

Kapitel 1

Netzwerke, Routing, Firewalls und Grundlagen

| | |
|--|------|
| Weiterführende Dokumente | 1-1 |
| Grundlegende Routerkonzepte | 1-1 |
| Was ist ein Router? | 1-1 |
| Routing Information Protocol (RIP) | 1-2 |
| IP-Adressen und das Internet | 1-2 |
| Netzmaske | 1-4 |
| Subnetzadressierung | 1-5 |
| Private IP-Adressen | 1-8 |
| Betrieb mit einer einzelnen IP-Adresse mit Hilfe von NAT | 1-8 |
| MAC-Adressen und ARP (Address Resolution Protocol) | 1-9 |
| Weiterführende Dokumente | 1-10 |
| DNS-Server | 1-10 |
| IP-Konfiguration über DHCP | 1-11 |
| Internetsicherheit und Firewalls | 1-11 |
| Was ist eine Firewall? | 1-11 |
| Netzwerk-Verkabelung | 1-12 |
| Kabel der Kategorie 5 | 1-13 |
| Das Innenleben eines Twisted-Pair-Kabels | 1-13 |
| Uplink-Switches, Crossover-Kabel und MDI-/MDIX-Umschaltung | 1-15 |

Kapitel 1

Netzwerke, Routing, Firewalls und Grundlagen

Dieses Kapitel gibt einen Überblick über IP-Netzwerke, Routing und allgemeine Netzwerkfragen.

Weiterführende Dokumente

In diesem Anhang wird häufiger auf RFC-Dokumente mit weiteren Informationen verwiesen. „RFC“ steht für „Request For Comment“. RFCs werden von der Internet Engineering Task Force (IETF) herausgegeben, einer offenen Vereinigung, die für die Architektur und Funktionsweise des Internets zuständig ist. In den RFC-Dokumenten werden die Standardprotokolle und -verfahren für das Internet festgelegt. Diese Dokumente sind im Internet unter www.ietf.org zu finden. Zahlreiche andere Websites enthalten ebenfalls Auszüge und Querverweise auf diese Dokumente.

Grundlegende Routerkonzepte

In einem LAN (Local Area Network) können große Bandbreiten einfach und relativ preisgünstig bereitgestellt werden. Die Bereitstellung einer großen Bandbreite zwischen einem lokalen Netzwerk und dem Internet kann dagegen sehr kostspielig sein. Auf Grund dieser Kosten wird der Internetzugang in der Regel über eine langsamere WAN-Verbindung (Wide Area Network) hergestellt, z. B. über ein Kabel- oder DSL-Modem. Um eine optimale Ausnutzung der langsameren WAN-Verbindung zu gewährleisten, benötigt man einen Mechanismus, der den für das Internet bestimmten Datenverkehr auswählt und dafür sorgt, dass nur diese Daten übertragen werden. Die Auswahl und Weiterleitung dieser Daten wird von einem Router übernommen.

Was ist ein Router?

Ein Router ist ein Gerät, das den Datenverkehr zwischen Netzwerken weiterleitet. Die Weiterleitung erfolgt anhand der in den Daten enthaltenen Informationen aus der Vermittlungsschicht und der vom Router geführten Routingtabellen. In diesen Routingtabellen legt der Router ein logisches Abbild des gesamten Netzwerks an, indem er Daten sammelt und diese mit anderen Routern im Netzwerk austauscht. Anhand dieser Informationen wählt der Router dann den besten Pfad für die Weiterleitung des Netzwerkverkehrs.

Router unterscheiden sich in ihrer Leistung und ihrem Umfang, der Anzahl der unterstützten Routingprotokolle und der Arten von WAN-Verbindungen, die sie unterstützen. Der - ist ein kleiner Router für Büro Zwecke, der das IP-Protokoll über eine Einzelbenutzer-Breitbandverbindung leitet.

Routing Information Protocol (RIP)

Zu den Protokollen, mit deren Hilfe Router ein Abbild des Netzwerks aufbauen und aktualisieren, gehört das Routing Information Protocol (RIP). Mit Hilfe von RIPs senden Router sich gegenseitig in regelmäßigen Abständen Aktualisierungen zu und suchen nach Veränderungen, die in die Routingtabelle aufgenommen werden müssen.

Der - unterstützt sowohl das ältere Protokoll RIP-1 als auch das neuere RIP-2. Zu den Neuerungen von RIP-2 gehört die Unterstützung von Subnetz- und Multicast-Protokollen. RIP ist für die meisten in Privathaushalten eingesetzten Anwendungen nicht erforderlich.

IP-Adressen und das Internet

Da TCP/IP-Netzwerke in der gesamten Welt miteinander verbunden sind, benötigt jedes Gerät im Internet eine eindeutige Adresse. Nur so kann sichergestellt werden, dass gesendete Daten am vorgesehenen Ziel ankommen. Die Vergabe von Adressen erfolgt blockweise durch die IANA (Internet Assigned Numbers Authority). Einzelne Benutzer und kleinere Unternehmen und Organisationen können ihre Adressen entweder direkt von der IANA oder über einen Internet-Provider beziehen. Sie können die IANA unter www.iana.org kontaktieren.

Das Internet Protocol (IP) verwendet eine 32-Bit-Adressstruktur. Die Adresse wird normalerweise in der Dezimalschreibweise (auch als Punktnotation bezeichnet) angegeben. Dabei werden die einzelnen Gruppen von jeweils acht Bit in dezimaler Form und durch Punkte getrennt angegeben.

So erscheint z. B. die folgende binäre Adresse

```
11000011 00100010 00001100 00000111
```

in der Regel als

```
195.34.12.7
```

Die zweite Version prägt sich besser ein und ist außerdem bequemer für die Eingabe.

Die 32 Bit der Adresse werden zudem in zwei Teile unterteilt: Der erste Teil der Adresse identifiziert das Netzwerk, der zweite Teil den Host-Knoten oder die Host-Station des Netzwerks. Der Trennpunkt zwischen dem ersten und zweiten Teil kann je nach Adressabschnitt und Anwendung unterschiedlich sein.

Es gibt fünf Standardklassen von IP-Adressen. Bei jeder dieser Adressklassen wird der Netzwerk- und Hostabschnitt der Adresse auf unterschiedliche Weise festgelegt, um die unterschiedliche Hostanzahl in Netzwerken zu berücksichtigen. Jede Adresse beginnt mit einem eindeutigen Bit-Muster, über das die TCP/IP-Software die Adressklasse identifizieren kann. Anhand der Adressklasse kann die Software den Hostabschnitt der Adresse ermitteln. Die folgende Abbildung zeigt die drei wichtigsten Adressklassen mit den jeweiligen Netzwerk- und Hostabschnitten.

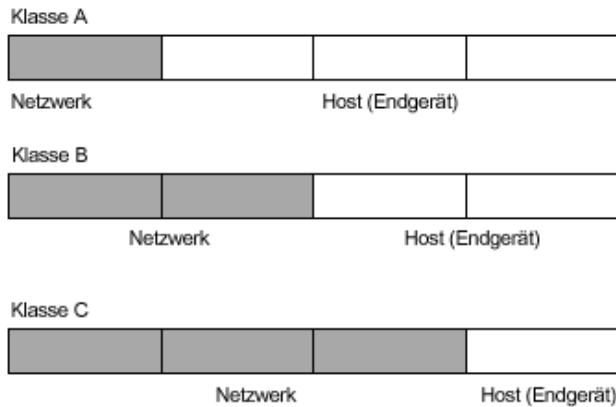


Abbildung 1-1 Die drei wichtigsten Adressklassen

Die fünf Adressklassen sind:

- Klasse A
Adressen der Klasse A lassen bis zu 16.777.214 Hosts in einem einzigen Netzwerk zu. Sie verwenden 8 Bit für die Netzwerknummer und 24 Bit für die Hostadresse. Die Adressen der Klasse A befinden sich in diesem Bereich:

1.x.x.x bis 126.x.x.x.

- Klasse B
Adressen der Klasse B lassen bis zu 65.354 Hosts in einem Netzwerk zu. Sie verwenden jeweils 16 Bit für die Netzwerknummer und die Hostadresse. Die Adressen der Klasse B befinden sich in diesem Bereich:

128.1.x.x bis 191.254.x.x.

- Klasse C
Adressen der Klasse C lassen bis zu 254 Hosts in einem Netzwerk zu. Sie verwenden 24 Bit für die Netzwerkadresse und 8 Bit für die Hostadresse. Die Adressen der Klasse C befinden sich in diesem Bereich:

192.0.1.x bis 223.255.254.x.

- Klasse D
Die Adressen der Klasse D werden für Multicasts (Übersenden von Nachrichten an mehrere Hosts) verwendet. Sie befinden sich in diesem Bereich:

224.0.0.0 bis 239.255.255.255.

- Klasse E
Die Adressen der Klasse E dienen experimentellen Zwecken.

Dank dieser Adressstruktur können IP-Adressen jedes physikalische Netzwerk und jeden Host in jedem physikalischen Netzwerk eindeutig identifizieren.

Als Netzwerkadresse für jeden eindeutigen Wert des Netzwerkabschnitts der Adresse wird die Basisadresse des Bereichs (mit lauter Nullen als Hostadresse) verwendet. Diese wird in der Regel nicht einem Host zugewiesen. Die höchste Adresse des Bereichs (bei der die Hostadresse aus lauter Einsen – bzw. dem Wert 255 – besteht) wird ebenfalls nicht vergeben, sondern als Broadcast-Adresse verwendet. Über die Broadcast-Adresse kann ein Paket simultan an alle Hosts mit derselben Netzwerkadresse versendet werden.

Netzmaske

In den oben beschriebenen Adressklassen wird die Größe der beiden Abschnitte (Netzwerkadresse und Hostadresse) durch die Klasse festgelegt. Dieses Unterteilungsschema kann auch durch eine der IP-Adresse zugeordnete Netzmaske ausgedrückt werden. Über die 32 Bit lange Netzmaske lässt sich durch logische UND-Verknüpfung mit einer IP-Adresse die Netzwerkadresse ermitteln. Die Netzmasken für die Klassen A, B und C lauten z. B.: 255.0.0.0, 255.255.0.0 und 255.255.255.0.

Die IP-Adresse 192.168.170.237 ist eine Adresse der Klasse C, deren Netzwerkabschnitt aus den vorderen 24 Bit besteht. Wenn diese Adresse, wie hier gezeigt, mit der Netzmaske für die Klasse C logisch mit UND verknüpft wird, bleibt nur der Netzwerkabschnitt der Adresse übrig:

```
11000000 10101000 10101010 11101101 (192.168.170.237)
```

verknüpft mit

```
11111111 11111111 11111111 00000000 (255.255.255.0)
```

ist gleich

```
11000000 10101000 10101010 00000000 (192.168.170.0)
```

Als kürzere Alternative zur Dezimalschreibweise kann die Netzmaske auch als Anzahl der Einsen von links gezählt angegeben werden. Diese Anzahl wird nach einem Backslash (/) an die IP-Adresse angehängt: „/n“. In unserem Beispiel könnte die IP-Adresse also auch als 192.168.170.237/24 geschrieben werden. Dieser Schreibweise ist zu entnehmen, dass die Netzmaske aus 24 Einsen gefolgt von 8 Nullen besteht.

Subnetzadressierung

Ein Blick auf die Adressstrukturen lässt erkennen, dass selbst bei Adressen der Klasse C eine große Anzahl von Hosts pro Netzwerk zulässig ist. Eine solche Struktur bedeutet eine ineffiziente Adressennutzung, wenn für jedes Ende einer Routerverbindung eine andere Netzwerkadresse erforderlich ist. Kleinere Büro-LANs verfügen häufig nicht über die dafür erforderliche Geräteanzahl. Die Lösung für dieses Problem heißt Subnetzadressierung.

Die Subnetzadressierung ermöglicht die Aufteilung einer IP-Netzwerkadresse in mehrere kleinere physikalische Netzwerke, die auch als Subnetze bezeichnet werden. Dabei werden einige der Hostadressen als Subnetznummern verwendet. Eine Adresse der Klasse B ergibt 16 Bit an Hostadressen bzw. 64.000 Hosts. Da die meisten Organisationen keine 64.000 Hosts benötigen, bleiben freie Bits übrig, die anders vergeben werden können. Mit Hilfe der Subnetzadressierung können diese freien Bits genutzt werden (vgl. Abbildung unten).



Abbildung 1-2

Eine Adresse der Klasse B kann in viele Adressen der Klasse C aufgeteilt werden. Ein Beispiel: Die IP-Adresse „172.16.0.0“ wurde vergeben, doch es gibt nicht mehr als 255 Hostadressen. Dadurch stehen 8 zusätzliche Bits für die Subnetzadresse zur Verfügung. Zur Verdeutlichung: Bei der IP-Adresse „172.16.97.235“ ist 172.16 die IP-Netzwerkadresse, 97 die Subnetzadresse und 235 die Hostadresse. Neben der Erweiterung der verfügbaren Adressen hat die Subnetzadressierung jedoch auch noch andere Vorteile. Mit Hilfe der Subnetzadressierung kann ein Netzwerkmanager ein Adressschema für das Netzwerk entwickeln, bei dem für die einzelnen geografischen Standorte oder Abteilungen der Organisation unterschiedliche Subnetze eingerichtet werden.

Auch wenn im obigen Beispiel das gesamte dritte Oktett für eine Subnetzadresse verwendet wird, ist die Einrichtung von Subnetzen keineswegs auf die Grenzen eines Oktetts beschränkt. Wenn Sie weitere Netzwerknummern benötigen, müssen Sie lediglich einige Bits von der Hostadresse in die Netzwerkadresse verschieben. Angenommen, Sie möchten eine Netzwerknummer der Klasse C (z. B. 192.68.135.0) in zwei Nummern unterteilen. Dann verschieben Sie ein Bit von der Hostadresse in die Netzwerkadresse. Die neue Netzmaske (oder Subnetzmaske) lautet: 255.255.255.128. Das erste Subnetz hat die Netzwerknummer 192.68.135.0 mit Hosts von 192.68.135.1 bis 192.68.135.126, das zweite Subnetz hat die Netzwerknummer 192.68.135.128 mit Hosts von 192.68.135.129 bis 192.68.135.254.



Hinweis: Die Nummer 192.68.135.127 wird nicht vergeben, da sie die Broadcast-Adresse des ersten Subnetzes ist. Die Nummer 192.68.135.128 wird nicht vergeben, da sie die Netzwerk-Adresse des zweiten Subnetzes ist.

In der folgenden Tabelle sind die zusätzlichen Subnetzmaskenbits in Dezimalschreibweise aufgeführt. So verwenden Sie diese Tabelle: Schreiben Sie die ursprüngliche Netzmaske der Klasse auf und ersetzen Sie die Oktetts durch den Wert „0“ mit dem Wert der zusätzlichen Subnetz-Bits in Dezimalschreibweise. Wenn Sie zum Beispiel ein Netzwerk der Klasse C mit der Subnetzmaske 255.255.255.0 in 16 Subnetze (4 Bit) unterteilen möchten, ist die neue Subnetzmaske 255.255.255.240.

Tabelle 1-1. Tabelle zur Netzmaskennotationsumwandlung für ein Oktett

| Bits | Wert in Dezimalschreibweise |
|------|-----------------------------|
| 1 | 128 |
| 2 | 192 |
| 3 | 224 |
| 4 | 240 |
| 5 | 248 |
| 6 | 252 |
| 7 | 254 |
| 8 | 255 |

Die folgende Tabelle enthält eine Auswahl häufiger Netzmaskenwerte in Dezimalschreibweise und die Maskenlängenformate.

Tabelle 1-2. Netzmaskenformate

| Dezimalschreibweise | Maskenlänge |
|---------------------|-------------|
| 255.0.0.0 | /8 |
| 255.255.0.0 | /16 |
| 255.255.255.0 | /24 |
| 255.255.255.128 | /25 |
| 255.255.255.192 | /26 |
| 255.255.255.224 | /27 |
| 255.255.255.240 | /28 |
| 255.255.255.248 | /29 |
| 255.255.255.252 | /30 |
| 255.255.255.254 | /31 |
| 255.255.255.255 | /32 |

Achten Sie bei der Konfiguration darauf, dass alle Hosts in einem LAN-Segment dieselbe Netzmaske verwenden. Dies empfiehlt sich aus folgenden Gründen:

- Nur so können alle Hosts lokale IP-Broadcast-Datenpakete erkennen.
Wenn ein Gerät Broadcasts an seine Segmentnachbarn überträgt, verwendet es als Zieladresse die lokale Netzwerkadresse mit lauter Einsen als Hostadresse. Damit diese Vorgehensweise funktioniert, müssen auf allen Geräten im Segment dieselben Bits als Hostadresse konfiguriert sein.
- Nur so kann ein lokaler Router oder eine lokale Bridge erkennen, welche Adressen lokal und welche entfernt sind.

Private IP-Adressen

Wenn Ihr lokales Netzwerk vom Internet isoliert ist (z. B. wenn Sie NAT verwenden), können Sie den Hosts beliebige IP-Adressen zuweisen, ohne dass dadurch Probleme entstehen. Die folgenden drei Blöcke von IP-Adressen wurden jedoch von der IANA speziell für private Netzwerke reserviert:

10.0.0.0 bis 10.255.255.255
172.16.0.0 bis 172.31.255.255
192.168.0.0 bis 192.168.255.255

Wählen Sie Ihre private Netzwerknummer also am besten aus diesen Bereichen aus. Der DHCP-Server des -s ist so vorkonfiguriert, dass er automatisch private Adressen vergibt.

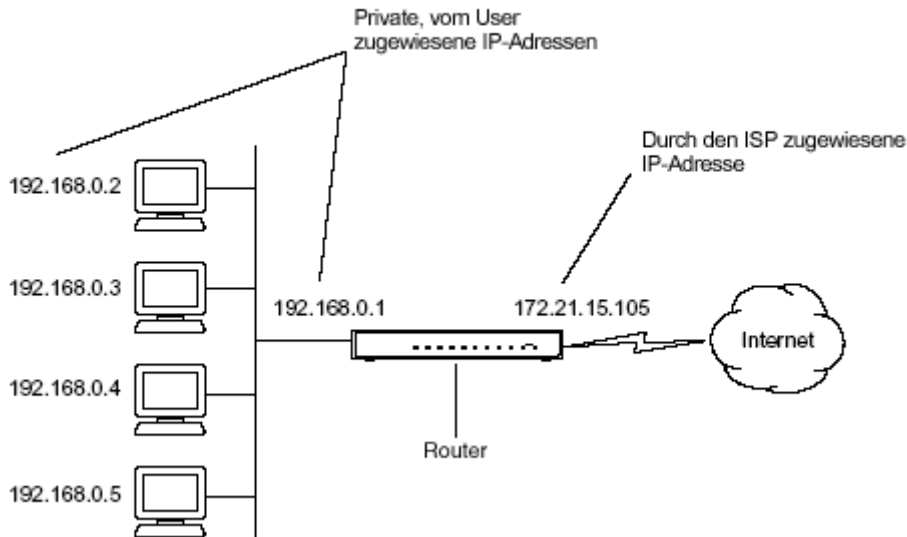
Erstellen Sie unter keinen Umständen beliebige IP-Adressen, sondern folgen Sie immer den Hinweisen hier. Weitere Informationen zur Adresszuweisung finden Sie in den Dokumenten RFC 1597, „*Address Allocation for Private Internets*“, und RFC 1466, „*Guidelines for Management of IP Address Space*“. Die RFCs sind auf der Website der Internet Engineering Task Force (IETF) unter www.ietf.org veröffentlicht.

Betrieb mit einer einzelnen IP-Adresse mit Hilfe von NAT

Um mehreren Computern eines LAN gleichzeitig den Zugriff aufs Internet zu ermöglichen, musste man lange Zeit mehrere IP-Adressen vom Internet-Provider beziehen. Diese Art von Internetzugang ist teurer als ein Konto mit einer einzigen Adresse, wie es normalerweise von einem Einzelbenutzer mit einem Modem (statt eines Routers) eingesetzt wird. Der - verwendet zur gemeinsamen Nutzung von Adressen eine Methode namens NAT (Network Address Translation). Mit Hilfe dieser Methode können mehrere vernetzte Computer ein Internetkonto mit einer einzigen IP-Adresse gemeinsam nutzen. Die IP-Adresse kann dabei vom Internet-Provider statisch oder dynamisch vergeben werden.

Diese gemeinsame Nutzung der Adresse wird dadurch ermöglicht, dass der Router die internen LAN-IP-Adressen in eine einzige Adresse umwandelt, die im Internet weltweit eindeutig ist. Die internen LAN-IP-Adressen können dabei entweder private oder registrierte Adressen sein. Weitere Informationen zur Umwandlung von IP-Adressen finden Sie im Dokument RFC 1631, „*The IP Network Address Translator (NAT)*“.

Die folgende Abbildung illustriert den Betrieb mit einer einzigen IP-Adresse.

**Abbildung 1-3**

Die abgebildete Lösung bietet zudem einen Firewall-ähnlichen Schutz, da die internen LAN-Adressen im Internet auf Grund der Umwandlung bei der Verbindung nicht zu erkennen sind. Alle eingehenden Anforderungen werden durch den Router gefiltert. Diese Filterung kann verhindern, dass unbefugte Eindringlinge Ihr System ausspionieren. Mit Hilfe einer Portweiterleitung können Sie aber dennoch einen Computer in Ihrem lokalen Netzwerk (z. B. einen Webserver) für externe Benutzer zugänglich machen.

MAC-Adressen und ARP (Address Resolution Protocol)

Eine IP-Adresse allein reicht nicht aus, um Daten von einem LAN-Gerät an ein anderes zu senden. Um den Versand von Daten zwischen LAN-Geräten zu ermöglichen, muss die IP-Adresse des Zielgeräts in dessen MAC-Adresse (Media Access Control) umgewandelt werden. Jedes Gerät in einem Netzwerk verfügt über eine eindeutige MAC-Adresse. Bei der MAC-Adresse handelt es sich um eine 48-Bit-Nummer, die jedem Gerät vom Hersteller zugewiesen wird. Zur Zuordnung von IP-Adressen zu MAC-Adressen wird ein Protokoll namens ARP (Address Resolution Protocol) verwendet. IP verwendet ARP zum Ermitteln von MAC-Adressen.

Wenn ein Gerät Daten an eine andere Station im Netzwerk sendet und die MAC-Zieladresse noch nicht erfasst ist, wird ARP verwendet. Dazu wird eine ARP-Anforderung an das Netzwerk gesendet. Alle Stationen des Netzwerks empfangen und lesen diese Anforderung. Die IP-Zieladresse der gewünschten Station ist in dieser Anforderung enthalten. So antwortet nur die Station mit dieser IP-Adresse auf die ARP-Anforderung. Alle anderen Stationen ignorieren die Anfrage.

Weiterführende Dokumente

Die Station mit der richtigen IP-Adresse antwortet mit ihrer eigenen MAC-Adresse direkt an das sendende Gerät. Die Empfängerstation gibt die gewünschte MAC-Zieladresse an die übertragende Station weiter. Die IP- und MAC-Adressdaten für die einzelnen Stationen werden in einer ARP-Tabelle gespeichert. Beim nächsten Versand von Daten kann die Adresse den in der Tabelle gespeicherten Informationen entnommen werden.

Weitere Informationen zur Adresszuweisung finden Sie in den IETF-Dokumenten RFC 1597, „*Address Allocation for Private Internets*“, und RFC 1466, „*Guidelines for Management of IP Address Space*“.

Weitere Informationen zur Umwandlung von IP-Adressen finden Sie im Dokument RFC 1631, „*The IP Network Address Translator (NAT)*“.

DNS-Server

Viele der Ressourcen im Internet können über einfache beschreibende Namen wie www.NETGEAR.com erreicht werden. Diese Art der Adressierung ist auf der Anwendungsebene sehr praktisch, doch damit ein Benutzer wirklich auf die Ressource zugreifen kann, muss der beschreibende Name in eine IP-Adresse umgewandelt werden. Ähnlich wie ein Telefonbuch bestimmten Namen bestimmte Telefonnummern zuordnet oder eine ARP-Tabelle IP-Adressen die entsprechenden MAC-Adressen zuordnet, ordnet ein DNS-Server (Domain Name System) beschreibenden Namen die richtigen IP-Adressen zu.

Wenn ein Computer über einen beschreibenden Namen auf eine Ressource zugreift, kontaktiert er dabei zuerst einen DNS-Server, um die IP-Adresse der Ressource zu erfahren. Der Computer sendet die gewünschte Nachricht über die IP-Adresse. Viele große Unternehmen, wie z. B. Internet-Provider, haben eigene DNS-Server und gestatten ihren Kunden die Benutzung dieser Server zum Nachschlagen von Adressen.

IP-Konfiguration über DHCP

Bei der Installation eines IP-basierten LANs muss für jeden Computer eine IP-Adresse konfiguriert werden. Wenn der Computer auf das Internet zugreifen soll, sollten zudem eine Gateway-Adresse und eine oder mehrere DNS-Serveradressen konfiguriert werden. Als Alternative zur manuellen Konfiguration gibt es auch eine Methode, mit der jeder Computer im Netzwerk diese Konfigurationsdaten automatisch abrufen kann: Ein Gerät im Netzwerk wird als DHCP-Server (Dynamic Host Configuration Protocol) eingesetzt. Der DHCP-Server speichert neben anderen Informationen (darunter Gateway- und DNS-Adressen) eine Liste von IP-Adressen, die er an andere Geräte im Netzwerk vergeben kann. Der - kann als DHCP-Server eingesetzt werden.

Beim Verbindungsaufbau zum Internetdienstarbeiter dient der - außerdem als DHCP-Client. Falls der Internet-Provider diese Informationen per DHCP zur Verfügung stellt, kann die Firewall automatisch IP-Adresse, Subnetzmaske, DNS-Serveradressen und eine Gateway-Adresse abrufen.

Internetsicherheit und Firewalls

Wenn Ihr LAN über einen Router an das Internet angeschlossen ist, besteht die Gefahr, dass Eindringlinge von außen auf Ihr Netzwerk zugreifen oder Störungen verursachen. Ein NAT-Router gewährt hier einen gewissen Schutz, da bei diesem Verfahren das Netzwerk hinter dem Router vor externen Zugriffen über das Internet geschützt ist. Hartnäckige Hacker können sich allerdings dennoch Informationen über Ihr Netzwerk verschaffen oder zumindest Ihre Internetverbindung unterbrechen. Besseren Schutz bietet ein Firewall-Router.

Was ist eine Firewall?

Eine Firewall ist ein Gerät, das ein Netzwerk vor einem anderen Netzwerk schützt, aber dennoch einen Austausch zwischen den beiden Netzwerken zulässt. Eine Firewall beinhaltet die Funktionen eines NAT-Routers, ergänzt diese jedoch um weitere Funktionen zur Abwehr von unbefugten Zugriffen und Angriffen durch Hacker. Eine Reihe bekannter Typen von Zugriffsversuchen und Hackerangriffen kann erkannt werden, sobald sie auftreten. Wenn es zu einem Vorfall kommt, kann die Firewall Einzelheiten des Angriffsversuchs protokollieren und ggf. den Administrator per E-Mail benachrichtigen. Mit den im Protokoll festgehaltenen Daten kann der Administrator sich dann an den Internet-Provider des Hackers wenden. Bei manchen Arten von Zugriffsversuch kann die Firewall den Hacker abwehren, indem alle weiteren Pakete, die von der IP-Adresse des Hackers stammen, für eine gewisse Zeit ignoriert werden.

SPI (Stateful Packet Inspection)

Anders als gewöhnliche Router für die gemeinsame Internetnutzung verwendet eine Firewall einen Prozess namens SPI (Stateful Packet Inspection). Dabei wird das Netzwerk durch sichere Firewall-Filterung vor Angriffen und Zugriffsversuchen geschützt. Da Benutzeranwendungen wie FTP und Webbrowser komplexe Netzwerkverkehrsmuster schaffen können, muss die Firewall in der Lage sein, den Status von Netzwerkverbindungen gruppenweise zu analysieren. Durch SPI werden eingehende Pakete in der Vermittlungsschicht abgefangen und dann in Bezug auf statusbezogene Informationen zu allen Netzwerkverbindungen analysiert. Ein zentraler Cache-Speicher innerhalb der Firewall protokolliert die Statusinformationen zu allen Netzwerkverbindungen. Der gesamte Datenverkehr, der durch die Firewall geht, wird im Hinblick auf den Status dieser Verbindung analysiert. Dadurch wird bestimmt, ob die Daten durchgelassen oder abgelehnt werden.

Denial-of-Service-Angriffe

Mit Denial-of-Service-Angriffen (DoS) können Hacker Ihr Netzwerk funktionsunfähig machen oder die Kommunikation verhindern. Ein derartiger Angriff kann mit ganz einfachen Mitteln geschehen. Es reicht schon aus, Ihre Website mit mehr Anfragen zu überschwemmen, als diese verarbeiten kann. Ein etwas raffinierterer Angreifer versucht vielleicht, Schwachstellen im Betriebssystem Ihres Routers oder Gateways auszunutzen. Manche Betriebssysteme können z. B. schon durch Senden eines Datenpakets mit falschen Längenangaben gestört werden.

Netzwerk-Verkabelung

Ursprünglich wurden für Netzwerke dicke oder dünne Koaxialkabel verwendet, doch inzwischen werden meistens ungeschirmte Twisted-Pair-Kabel (UTP) eingesetzt. Ein UTP-Kabel besteht aus vier miteinander verdrehten Aderpaaren und hat einen RJ45-Stecker. Ein normales UTP-Patchkabel (Durchgangskabel) entspricht der Standardverdrahtung nach EIA568B, die unten in [Table 0-1](#) dargestellt ist.

Tabelle 0-1. Verdrahtung eines UTP-Patchkabels

| Pin | Leitungsfarbe | Signal |
|-----|---------------|------------------|
| 1 | Orange/Weiß | Senden (Tx) + |
| 2 | Orange | Senden (Tx) - |
| 3 | Grün/Weiß | Empfangen (Rx) + |
| 4 | Blau | |
| 5 | Blau/Weiß | |

Tabelle 0-1. Verdrahtung eines UTP-Patchkabels (Fortsetzung)

| Pin | Leitungsfarbe | Signal |
|-----|---------------|------------------|
| 6 | Grün | Empfangen (Rx) - |
| 7 | Braun/Weiß | |
| 8 | Braun | |

Kabel der Kategorie 5

Kabel der Kategorie 5 (CAT 5), die den Standards ANSI/EIA/TIA-568-A entsprechen, dürfen eine Gesamtlänge von 100 m nicht überschreiten. Diese Länge ist wie folgt aufzuteilen:

6 m zwischen dem Switch und dem Patch-Panel (falls eines verwendet wird)

90 m zwischen dem Kabelschrank und der Wandsteckdose

3 m zwischen der Wandsteckdose und dem Desktop-Gerät

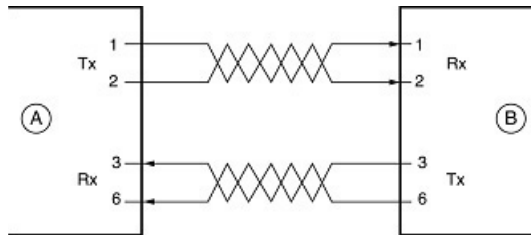
Das Patch-Panel und sonstige Geräte müssen den Anforderungen für den Betrieb bei 100 MBit/s (Kategorie 5) entsprechen. An den Schnittstellen darf das Leitungspaar jeweils max. 1,5 cm entdrillt werden.

Bei Twisted-Pair-Netzwerken, die mit 10 MBit/s (10BASE-T) arbeiten, wirkt es sich meist nicht nachteilig aus, wenn Kabel von niedriger Qualität verwendet werden. Bei 100 MBit/s (100BASE-Tx) muss das Kabel dagegen der Kategorie 5 (Cat 5) der EIA (Electronic Industries Alliance) entsprechen. Diese Kategorie ist auf die Kabelummantelung aufgedruckt. Ein Kabel der Kategorie 5 erfüllt besondere Anforderungen hinsichtlich Datenverlust und Störsignalen. Sowohl bei Netzwerken mit 10 MBit/s als auch bei Netzwerken mit 100 MBit/s sind zudem Einschränkungen bezüglich der maximalen Kabellänge zu berücksichtigen.

Das Innenleben eines Twisted-Pair-Kabels

Damit zwei Geräte miteinander kommunizieren können, muss der Sender jedes Geräts mit dem Empfänger des jeweils anderen Geräts verbunden sein. Die Crossover-Funktion ist normalerweise in die Schaltkreise des Geräts integriert. Adapterkarten für Computer und Workstations sind in der Regel MDI-Ports (Media Dependent Interface), die auch als Uplink-Ports bezeichnet werden. Die meisten Repeater und Switch-Ports sind als MDI mit integrierten Crossover-Ports konfiguriert. Diese werden als MDI-X-Ports oder normale Ports bezeichnet. Die Auto Uplink-Technologie erkennt automatisch, welche Verbindungsart (MDI oder MDI-X) benötigt wird, und stellt die richtige Verbindung her.

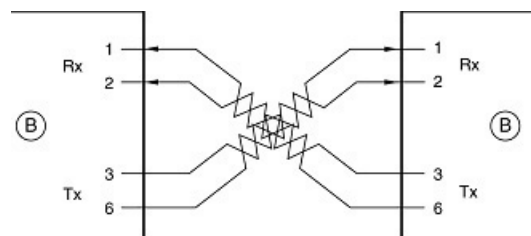
Figure 1-4 zeigt ein Twisted-Pair-Durchgangskabel



A = Uplink- oder MDI-Port (z. B. an einem PC)
B = Normal- oder MDI-X-Port (z. B. an einem Switch)
1, 2, 3, 6 = Pinnummern

Abbildung 1-4

Figure 1-5 zeigt ein Twisted-Pair-Crossover-Kabel



B = Normal- oder MDI-X-Port (z. B. an einem Switch)
1, 2, 3, 6 = Pinnummern

Abbildung 1-5

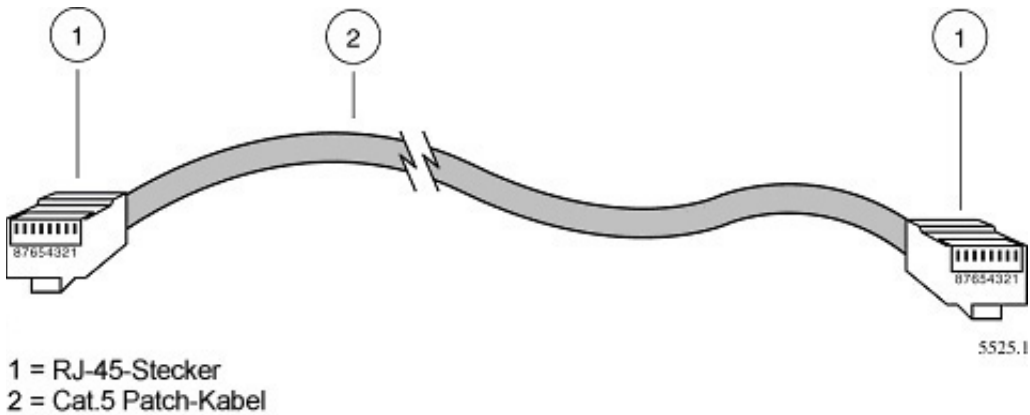


Abbildung 1-6



Hinweis: Manche Telefonkabel können auch über einen RJ-45-Stecker verfügen. Die Verwendung von Telefonkabeln führt jedoch zu einer Vielzahl von Kollisionen, so dass der darüber angeschlossene Port partitioniert oder vom Netzwerk getrennt wird.

Uplink-Switches, Crossover-Kabel und MDI-/MDIX-Umschaltung

In der Verdrahtungstabelle weiter oben sind die Signale „Senden“ und „Empfangen“ aus der Perspektive des Computers dargestellt, der als MDI (Media Dependent Interface) verdrahtet ist. Bei dieser Verdrahtung sendet der Computer über die Pins 1 und 2. Im Switch wird die Perspektive umgekehrt, und über die Pins 1 und 2 erfolgt der Empfang. Diese Art der Verdrahtung wird als „MDI-X“ (Media Dependant Interface – Crossover) bezeichnet.

Wenn ein Computer mit einem anderen Computer oder ein Switch-Port mit einem anderen Switch-Port verbunden werden soll, muss das Senderpaar mit dem Empfängerpaar vertauscht werden. Dieser Tausch kann über einen der folgenden zwei Mechanismen bewerkstelligt werden. Die meisten Switches verfügen über einen Uplink-Umschalter, der es ermöglicht, die Paare an einem Port zu vertauschen, so dass dieser Port über ein normales Netzkabel mit einem anderen Switch verbunden werden kann. Die zweite Möglichkeit ist die Verwendung eines Crossover-Kabels. Dabei handelt es sich um ein spezielles Kabel, bei dem das Sender- und Empfängerpaar in einem der Anschlüsse vertauscht ist. Crossover-Kabel sind oft nicht als solche gekennzeichnet, können jedoch durch einen Vergleich der beiden Anschlüsse identifiziert werden. Da die Stecker aus durchsichtigem Plastik sind, kann man sie leicht nebeneinander legen und die Reihenfolge der Leitungsfarben vergleichen. Bei einem Durchgangskabel ist die Farbreihenfolge in beiden Steckern gleich. Bei einem Crossover-Kabel sind das orangefarbene und das grüne Paar bei einem der beiden Stecker vertauscht.

Der - verwendet die Auto Uplink™-Technologie (auch als MDI/MDIX bezeichnet). Dies bedeutet, dass jeder LAN-Port automatisch erkennt, ob für das eingesteckte Netzkabel eine normale Verbindung (d. h. eine Verbindung zu einem Computer) oder eine Uplink-Verbindung (d. h. eine Verbindung zu einem Router oder Switch) erforderlich ist. Daraufhin wird der Anschluss automatisch für die benötigte Verbindung konfiguriert. Diese Funktion macht zudem die Verwendung von Crossover-Kabeln unproblematisch, da Auto Uplink™ bei beiden Kabeltypen die richtige Verbindung herstellt.