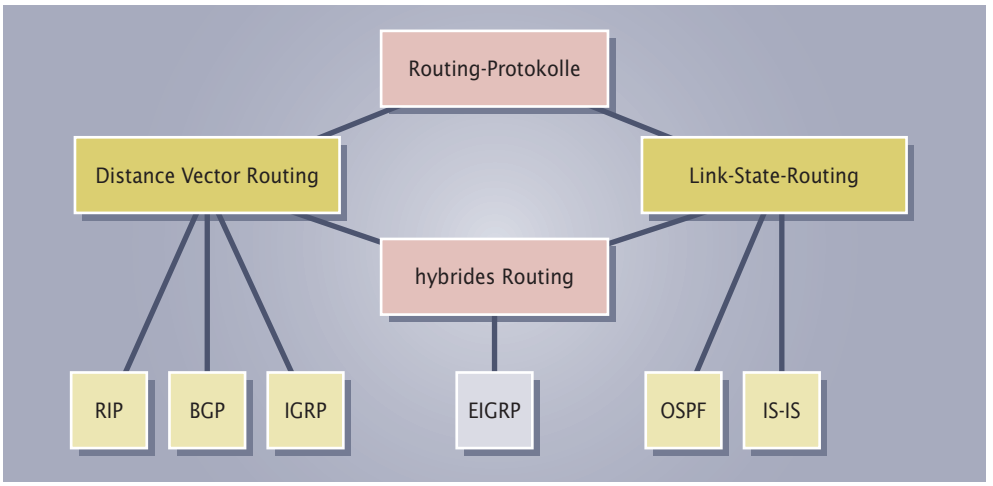
Stehen Netze unter einer gemeinsamen Verwaltung mit einer einheitlichen Routingstrategie, bezeichnet man sie als Autonome Systeme (AS).

Diese Autonomen Systeme tauschen dann wiederum an ihren Verbindungsstellen Routinginformationen aus. Aus dieser Einteilung heraus werden Routingprotokolle nicht primär nach dem verwendeten Algorithmus eingeteilt, sondern nach ihrem Einsatz in Autonomen Systemen oder zwischen Autonomen Systemen.

- Routingprotokolle, die zu den Interior Gateway Protocols (IGP) gehören, werden in Autonomen Systemen verwendet.
- Routingprotokolle, die zu den Exterior Gateway Protocols (EGP) gehören, werden zur Kommunikation zwischen Autonomen Systemen verwendet.

Router, die zwischen Autonomen Systemen routen, werden als Core-Router[2] bezeichnet.

Die folgende Grafik ordnet die gängigsten Routingprotokolle ein:



11.3.2-1
Einordnung von Routingprotokollen

Beispielhaft sollen im Folgenden drei typische Routing-Protokolle vorgestellt werden:

Routing Information Protocol

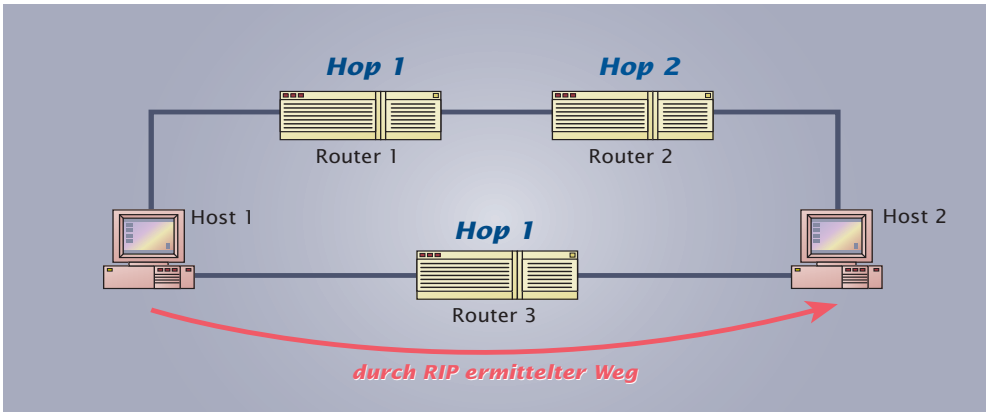
Das Routing Information Protocol (RIP[3]) ist eng mit der Entwicklung von UNIX und damit der Protokollfamilie TCP/IP verbunden. Es ist eines der ältesten dynamischen Routingprotokolle. Da eine Vielzahl von Internet-Servern auf der Basis von UNIX oder einem Derivat arbeiten, ist RIP auch heute noch weit verbreitet. RIP gehört zu

[1] **Link State Routing:** engl. Routing nach dem Status der Verbindung
[2] **Core:** engl. Kern
[3] **RIP: R**outing **I**nformation **P**rotocol, engl. Routing Informations Protokoll

den Distance Vector Protokollen. Bei der Nutzung von RIP werden die Routerinformationen regelmäßig alle 30 Sekunden mit Hilfe eines so genannten RIP-Broadcast allen erreichbaren Routern mitgeteilt. Die übermittelten Informationen betreffen diejenigen Netzwerke,

- auf die der sendende Router zugreifen kann
- und welches der jeweils kürzeste Weg für ein Datenpaket ist.

Die Nachrichten werden über den UDP-Port 520 und das UDP-Protokoll versandt. RIP-Datagramme haben eine Paketgröße von 520 Bytes. Sind die Informationen umfangreicher, so wird die Nachricht in einzelne aufeinander folgende UDP-Datagramme zerlegt. Wird innerhalb von 180 Sekunden keine Information von einem Router empfangen, so wird der Eintrag über diese Gegenstelle als nicht mehr erreichbar betrachtet. Darin liegt eine der Schwachstellen des Protokolls. Ein nicht erreichbarer Router wird frühestens nach 180 Sekunden erkannt. Innerhalb dieser Zeit wird dieser Weg jedoch weiterhin genutzt, was zu einem erhöhten Kommunikationsaufkommen führt. In den Informationen wird auch angegeben, welche Ziele der sendende Router erreichen kann und wie viele Hops die Nachricht zum Ziel benötigt. Die Auswahl der Route basiert im Wesentlichen auf den Informationen über die Anzahl der Hops zum Zielhost. Da diese Anzahl durch das UDP-Protokoll auf 16 Hops begrenzt ist, werden Ziele, die weiter entfernt sind, nicht erreicht. Gängige eingesetzte Version ist RIP2, die auf RIP1 aufbaut.

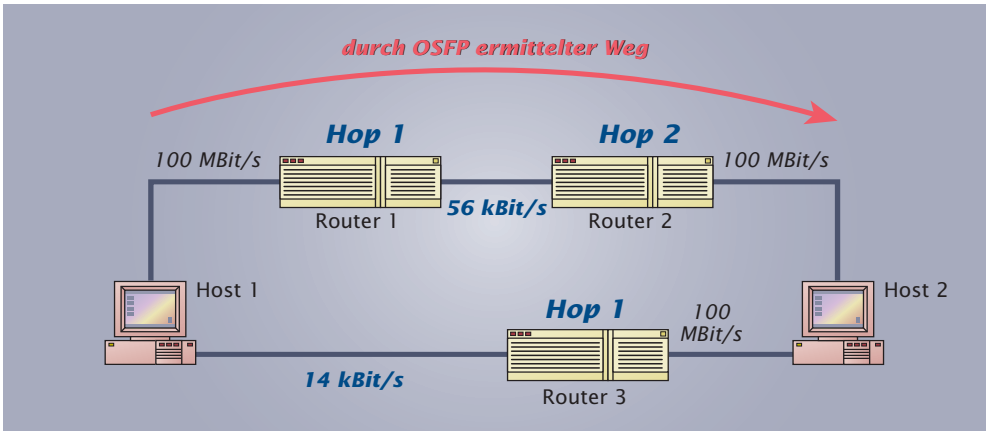


11.3.2-2
Funktionsweise von RIP

OSPF-Protokoll

Das OSPF-Protokoll (Open Shortest Path First[1]) basiert auf dem Link-State-Algorithmus. Router, die nach diesem Verfahren arbeiten, senden an ihre Nachbarn Angebote aus, die den Namen und eine Kenngröße für die Verbindungskosten enthalten. Diese Angebote werden als Link-State-Advertise (LSA) bezeichnet. Jedes LSA wird wiederum vom empfangenden Router an alle benachbarten Router weitergeleitet. So erhält jeder Router eine Übersicht über die Struktur des Netzes und über die einzelnen Verbindungskosten. Auf dieser Basis kann er dann die optimale Verbindung für die Übertragung einer Nachricht berechnen. OSPF ist deshalb besonders für den Einsatz innerhalb von Autonomen Systemen geeignet, da immer die Topologieinformationen vorhanden sind. OSPF-organisierte Netze sind in Bereiche (Areas) aufgeteilt. Alle Router einer Area haben die gleichen Topologieinformationen gespeichert. Über spezielle Router (Area Border Router) werden die einzelnen Areas miteinander in einer Art Backbone verbunden. Besteht ein OSPF-Netz nur aus einer Area, ist diese zugleich auch als Backbone zu betrachten. Der Verbund von Areas ist ein Autonomes System, das mit anderen Autonomen Systemen über „AS Boundary Router“ unter Verwendung eines Exterior Gateway Protocols eine Verbindung organisiert.

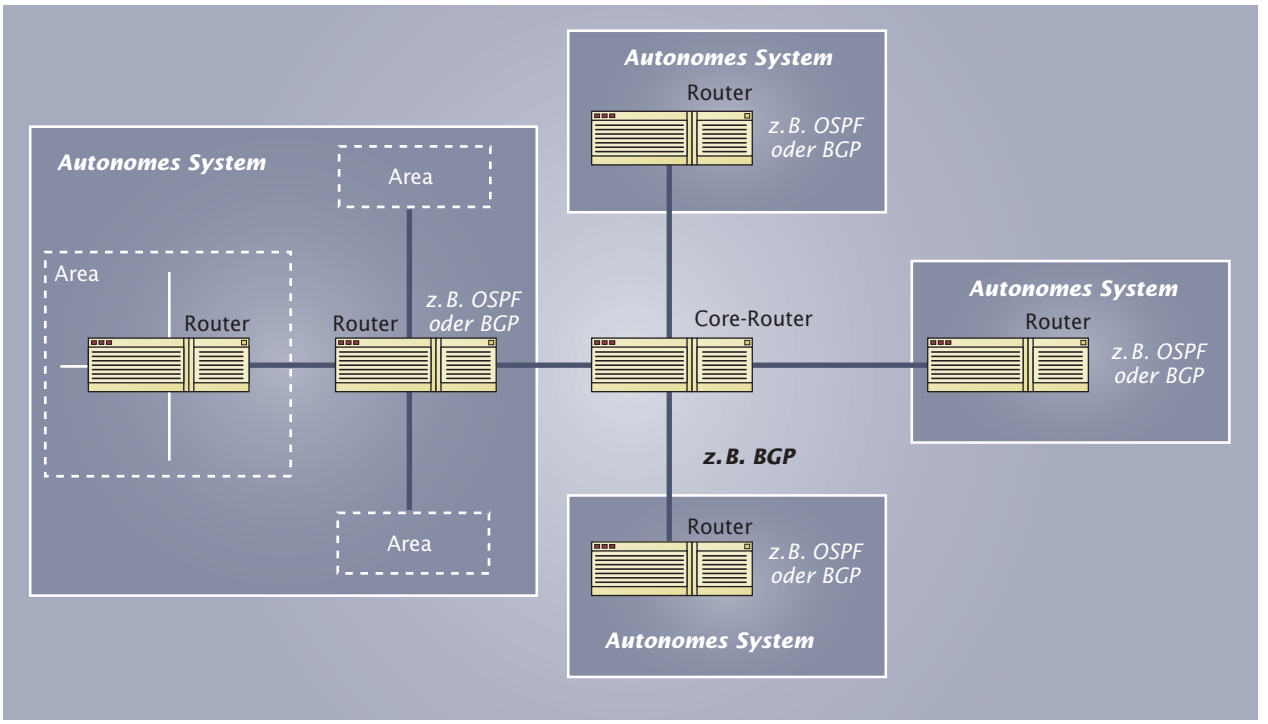
[1] **OSPF: O**pen **S**hortest **P**ath **F**irst, engl. „öffne den kürzesten Pfad zuerst“



11.3.2-3 Funktionsweise von OSPF

Border Gateway Protocol

Das Border Gateway Protocol (BGP) gehört zu den Exterior Gateway Protokollen. Es beschreibt, wie Router untereinander die Verfügbarkeit von Verbindungswegen zwischen zwei Netzen austauschen. Somit stellt es die Verbindung zwischen Autonomen Systemen her. BGP kann mit OSPF zusammenarbeiten. Dazu werden periodisch die benachbarten Router kontaktiert und es wird überprüft, ob sie noch vorhanden sind. Die übermittelten Entfernungen beziehen sich dabei stets auf das sendende System. Bei einem ersten Kontakt werden jeweils die kompletten Routing-Tabellen übertragen. Die folgenden Kommunikationen zwischen den Routern werden lediglich für die Aktualisierung der Tabellen genutzt. Für diese Update-Nachrichten wird TCP verwendet, was eine sichere Übertragung dieser Informationen garantiert. Der unberechtigte Zugriff auf einen Router wird durch eine Authentisierung vermieden. BGP-Router speichern alle möglichen Wege zu angeschlossenen Netzen in ihren Routingtabellen. Für die Übertragung von Update-Nachrichten werden jedoch nur die besten Wege genutzt.



11.3.2-4 Dynamisches Routen zwischen Autonomen Systemen

1. Recherchieren Sie weitere Routing-Protokolle z. B. im Poster des Anhangs.
2. Informieren Sie sich darüber, welche Routingprotokolle im Internetverkehr genutzt werden.

11.3.3 Zusätzliche Routerfunktionen

In der Firma Lütgens soll ein Router die Verbindung zu mehreren Internet-Providern herstellen. Neben den reinen Routingfunktionen, wie sie bisher dargestellt wurden, werben die Router-Anbieter mit weiteren Funktionen.

Router für WAN-Verbindungen bieten häufig über die Routerfunktionen hinaus weitere Funktionen an, wie die Sicherstellung und effiziente Nutzung von Weitverkehrsverbindungen wie zum Beispiel Wählverbindungen. Darüber hinaus werden oft auch Sicherheitsdienste wie die Einrichtung einer Firewall angeboten (siehe Kapitel 14: „Sicherheit in Netzwerken“ und Exkurs „Konfiguration einer Firewall“). Folgende Funktionen können insbesondere von Bedeutung sein:

Dial on Demand[1]
Gibt es zwischen den Kommunikationsendgeräten keine Nachrichtenübertragung, so wird nur eine logische Verbindung gehalten. Es fallen dann keine Leitungskosten an. Bei erneutem Kommunikationsbedarf wird die physikalische Verbindung wieder hergestellt.

Bandwidth on Demand[2]
Der Router schaltet je nach Bandbreitenbedarf weitere WAN-Verbindungswege hinzu bzw. ab.

Dial Backup[3]
Fällt eine Kommunikationsverbindung aus, so schaltet der Router automatisch eine Ersatzverbindung.

Kanalbündelung
Bei ISDN-Leitungen ist der Router in der Lage, automatisch mehrere ISDN-Kanäle zu bündeln, um einen logischen Kanal mit höherer Bandbreite zur Verfügung zu stellen.

Load Balancing[4]
Bei hohem Lastaufkommen kann der Router die Kommunikationen auf mehrere Leitungen verteilen.

Spoofing[5]
Einem Host wird bei unterbrochener Wählverbindung vom Router vorgetäuscht, dass diese Verbindung immer noch aktiv ist. Dies ist sinnvoll, wenn eine Wählverbindung unterbrochen wurde um Kosten zu reduzieren, der Host aber periodisch abprüft, ob diese Verbindung existiert.

Analysieren Sie die Funktionen, die ein DSL-Router für die gemeinsame Nutzung eines DSL-Anschlusses durch mehrere Teilnehmer zur Verfügung stellt.

[1] **Dial on Demand:** engl. Wählen bei Bedarf
[3] **Bandwidth on Demand:** engl. Bandbreite nach Bedarf
[3] **Dial Backup:** engl. Wählen einer Alternative bei Ausfall
[4] **Load Balancing:** engl. Lastverteilung
[5] **Spoof:** engl. Humbug, Schwindel

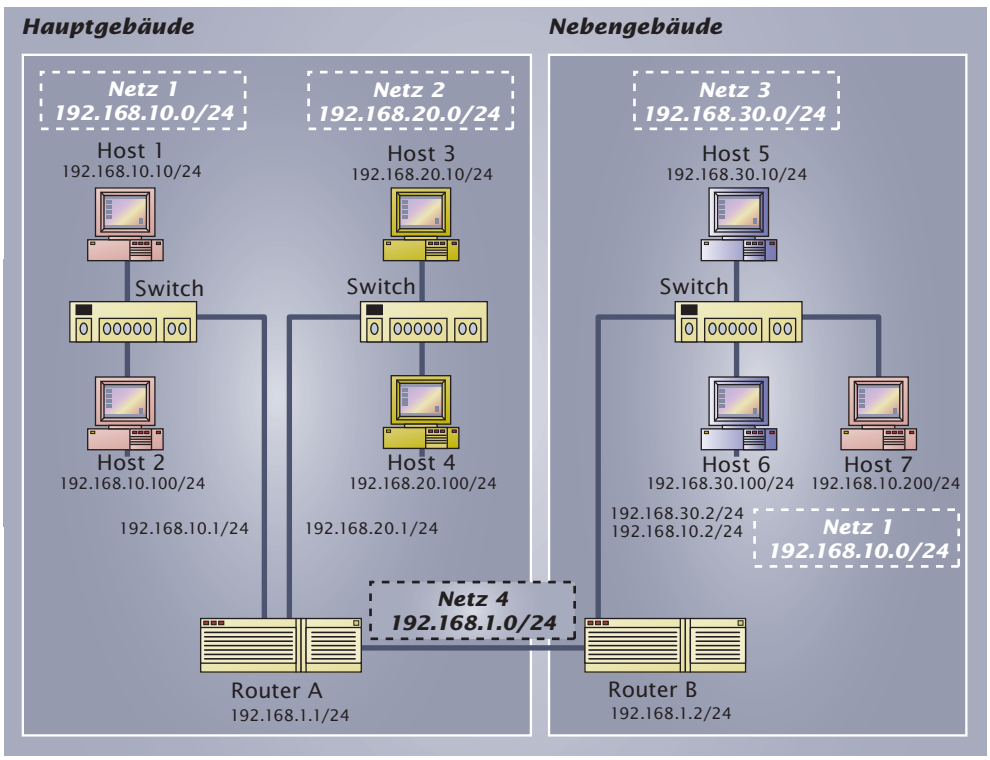
1. Problemstellung

Für das Verständnis des Routings soll an einem Beispiel die Bildung von statischen Routen in einem Netzwerk vertieft werden. Basis dafür ist das Grundwissen aus dem Kapitel 11: Routing.

Insgesamt werden drei Subnetze miteinander verbunden (siehe Grafik 1). Im Gebäude A befinden sich zwei Netze (Netz 1 und Netz 2). Sie sind durch den Router A miteinander verbunden. Dieser Router stellt über eine Standleitung auch die Verbindung zum Gebäude B her (Netz 4). Dort organisiert der Router B die Netzwerkverbindungen. An Router B befinden sich die Systeme des Netzes 3. Grundsätzlich ist nur der Zugriff der Clients auf die Server von Bedeutung. Für Administrationszwecke können nur Clients des Netzes 2 genutzt werden. Als Besonderheit ist ein Client-System (Host 7) zu betrachten, welches zwar physikalisch an den Switch des Netzes 3 angeschlossen ist, aber nur auf den Server (Host 1) des Netzes 1 zugreifen darf.

Folgende organisatorischen Rahmenbedingungen wurden für die Vergabe von IP-Adressen festgelegt:

- Die Netzadressen werden im Adressraum 192.168.XX.0 vergeben (192.168.10.0 bis 192.168.30.0, also „zweistellig“).
- Die Netzadresse des verbindenden Backbone-Netzes hat die IP-Adresse 192.168.1.0 (also „einstellig“).
- Die Server der Netze sind „zweistellig“ zu adressieren (z. B. 192.168.10.10 bis 192.168.10.99).
- Die Clients der Netze sind „dreistellig“ zu adressieren (z. B. 192.168.10.100 bis 192.168.10.254).

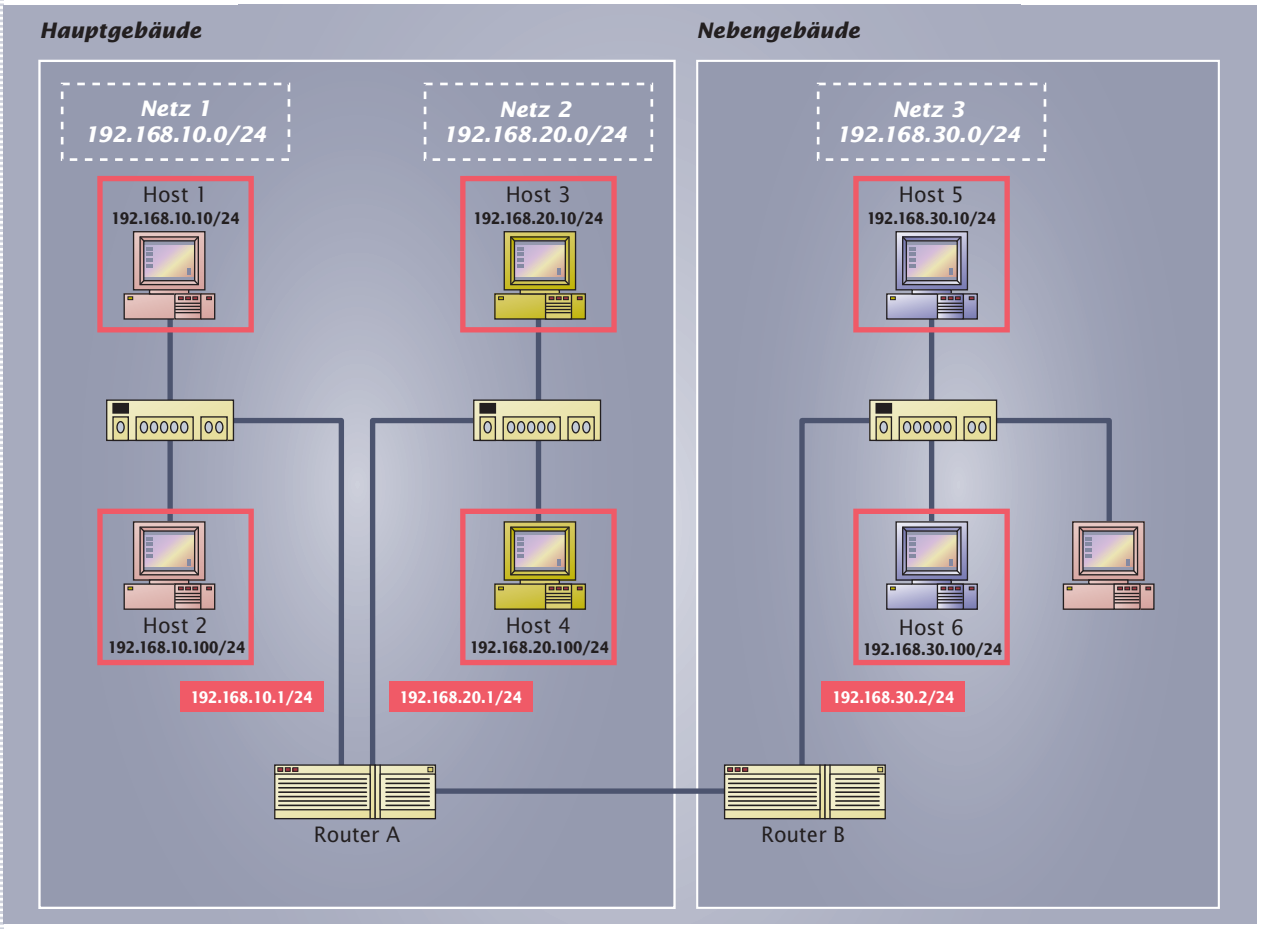


1 Gesamtnetzplan

Für die Organisation der Kommunikation sind für alle im Netzwerk befindlichen Systeme die entsprechenden Routingtabellen zu entwickeln.

2. Erster Ansatz

Für eine strukturierte Vorgehensweise ist es sinnvoll, die einzelnen Routingtabellen jeweils aus der Position des einzelnen Hosts zu betrachten. Dies entspricht auch der Vorgehensweise in der Praxis, da überwiegend Geräte zu Systemen hinzugefügt werden. Oder mit anderen Worten: für den Zugang zum Intranet/Internet interessiert nicht die Kenntnis des Gesamtsystems sondern nur der Zugang zum nächsten Übertragungssystem (Router). Ausgenommen aus den Betrachtungen ist das gesondert zu behandelnde System im Nebengebäude (Host 7). Diese Verbindung wird erst zum Abschluss betrachtet.



2 Konfiguration der Hosts

Für die einzelnen Hosts (Client und Server) sind in den Betriebssystemen folgende Informationen einzutragen:

- IP-Adresse
- Subnetzmaske
- Standardroute

Der Begriff Standardroute bezeichnet eine Adresse, an die alle im Netz nicht adressierbaren Pakete weitergeleitet werden. Dieser Begriff wird leider von den Betriebssystemherstellern nicht konsequent angewendet, sondern man findet auch die

Bezeichnungen Default (-Route, -Gateway) und Gateway. Aus der Sicht eines Host bedeutet dies, dass die eigene Hostadresse und die dazugehörige Subnetzmaske eingetragen werden müssen. Über diese Kombination ist automatisch die Netzadresse festgelegt. Für alle nicht im Subnetz bekannten IP-Adressen soll ein System (Router) die Anforderungen weiterleiten.

Für die einzelnen Hosts ergeben sich deshalb folgende Einstellungen:

Host Nr.	IP-Adresse	Subnetzmaske	Standardroute
Host 1	192.168.10.10	255.255.255.0	192.168.10.1
Host 2	192.168.10.100	255.255.255.0	192.168.10.1
Host 3	192.168.20.10	255.255.255.0	192.168.20.1
Host 4	192.168.20.100	255.255.255.0	192.168.20.1
Host 5	192.168.30.10	255.255.255.0	192.168.30.2
Host 6	192.168.30.100	255.255.255.0	192.168.30.2

Das Betriebssystem erzeugt aus diesen Einträgen eine Routingtabelle. Dabei werden auch Standardeinträge erzeugt, die für die korrekte Kommunikation notwendig sind, wie z. B. die Loopback-Adresse der Netzwerkkarte. Die Standardeinträge wurden im Kapitel 11 „Routing“ erläutert. Zu beachten ist der Server Host 1, der für die besonderen Anforderungen des Host-Routing nachkonfiguriert werden muss. Host 7 ist bezüglich der Standardroute besonders zu konfigurieren.

Der tatsächliche Aufbau der Routingtabelle kann zum Beispiel in Windows durch den Aufruf von „`route print`“ angezeigt werden. Für den Host 3 ergibt sich folgende Routingtabelle:

Verwendung	Netzwerkadresse	Subnetzmaske	Gateway-Adresse	Schnittstelle	Anzahl
Default Route	0.0.0.0	0.0.0.0	192.168.20.1	192.168.20.10	1
Loopback Network	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
Directly attached Network	192.168.20.0	255.255.255.0	192.168.20.10	192.168.20.10	1
Local Host	192.168.20.10	255.255.255.255	127.0.0.1	127.0.0.1	1
Network Broadcast	192.168.20.255	255.255.255.255	192.168.20.10	192.168.20.10	1
Multicast Address	224.0.0.0	224.0.0.0	192.168.20.10	192.168.20.10	1
Limited Broadcast	255.255.255.255	255.255.255.255	192.168.20.10	192.168.20.10	1

Im jetzt erreichten Zustand sollten alle Hosts in ihren Subnetzen miteinander kommunizieren können. Das betrifft evtl. auch die im jeweilige Subnetz beheimatete Seite des angeschlossenen Routers. Eine Kommunikation über die Router hinaus ist nicht möglich, da diese noch nicht konfiguriert sind. Zu überprüfen ist dieser Zustand durch den Aufruf des „`ping`"-Befehls (siehe Kapitel 9: Netzwerkprotokolle). Mit Hilfe dieses Befehls wird der erfolgreiche Aufbau eines TCP/IP-Protokollstapels überprüft. Auf die Kommunikationsaufforderung hin quittiert die Gegenstelle diese Anforderung mit einer Rückmeldung. Als erstes sollte die eigene IP-Adresse angesprochen werden, um zu überprüfen, ob der eigene Rechner kommunikationsfähig ist (siehe Loopback).

Folgendermaßen könnte eine erfolgreiche Überprüfung der Kommunikation zwischen Host 1 und Router A aus der Sicht des Host 1 aussehen:

```
C:\ping 192.168.10.1
Ping wird ausgeführt für 192.168.10.1 mit 32 Bytes Daten:

Antwort von 192.168.10.1: Bytes=32 Zeit=5ms TTL=128
Antwort von 192.168.10.1: Bytes=32 Zeit=2ms TTL=128
Antwort von 192.168.10.1: Bytes=32 Zeit=2ms TTL=128
Antwort von 192.168.10.1: Bytes=32 Zeit=2ms TTL=128

Ping-Statistik für 192.168.10.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0 % Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 2, Maximum = 5, Mittelwert = 2
```

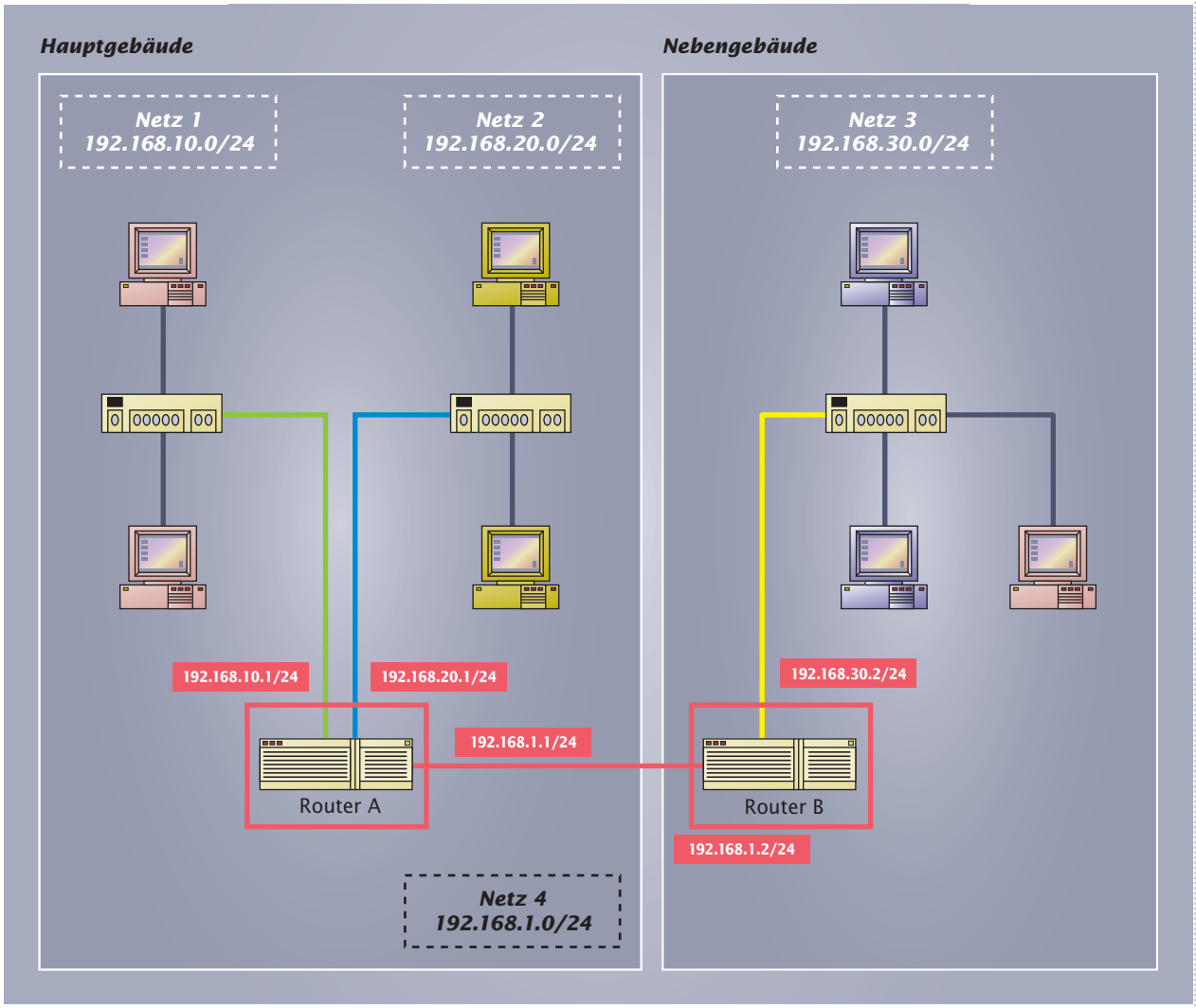
Im Fehlerfall kann z. B. folgendes Ergebnis für einen nicht angeschlossenen Rechner gemeldet werden:

```
C:\ping 192.168.10.1
Ping wird ausgeführt für 192.168.10.1 mit 32 Bytes Daten:

Zeitüberschreitung der Anforderung
Zeitüberschreitung der Anforderung
Zeitüberschreitung der Anforderung
Zeitüberschreitung der Anforderung

Ping-Statistik für 192.168.10.1:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
    (100 % Verlust)
```

Die IP-Konfiguration eines Systems kann z. B. mit dem Windows-Befehl „`ipconfig`" (LINUX: `ifconfig`) überprüft werden (siehe Kapitel 9: Netzwerkprotokolle). Es werden dann die Adresskonfigurationen aller im Hostsystem befindlichen und aktiven Netzadapter angezeigt.

3. Zweiter Ansatz

Im zweiten Durchlauf können die Routingtabellen aus der Position der beiden Router entwickelt werden. Auch jetzt noch soll die besondere Situation des Hosts 7 unberücksichtigt bleiben.



3 Konfiguration der Router

Für die Konfiguration der Router sind folgende Einträge zu berücksichtigen:

- IP-Adressen der Netzwerkschnittstellen
- IP-Adressen der angeschlossenen Netze
- IP-Adressen angeschlossener Router
- Standardrouten

Auch bei den Routern werden einige Standardeinträge wie Standardrouten und Loopback-Adressen erzeugt bzw. müssen eingegeben werden. Außerdem ist möglicherweise zu beachten, dass in einigen Betriebssystemen die Funktion „IP-Forwarding“ aktiviert ist.

Für die Router ergeben sich folgende Routingtabellen (Beispiel Windows):

Ausschnitt aus der Routingtabelle des Routers A. Gekennzeichnet sind die Festlegungen für die Netze 1,2 und 4 sowie die Route in das Netz 3.

Netzwerkziel	Subnetzmaske	Gateway	Schnittstelle	Anzahl
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.1	192.168.1.1	1
192.168.1.1	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.1.255	255.255.255.255	192.168.1.1	192.168.1.1	1
192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.1	1
192.168.10.1	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.10.255	255.255.255.255	192.168.10.1	192.168.10.1	1
192.168.20.0	255.255.255.0	192.168.20.1	192.168.20.1	1
192.168.20.1	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.20.255	255.255.255.255	192.168.20.1	192.168.20.1	1
192.168.30.0	255.255.255.0	192.168.1.2	192.168.1.1	1
224.0.0.0	224.0.0.0	192.168.1.1	192.168.1.1	1
224.0.0.0	224.0.0.0	192.168.10.1	192.168.10.1	1
224.0.0.0	224.0.0.0	192.168.20.1	192.168.20.1	1

Ausschnitt aus der Routingtabelle des Routers B. Gekennzeichnet sind die Festlegungen für die Netze 3 und 4 sowie die Route in die Netze 1 und 2.

Netzwerkziel	Subnetzmaske	Gateway	Schnittstelle	Anzahl
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.2	192.168.1.2	1
192.168.1.2	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.1.255	255.255.255.255	192.168.1.2	192.168.1.2	1
192.168.10.0	255.255.255.0	192.168.1.1	192.168.1.2	1
192.168.20.0	255.255.255.0	192.168.1.1	192.168.1.2	1
192.168.30.0	255.255.255.0	192.168.30.2	192.168.30.2	1
192.168.30.2	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.30.255	255.255.255.255	192.168.30.2	192.168.30.2	1
224.0.0.0	224.0.0.0	192.168.1.2	192.168.1.2	1
224.0.0.0	224.0.0.0	192.168.30.2	192.168.30.2	1
255.255.255.255	255.255.255.255	192.168.30.2	192.168.30.2	1

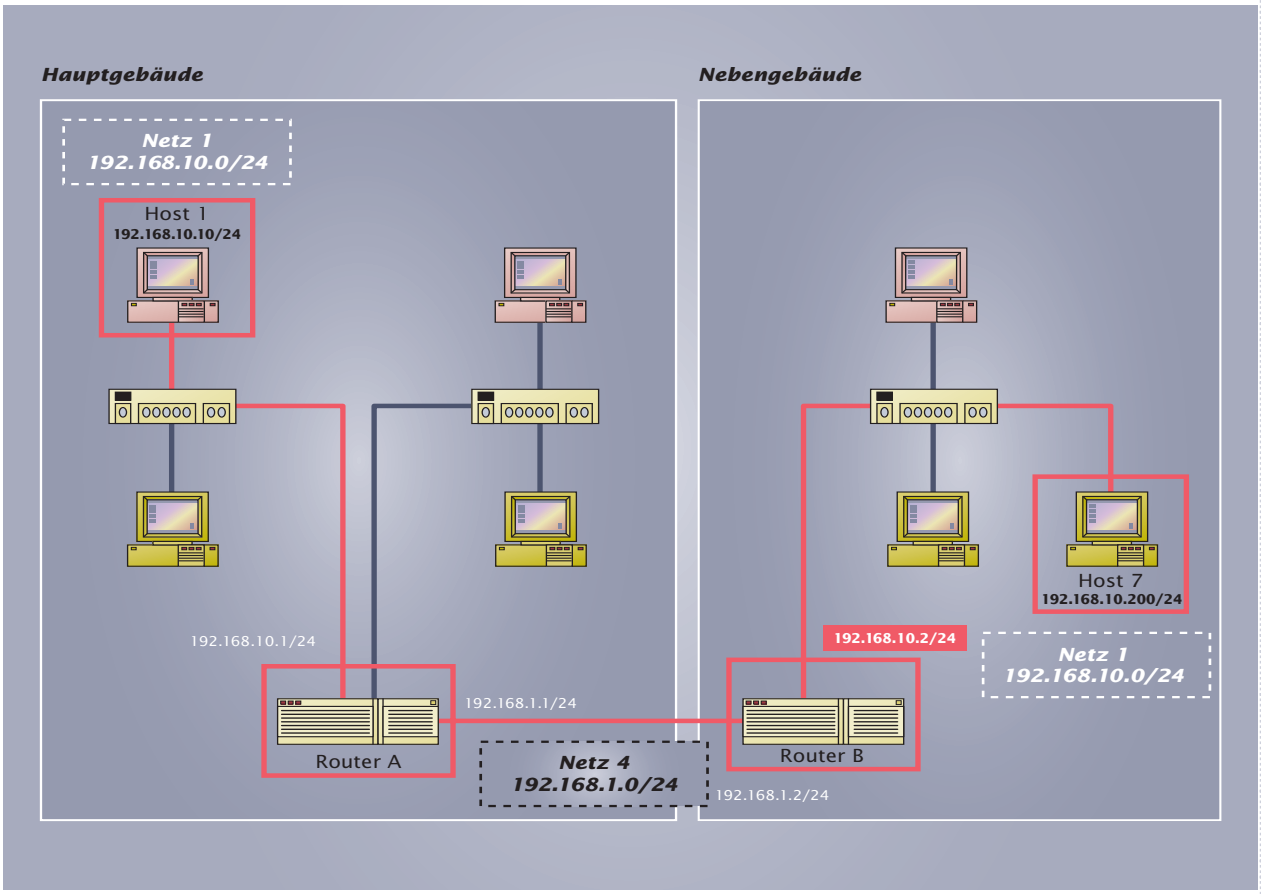
Auffällig ist, dass auf den Routern keine Default-Routen eingetragen wurden. Diese sind auch nicht notwendig, da keine weiteren Verbindungen mit „unbekannten“ Netzadressen wie zum Beispiel Internetverbindungen vorgesehen sind.

1. Analysieren Sie alle Einträge der Routingtabellen der Router. Beschreiben Sie in kurzen Sätzen die jeweiligen Aufgaben der Einträge.
2. Vergleichen Sie die Routingtabellen der Router. Erläutern Sie Gemeinsamkeiten und Unterschiede.
3. Überprüfen Sie die Routingfunktionen auf dem aktuellen Stand der Router- und Hostkonfigurationen. Nutzen Sie dazu in der Kommandozeileneingabe den „`ping`“-Befehl und den „`tracert`“-Befehl (Windows).

4. Konfiguration des Host-Routings

Im letzten Durchlauf soll der Zugriff des Hosts 7 auf den Host 1 (Server) organisiert werden. Zu beachten ist, dass der Host 7 nicht auf andere Server und Hosts als auf den fest zugewiesenen Partner zugreifen darf. Dies vereinfacht zusätzlich die Entwicklung der Routingtabellen, da dann nur folgende beteiligte Systeme konfiguriert werden müssen:

- Router A
- Router B
- Host 1
- Host 7



4 Konfiguration des Host-Routings

Für den Router A ist die Route zum Host 7 über den Router B der Routingtabelle hinzuzufügen.

Ergänzung der Routingtabelle des Routers A:

Netzwerkziel	Subnetzmaske	Gateway	Schnittstelle	Anzahl
…	…	…	…	…
…	…	…	…	…
192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.1	1
192.168.10.1	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.10.200	255.255.255.255	192.168.1.2	192.168.1.1	1
192.168.10.255	255.255.255.255	192.168.10.1	192.168.10.1	1
…	…	…	…	…
…	…	…	…	…

Für Router B gilt Ähnliches. Zusätzlich zu dem Eintrag des Netzes 192.168.10.0 sind die Einträge für die spezielle Verbindung zwischen der (neuen) Schnittstelle 192.168.10.2 und dem Host 1 inklusive der Broadcast-Nachrichten zu berücksichtigen. Dies bedeutet auch, dass dem Netzwerkadapter auf der Seite zum Netz 3 zwei IP-Adressen zugewiesen wurden.

Ergänzung der Routingtabelle des Routers B:

Netzwerkziel	Subnetzmaske	Gateway	Schnittstelle	Anzahl
…	…	…	…	…
…	…	…	…	…
192.168.1.255	255.255.255.255	192.168.1.2	192.168.1.2	1
192.168.10.0	255.255.255.0	192.168.10.2	192.168.30.2	1
192.168.10.2	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.10.10	255.255.255.255	192.168.1.1	192.168.1.2	1
192.168.10.255	255.255.255.255	192.168.10.2	192.168.30.2	1
192.168.20.0	255.255.255.0	192.168.1.1	192.168.1.2	1
…	…	…	…	…
…	…	…	…	…

Untersuchen Sie die zusätzlichen Einstellungen. Vergleichen Sie dazu die Routingtabellen mit den vorherigen Tabellen (s. o.)
Überprüfen Sie mit dem „`ipconfig`“ (Windows) die Zuordnung der IP-Adressen zu den Netzwerkkarten der Router.

Der Host 7 erhält die folgende Routingtabelle. Zu beachten ist, dass keine Default-Route eingetragen ist. Ein Eintrag z. B. der Routerschnittstelle 192.168.30.2 wäre nicht zulässig, da sonst eine Kommunikation mit einem anderen Netz möglich wäre. Gekennzeichnet ist die Route zum Host 1 über den Router B.

Ausschnitt aus der Routingtabelle des Hosts 7:

Netzwerkziel	Subnetzmaske	Gateway	Schnittstelle	Anzahl
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.1	255.255.255.255	192.168.10.2	192.168.10.200	1
192.168.10.0	255.255.255.0	192.168.10.200	192.168.10.200	1
192.168.10.10	255.255.255.255	192.168.10.2	192.168.10.200	1
192.168.10.200	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.10.255	255.255.255.255	192.168.10.200	192.168.10.200	1
224.0.0.0	224.0.0.0	192.168.10.200	192.168.10.200	1
255.255.255.255	255.255.255.255	192.168.10.200	192.168.10.200	1

Als letztes Gerät wird der Host 1 konfiguriert. Hier ist die Festlegung der Route zum Host 7 über den Router A von Bedeutung.

Ausschnitt aus der Routingtabelle des Hosts 1:

Netzwerkziel	Subnetzmaske	Gateway-Adresse	Schnittstelle	Anzahl
0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.10.0	255.255.255.0	192.168.10.10	192.168.10.10	1
192.168.10.10	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.10.200	255.255.255.255	192.168.10.1	192.168.10.10	1
192.168.10.255	255.255.255.255	192.168.10.10	192.168.10.10	1
224.0.0.0	224.0.0.0	192.168.10.10	192.168.10.10	1
255.255.255.255	255.255.255.255	192.168.10.10	192.168.10.10	1

5. Überprüfung des Routings

Nachdem alle Systeme konfiguriert worden sind, müssen alle Kommunikationswege überprüft werden. Dies geschieht zum Beispiel durch die Verwendung des „`ping`“-Befehls. Auf diese Weise sollten dann alle Rechner im Gesamtsystem unter den vorgegebenen Rahmenbedingungen erreichbar sein. Der tatsächliche Verlauf der Routen von einem Host zu einem Ziel kann jetzt mit dem Windows-Aufruf „`tracert Zieladresse`“ (LINUX: „`traceroute Zieladresse`“) überprüft werden. Sinnvollerweise sind auch die Wege zu prüfen, die eigentlich nicht zur Verfügung stehen sollen (Beispiel: Zugriff von Host 7 auf einen Host des Netzes 3).

1. Erstellen Sie für jeden Host eine Tabelle, in der aufgeführt ist, auf welche Hosts dieses System per „`ping`“ zugreifen kann und von welchen Hosts auf das System zugegriffen werden kann.
2. Vergleichen Sie Ihre Ergebnisse mit der vorgegebenen Aufgabenstellung.
3. Ermitteln Sie die komplette Route von Ihrem Arbeitsplatzrechner zu einem Server im Netzwerk Ihres Betriebs/Ihrer Schule. Interpretieren Sie alle angezeigten Informationen.