In der nachfolgenden Tabelle sind die verschiedenen Klasseneinteilungen und die damit verbundene Adresszuordnung zusammengefasst:

Klasse	Klassen-Bits	Anzahl Netze	Anzahl Hosts pro Netz
A	0	126	16.777.214 (2563-2)
B	10	16.384 (64 × 2561)	65.534 (2562-2)
C	110	2.097.152 (32 × 2562)	254 (2561-2)
D	1110	–	–
E	1111	–	–

3.2 Subnetzadressierung

Die Klassifizierung der IP-Adressen gemäß dem im letzten Abschnitt beschriebenen System in Klasse-A-, Klasse-B- und Klasse-C-Adressen (die Sonderklassen D und E bleiben unberücksichtigt, da sie nicht praktisch nutzbar sind) ist relativ starr und unflexibel. Betrachtet man die Entwicklung der öffentlichen Adressvergabe und Registrierung innerhalb der letzten Jahrzehnte, so ist es mittlerweile nahezu unmöglich, eine der überaus attraktiven (öffentlichen) Klasse-A-Adressen zu erhalten; selbst B-Adressen sind nur noch sehr schwer zu bekommen.

Adressen der Klasse C besitzen grundsätzlich einen stark eingeschränkten Adressraum (maximal 254 adressierbare Hosts pro Adresse), sodass man bei der Einrichtung umfangreicher IP-Netzwerke leicht an seine Grenzen stößt. Darüber hinaus scheint sich das Routing innerhalb des öffentlichen Internets zu einem Problem zu verdichten, da der Umfang der Adressinformationen (*Routing-Tabellen*) ein derartiges Ausmaß angenommen hat, dass er von der gegenwärtig verfügbaren Soft- und Hardware nur noch schwer zu verwalten ist. Es ist ferner zu erwarten, dass der zurzeit verfügbare Adressraum von 32 Bits innerhalb der nächsten Zeit sicher nicht mehr ausreichen wird, um den Bedarf an registrierten IP-Adressen zu befriedigen.

HINWEIS

Die Probleme bei der Adressvergabe unter IP, Version 4, und mögliche Lösungsansätze sind unter anderem im RFC 1519 vom September 1993 beschrieben: *Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy.*

Eine mögliche Lösung der Adressproblematik von IP, Version 4, liegt in der Bildung von Subnetzen, die das statische Klassenkonzept durchbrechen. Danach ist es möglich, innerhalb einer verfügbaren Klassenadresse alter Konvention weitere Subnetze zu definieren und die Anzahl adressierbarer Hosts auf die Subnetze aufzuteilen. Dazu passt der RFC 1817 vom August 1995, der die CIDR-Betrachtungen um die Fähigkeiten relevanter Routing-Protokolle erweitert, indem festgehal-

ten wird, dass Protokolle wie RIP, BGP-3, EGP und IGRP nicht für das CIDR-Konzept geeignet sind. Neuere Protokolle, wie OSPF, RIP II, Integrated IS-IS und Enhanced IGRP, lassen sich allerdings verwenden.

HINWEIS

Weitergehende Informationen zum Thema *Routing* und den Funktionen und Möglichkeiten der verschiedenen Routing-Protokolle enthält Kapitel 4.

Der RFC 4632 vom August 2006 liefert wichtige Informationen zum praktischen Einsatz des CIDR-Konzepts (siehe auch hierzu Aktivitäten der ROAD Workgroup in Abschnitt 3.4.2.2).

3.2.1 Prinzip

Angenommen, ein Unternehmen mittlerer Größe hat zwecks Aufbau eines IP-Netzwerks beim DENIC (*Deutsches Network Information Center*) eine öffentliche Adresse beantragt. Folgende Klasse-B-Adresse wird zugewiesen: 190.136.0.0. Mit dieser Adresse lassen sich bekanntlich 65.536 Hosts adressieren – eine Zahl, die nicht unbedingt dem Bedarfsprofil eines größeren Unternehmens entspricht, das durch den Einsatz von Routern das eigene Netzwerk strukturieren möchte. Für jeden Router muss ein expliziter Netzübergang definiert werden, d.h., der Router umfasst, sofern er lediglich zwei Netzwerke miteinander verbindet, zwei IP-Adressen mit zwei unterschiedlichen Netz-IDs. Da in diesem Beispiel lediglich ein einziges logisches Klasse-B-Netzwerk verfügbar ist, muss das gewünschte Ziel dadurch erreicht werden, dass überall dort, wo Router eingesetzt werden sollen, Subnetze gebildet werden.

3.2.2 Typen und Design der Subnetzmaske

Das zur Bildung von Subnetzen erforderliche Instrumentarium ist die *Subnetwork Mask* (Subnetzmaske). Sie stellt, ebenso wie die IP-Adresse, eine Folge von 32 Bits dar, die in der Regel gemeinsam mit der IP-Adresse auf den einzelnen Systemen (Router, Hosts usw.) konfiguriert wird. Ihre Schreibweise ist der IP-Adresse angepasst: *dotted decimal*. Die Funktionsweise einer Subnetzmaske ist allerdings wesentlich besser nachvollziehbar, wenn man ihren Binärcode betrachtet. Die zu vier Oktetten zusammengefasste »Maske« codiert nämlich überall dort, wo die IP-Adresse als Netz-ID interpretiert werden soll, eine binäre 1. Der restliche Teil der *Subnetwork Mask* bleibt für die Host-ID übrig, also genau die Stellen, wo binäre Nullen codiert sind.

Für den Fall, dass lediglich mit der registrierten IP-Adresse, also ohne »Subnetting«, gearbeitet wird, gilt eine *Default Subnetwork Mask*, denn der IP-Prozess eines Systems berücksichtigt auch dann eine Subnetzmaske, wenn keine eigene Maske definiert wurde. Sie entspricht dann der jeweiligen Klasse, so wie nachfolgend dargestellt:

Klasse	dotted decimal	binary
A	255.0.0.0	11111111 00000000 00000000 00000000
B	255.255.0.0	11111111 11111111 00000000 00000000
C	255.255.255.0	11111111 11111111 11111111 00000000

Soll jedoch eine individuelle Subnetzmaske verwendet werden, so erfolgt die Verteilung der 1er-Maske nicht mehr Byte-, sondern Bit-orientiert:

B	255.255.192.0	**11111111 11111111 11**000000 00000000

Zurück zum Beispiel: Die bei der Klasse-B-Adresse theoretisch verfügbaren 65.536 Hosts sollen auf verschiedene Subnetze aufgeteilt werden. Aufgrund von Überlegungen zur Infrastruktur des gewünschten Netzwerks wird die Entscheidung getroffen, mindestens fünf Subnetze zu bilden (siehe Abb. 3–5).

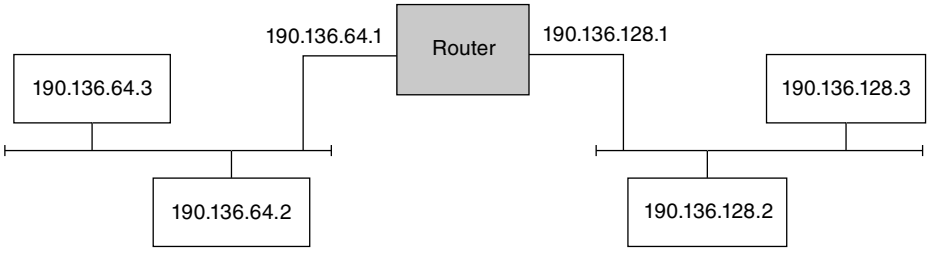

Abb. 3–5 *Aufbau und Struktur des gewünschten Netzwerks*

In diesem Fall bedeutet dies, dass vom dritten Byte der Subnetzmaske die ersten beiden Bits für die Netz-ID verwendet werden sollen; daraus ergibt sich eine Anzahl von maximal vier Subnetzen. Die restlichen sechs Bits des dritten Bytes und das vollständige vierte Byte führen zu einer Anzahl von maximal 16.384 adressierbaren Hosts pro Subnetz (64 x 256; 64 aus dem dritten und 256 aus dem vierten Oktett). Die geplante Subnetwork Mask ergibt daher folgende Teilnetze:

Netz-ID	Host-ID
190.136.0.0	10111110 10001000 **00**000000 00000000
190.136.64.0	10111110 10001000 **01**000000 00000000
190.136.128.0	10111110 10001000 **10**000000 00000000
190.136.192.0	10111110 10001000 **11**000000 00000000

Da die Mindestanzahl von fünf definierbaren Subnetzen nicht erreicht werden kann, muss der Plan, eine Subnetzbildung mit den ersten beiden Bits des dritten

Bytes der Subnetzmaske durchzuführen, verworfen werden. Als Ausweg bleibt die Hinzunahme eines weiteren Bits in der Subnetzmaske (im dritten Byte), um mindestens fünf Subnetze erzeugen zu können. Daraus wiederum ergibt sich die folgende Aufteilung:

Netz-ID	**Host-ID**
Subnetwork Mask:	**11111111 11111111 111**00000 00000000
Subnetz	
190.136.0.0	10111110 10001000 **000**00000 00000000
190.136.32.0	10111110 10001000 **001**00000 00000000
190.136.64.0	10111110 10001000 **010**00000 00000000
190.136.96.0	10111110 10001000 **011**00000 00000000
190.136.128.0	10111110 10001000 **100**00000 00000000
190.136.160.0	10111110 10001000 **101**00000 00000000
190.136.192.0	10111110 10001000 **110**00000 00000000
190.136.224.0	10111110 10001000 **111**00000 00000000

Aus dieser Aufstellung geht hervor, dass die angestrebten fünf Subnetze gebildet werden können (maximal acht Subnetze). In jedem Subnetz müssen zwei Adressen gestrichen werden, wobei es sich dabei theoretisch jeweils um die erste (z.B. 190.136.96.0) und die letzte Adresse eines Subnetzes (z.B. 190.136.127.255) handelt. Dies ist notwendig, da der Wert »0« das jeweilige Subnetz bezeichnet und »255« die lokale Broadcast-Adresse repräsentiert, also beide für eine Adressierung nicht zur Verfügung stehen.

Unter diesen Voraussetzungen können als Ergebnis für die weitere Planung der Subnetzstruktur folgende Bereiche verwendet werden:

Nr.	**Netz-ID**	**erster Host**	**letzter Host**	**Local Broadcast**
1	190.136.0.0	190.136.0.1	190.136.31.254	190.136.31.255
2	190.136.32.0	190.136.32.1	190.136.63.254	190.136.63.255
3	190.136.64.0	190.136.64.1	190.136.95.254	190.136.95.255
4	190.136.96.0	190.136.96.1	190.136.127.254	190.136.127.255
5	190.136.128.0	190.136.128.1	190.136.159.254	190.136.159.255
6	190.136.160.0	190.136.160.1	190.136.191.254	190.136.191.255
7	190.136.192.0	190.136.192.1	190.136.223.254	190.136.223.255
8	190.136.224.0	190.136.224.1	190.136.255.254	190.136.255.255

Jedes der acht Subnetze kann somit 8.190 Hosts adressieren (8.192, um die Netz-ID und den lokalen Broadcast reduziert). Die Wahl einer anderen Subnetzmaske könnte eine völlig andere Aufteilung ergeben. Wird beispielsweise nicht die Subnetzmaske 255.255.192.0, sondern 255.255.255.240 verwendet, ergeben sich folgende Subnetze:

Netz-ID	**Host-ID**
Subnetwork Mask:	**11111111 11111111 11111111 1111**0000
Subnetz	
190.136.0.0	10111110 10001000 00000000 **0000**0000
190.136.0.16	10111110 10001000 00000000 **0001**0000
190.136.0.32	10111110 10001000 00000000 **0010**0000
190.136.0.48	10111110 10001000 00000000 **0011**0000
190.136.0.64	10111110 10001000 00000000 **0100**0000
...	
...	
190.136.0.224	10111110 10001000 00000000 **1110**0000
190.136.0.240	10111110 10001000 00000000 **1111**0000

Analog erfolgt die Subnetzbildung für die weiteren Werte 2 bis 255 im dritten Oktett. Es können also bei einem vorliegenden Klasse-B-Netzwerk 190.136.0.0 durch *Subnetting* mit der Mask 255.255.255.240 insgesamt 4.096 Subnetze (256 × 16; 256 aus dem dritten und 16 aus dem vierten Oktett) mit jeweils 16 minus 2, also 14 IP-Adressen gebildet werden.

3.2.3 Verwendung privater IP-Adressen

Neben den öffentlich vergebenen und genutzten IP-Adressbereichen gibt es eine Vielzahl privater Subnetze, die ausschließlich zur internen Verwendung in Unternehmensnetzwerken genutzt werden können. Diese werden im Internet nicht berücksichtigt und können daher auch mehrfach vergeben werden, da sie ja die Unternehmensnetze nicht verlassen. Bei diesen reservierten privaten Adressbereichen handelt es sich um folgende Subnetze:

- Klasse A: 10.0.0.0/255.0.0.0
- Klasse B: 172.16.0.0/255.240.0.0
- Klasse C: 192.168.0.0/255.255.0.0

Beim Verlassen des Unternehmensnetzwerks bzw. bei der Anbindung an das öffentliche Netzwerk (Internet) erfolgt in der Regel ein »Übersetzen« der privaten Adressen auf öffentliche, legal zugewiesene Adressen. Ein Verfahren, das in diesem Zusammenhang eingesetzt wird, ist das Prinzip der *Network Address Translation* (NAT), also einer Art »Übersetzungstabelle«.

Werden beispielsweise zwei Standorte eines Unternehmens über IP-Router verbunden, wobei die beiden Standorte über ein eigenes Netzwerk verfügen, die wiederum mit einem Standort-Backbone verbunden sind, so erfolgt über diesen Backbone die WAN-Verbindung über einen dedizierten Router. Für das interne IP-Netzwerk wird die Klasse-A-Adresse 10.0.0.0 verwendet. Für die Strukturierung in verschiedene Subnetze wird die Subnetzmaske 255.255.255.0 verwendet. Pro Abteilung (drittes Oktett) innerhalb eines Standorts (zweites Oktett) stehen somit maximal 254 Host-IDs (viertes Oktett) zur Verfügung. Für den jeweiligen Standort lassen sich 255 verschiedene Abteilungsnetze etablieren. Für den Expansionsdrang des Unternehmens ist ebenfalls gesorgt: 255 Standorte können für die Zukunft mit einer eigenen Netz-ID adressiert werden. Es ergibt sich also folgende Adressstruktur:

Standort	Abteilung	Netz-ID
Hamburg	Auftragsbearbeitung	10.2.1.0
Hamburg	Buchhaltung	10.2.2.0
Hamburg	Versand	10.2.3.0
Hamburg	Datenverarbeitung	10.2.4.0
München	Auftragsbearbeitung	10.3.1.0
München	Buchhaltung	10.3.2.0
München	Versand	10.3.3.0
München	Datenverarbeitung	10.3.4.0
WAN-Verbindung der Standorte		10.1.1.0

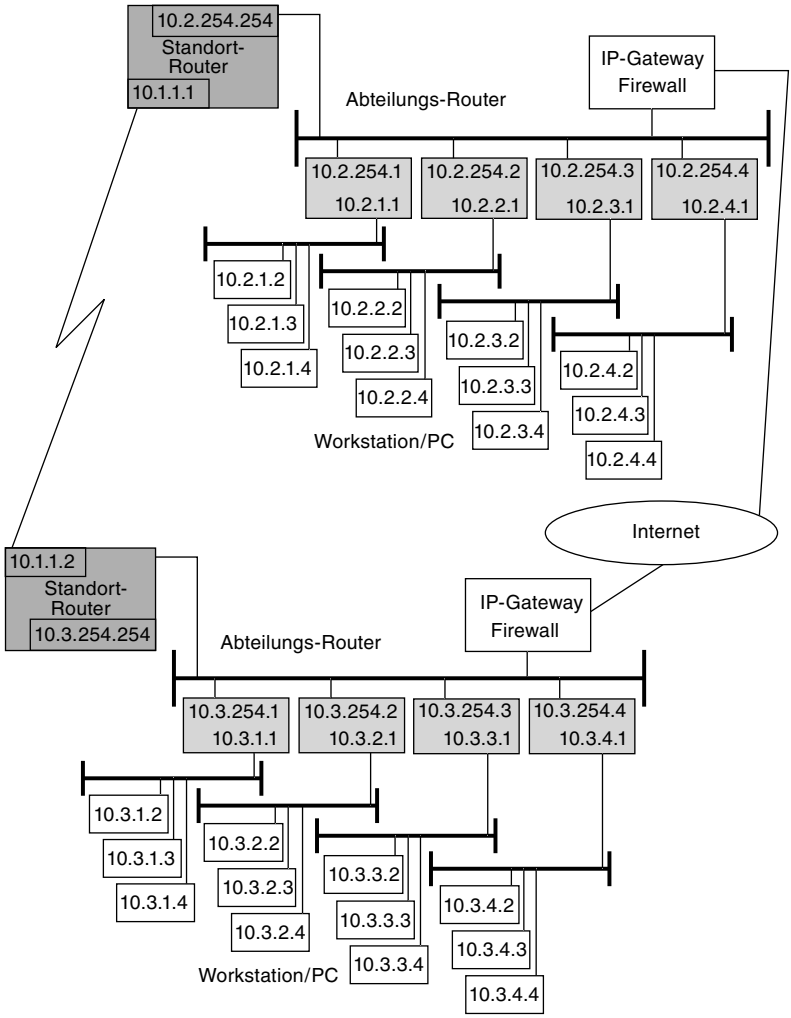

Abb. 3–6 *Beispiel: Adressstruktur bei einer WAN-Anbindung zweier Standorte*

3.2.4 Internetdomain und Subnetz

Ein erster Schritt zur eigenen Internetdomain ist zumeist die Kontaktaufnahme mit einem entsprechenden *Provider* bzw. *Hoster*, der in der Regel alle erforderlichen Formalitäten übernimmt. Somit entfällt ein direkter Vertragsabschluss mit dem DENIC, dem *Deutschen Network Information Center*. Das DENIC ist innerhalb Deutschlands für die kontrollierte Vergabe von Subdomains unterhalb der Top Level Domain »de« zuständig.

Will man eigene Internetdienste betreiben bzw. eigene Server ins Internet bringen (z.B. einen FTP- oder Webserver), so werden dazu legale Internetadressen

benötigt. Die Vergabe privater Adressen (gemäß RFC 1918) ist zu diesem Zweck nicht möglich, da man schließlich für weltweite Eindeutigkeit dieser IP-Adressen sorgen muss. Diese kann aber nur dann gewährleistet werden, wenn eine zentrale Instanz darüber wacht, dass eine IP-Adresse stets nur einmal vergeben wird. Für diese Aufgabe ist die ICANN verantwortlich (siehe auch hierzu Abschnitt 3.1.2).

Diese »Non-Profit-Organisation« verwaltet weltweit zentral eine Datensammlung von IP-Adressen und Subnetzen, wobei sie die Vergabe in anderen Ländern an weitere Instanzen delegiert. Dabei handelt es sich um das APNIC (*Asia-Pacific Network Information Center*; *www.apnic.net*), das ARIN (*American Registry for Internet Numbers*; *www.arin.net*), LACNIC (Latin America and Caribbean Network Information Centre; *www.lacnic.net*), AfriNIC (African Network Information Centre; *www.afrinic.net*) und das RIPE NCC (*Réseaux IP Européens*; *www.ripe.net*). Letzteres übernimmt diese Aufgabe für den europäischen Bereich des Internets.

Die wichtigsten Informationen zur IP-Adressierung, -Organisation und zu ihren Besonderheiten sind in den RFCs 2050 (*Internet Registry IP Allocation Guidelines*), 1918 (*Address Allocation for Private Internets*) und 1518 (*An Architecture for IP Address Allocation with CIDR*) hinterlegt. Es existieren auch weitere RFCs zu verschiedenen Registrierungsaufgaben. Diese kann man am besten im öffentlich verfügbaren RFC-Index nachlesen.

Da mit der Domainbeschaffung für Privatpersonen normalerweise kein eigenes IP-Subnetz (mehrere öffentliche IP-Adressen, die ausschließlich für den Antragsteller reserviert sind) erworben wird und der Kunde für den Internetzugang (nicht für die Bereitstellung eigener Dienste) dynamische IP-Adressen aus dem eigenen Kontingent des Providers erhält, wird der Prozess der Domain-Beantragung und Reservierung vom Provider meist in Eigenregie durchgeführt.

3.3 Dynamische Adressvergabe

Neben der statischen Zuordnung von Adressen für den Bereich der TCP/IP-Protokollfamilie gibt es je nach Anforderung auch andere Formen der Adresszuordnung, wie beispielsweise eine dynamische Vergabe der Adressen. Die beiden grundlegenden oder bekanntesten Verfahren sind dabei BootP und DHCP, wobei sich die Zuordnung nicht nur auf eine IP-Adresse bezieht, sondern damit auch weitere Angaben zur Netzwerkkonfiguration übermittelt werden können.

HINWEIS

Innerhalb von IP-Netzwerken folgt die Adressvergabe grundsätzlich sehr stringenten Vorgaben, die beispielsweise festlegen, dass in einem Netzwerk (IP-Segment) keine IP-Adresse doppelt vergeben werden darf. Sind IP-Adressen doppelt vorhanden, führt dies in der Regel zu den merkwürdigsten Effekten bis hin zum Ausfall der betreffenden Endgeräte.