Referat: IP-Adressen / NAT-PAT / Masquerading

von Lena Günzler und Dominik Jakob

Gliederung:

0. Was ist eine IP-Adresse?
1. Welche IP-Adresse hat mein PC?
2. Wie erhalte ich meine IP-Adresse?

    2.1. manuell
        2.1.1. bei Windowsen
        2.1.2. bei Linuxen
    2.2. automatisch
        2.2.1. dynamische Zuordnung
        2.2.1. statische Zuordnung
    2.3. Wie bringe nun meinem PC bei, dass er eine IP-Adresse vom DHPC-Server bekommt?
        2.3.1. bei Windowsen
        2.3.2. bei Linuxen

2.4. Was hat es aber mit der Subnetmaske; dem DNS-Eintrag und dem Gateway auf sich?
    2.4.1. Subnetmask
        2.4.1.1. herkömmliche Klassenschreibweise
        2.4.1.2. CIDR

    2.4.2. Gründe für Subnetting:

    2.4.3. Spezielle IP-Adressen

    2.4.4. Was ist nun der Default-Gateway?

        2.4.4.1. Eintrag Gateway beim PC???

3. Funktionsweise NAT/PAT (Ports)

    3.1. Wie funktioniert nun der Aufruf einer Internet-Seite bei NAT/PAT

    3.1.1 Vor und Nachteile von NAT/PAT

4. Und was macht nun der DNS-Server?

5. Und was macht nun ein Proxy?
    5.1. nicht transparenter Proxy
    5.2. transparenter Proxy

6. Und wie funktioniert jetzt die Weiterleitung von Datenpaketen im Internet?

    6.1 Eine kleine Übersicht über die gängigsten Routing-Protokolle
    6.2 Und was sind nun routbare Protokolle?

7. IPv6
    7.1 Warum ein neues Protokoll?
    7.2 Adressaufbau von IPv6
    7.3 Aufteilung des IPv6-Adressraums
    7.4 Adressvergabe und Autokonfiguration
    7.5 Probleme und Vorteile

0. Was ist eine IP-Adresse?

In einem LAN hat jeder PC eine eindeutige IP-Adresse.
Somit kann dieser PC über diese Adresse Daten mit anderen PC´s auszutauschen.
(Dies funktioniert ähnlich wie eine Telefonnummer oder eine Briefadresse)

Normalerweise wird diese 32 bitige Binärzahl zur besseren Lesbarkeit als eine Dezimalzahl, welche aus vier Trippeln besteht notiert.
z B.

Jedes Trippel besteht also aus 8 Bits

IP-Adresse: 192.168.100.4

192= 11000000
168= 10101000
100= 01100100
4 = 00000100

=> 11000000 | 10101000 | 01100100 | 00000100

Diese IP-Adressen werden als IPv4 bezeichnet, weil dies die vierte Version von IP-Adressen ist, nicht weil sie aus 4 Trippeln besteht.
Auf die Version 6 (IPv6) werden wir später genau eingehen.

Tipp. Mit dem Taschenrechner von Windows kann man sehr schön Dezimalzahlen in Binärzahlen umwandeln und umgekehrt.

1. Welche IP-Adresse hat mein PC?

Windowse:

Grafisch: Rechter Mausklick auf Netzwerkumgebung....o. ä.
(Problem die Anzeige kann stimmen, muss sie aber nicht, vor allem dann wenn man sie oft ändert)

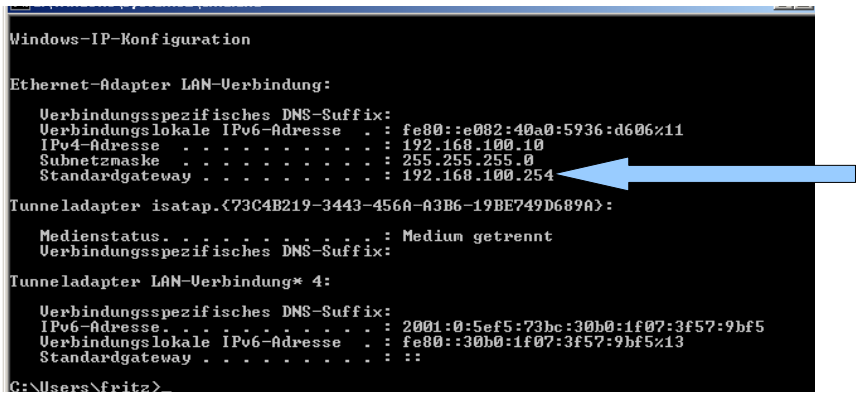
Konsole: (Start => Auführen => cmd)
ipconfig, bzw. ipconfig /all (gibt wesentlich detailierte Informationen aus, aber dazu später mehr)

Linuxe:

Grafisch: je nach GUI (Problem er Anzeige kann stimmen, muss sie aber nicht, vor allem dann wenn man sie oft ändert)

Konsole: ifconfig

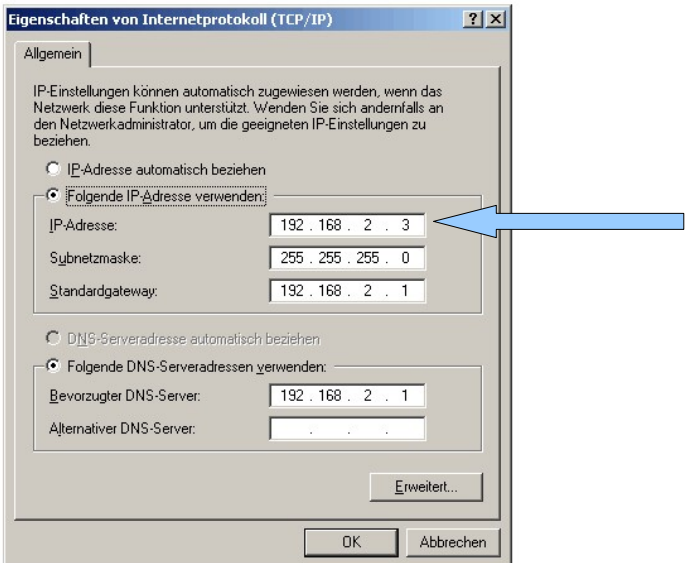
Hier eine Ansicht bei Windows 7



2. Wie erhalte ich meine IP-Adresse?

2.1. manuell

2.1.1. bei Windowsen (normalerweise nur grafisch)



Wie man sieht muss man hier noch zusätzliche Informationen eintragen, doch dazu später.

2.1.2. bei Linuxen

- entweder über die verschiedenen grafischen Werkzeuge, die es gibt, oder über die
- Konsole: mit dem Befehl:

ifconfig eth0 192.168.2.3/24

2.2. automatisch

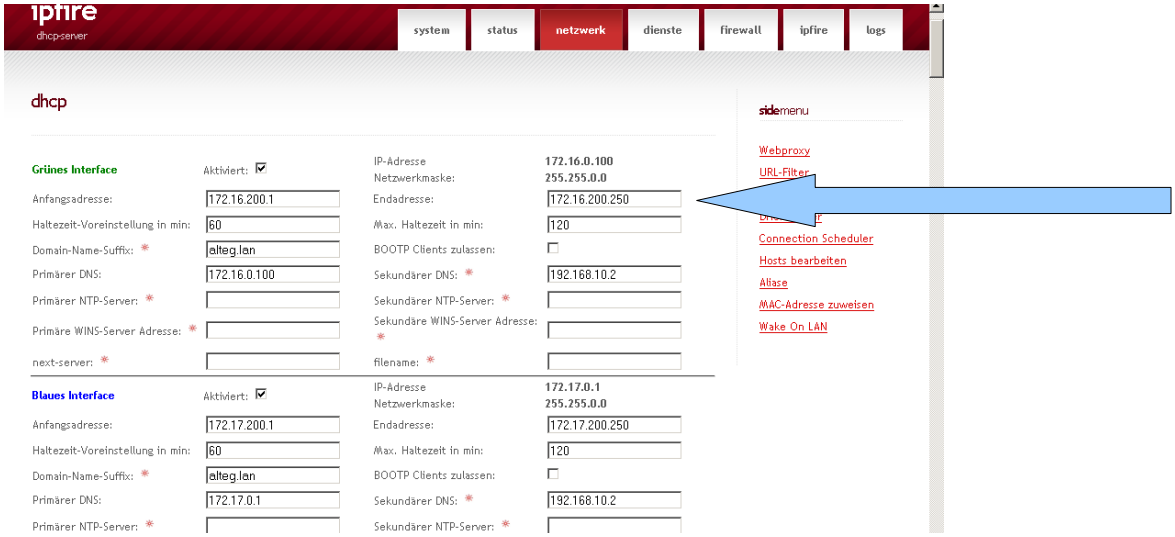
Dazu benötigt man jedoch einen PC, der den Serverdienst DHCP (Dynamic-Host-Configuration-Protocol) anbietet.

Wenn also so ein „Server“ vorhanden ist, verteilt er die IP-Adressen an die einzelnen PCs, Drucker, etc.....
Allerdings hat der DHCP-Server nun zwei Möglichkeiten IP-Adressen zu vergeben:

2.2.1. dynamische Zuordnung

Hierbei vergibt der DHCP-Server aus einem Pool von IP-Adressen jedem PC der eine Anfrage verlangt eine beliebige IP-Adresse. Diese IP-Adresse darf der PC solange behalten, wie es die „LEASE-Time“ vorsieht, danach verlangt der PC erneut eine Adresse.

Problem: heute habe ich diese IP-Adresse- morgen wieder eine andere...
Vor allem bei netzwerkfähigen Druckern ist das ein großes Problem.

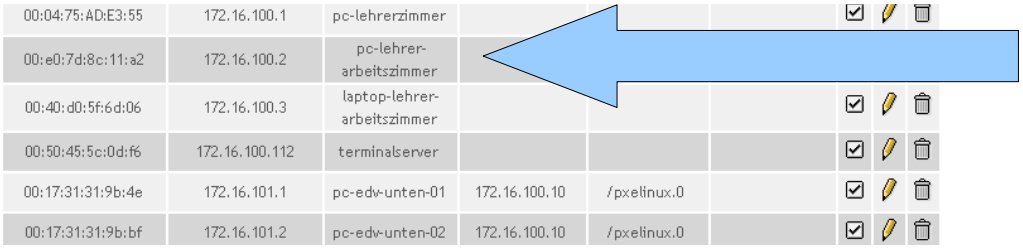


Backenend eines DHCP-Servers (IP-Fire / IP-Cop)

2.2.1. statische Zuordnung

Hier hat der DHCP-Server die Aufgabe einem PC bei einer Anfrage immer wieder die gleiche IP-Adresse zu vergeben.
Der DHCP-Server erkennt bei der Anfrage des PCs dessen MAC-Adresse und gibt ihm entsprechend seiner Liste immer wieder die gleiche IP-Adresse:

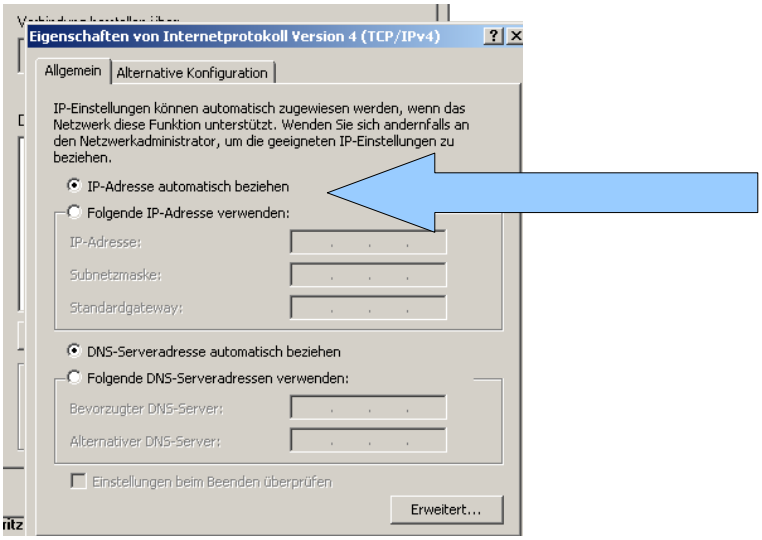
Backend eines DHCP-Servers (IP-Fire / IP-Cop)



00:04:75:AD:E3:55	172.16.100.1	pc-lehrerzimmer			
00:e0:7d:8c:11:a2	172.16.100.2	pc-lehrer-arbeitszimmer			
00:40:d0:5f:6d:06	172.16.100.3	laptop-lehrer-arbeitszimmer			
00:50:45:5c:0d:f6	172.16.100.112	terminalserver			
00:17:31:31:9b:4e	172.16.101.1	pc-edv-unten-01	172.16.100.10	/pxelinux.0	
00:17:31:31:9b:bf	172.16.101.2	pc-edv-unten-02	172.16.100.10	/pxelinux.0	

2.3. Wie bringe nun meinem PC bei, dass er eine IP-Adresse vom DHPC-Server bekommt?

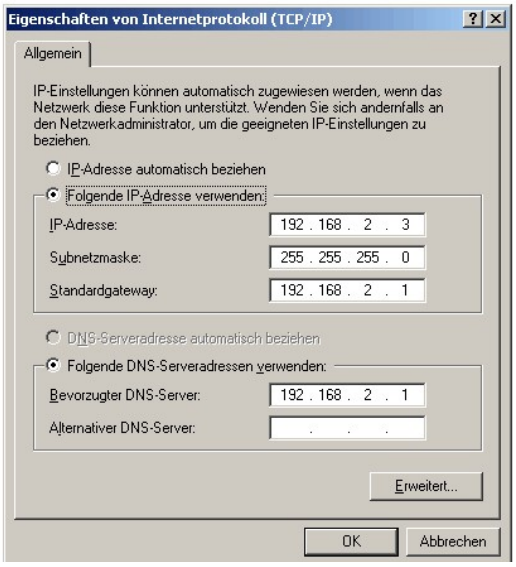
2.3.1. bei Windowsen:



2.3.2. bei Linuxen: auf der Konsole: dhclient

Hinweis:
Stellt ein PC eine Anfrage, dass er eine IP-Adresse von einem DHCP-Server erhalten möchte und er bekommt jedoch keine (DHCP-Server abgeschaltet, Netzkabel entfernt) so erhält der PC eine APIPA -Adresse. (*Automatic Private IP Addressing*) aus dem Adressraum 169.254.0.0/16 (also irgendwas mit 169).

2.4. Was hat es aber mit der Subnetmaske; dem DNS-Eintrag und dem Gateway auf sich?



2.4.1. Subnetmask

Eine IP-Adresse enthält einen Netzanteil und einen Hostanteil.

Der Netzanteil besagt in welchem Netz sich der PC befindet.
Der Hostanteil ist dann ein bestimmter Computer im Zielnetz.

Die Trennung von Netz- und Hostanteil erfolgt mit Hilfe der Subnetzmaske.

Wird der IP-Adresse 194.95.162.121 die Subnetzmaske 255.255.255.0 zugeordnet, so bedeutet dies, dass sich der Computer im Netz 194.95.162.0 befindet und die "Hausnummer" 121 besitzt.

Eine Netzmaske ist genau so lang wie eine IPv4-Adresse, also 32 Bit. Alle Bits des Netzwerkteils sind auf 1 gesetzt, alle Bits des Hostanteils haben den Wert 0.

```
IPv4-Adresse          11000000 10101000 00000001 10000001
Netzmaske             11111111 11111111 11111111 00000000
```

Die Netzwerkmaske wird als Dezimalzahl 255.255.255.0 geschrieben,

Computer, die sich im gleichen Netzwerk befinden, können problemlos miteinander kommunizieren. Dies ist mit dem Telefonnetz vergleichbar, eine Stadt hat eine Vorwahl, Bewohner dieser Stadt können ohne Vorwahl kommunizieren.

Computer in unterschiedlichen Netzwerken benötigen einen Router, der die Signale von einem Netzwerk in das andere Netzwerk weiterleitet, aber dazu später.
Um also von einer Stadt in eine andere Stadt zu telefonieren benötigt man eine Vorwahl (Netzanteil) und eine Vermittlungsstelle (Router).

2.4.1.1. herkömmliche Klassenschreibweise

Man unterscheidet verschiedene Standardnetzwerkklassen:

Netzklasse	Präfix	Adressbereich	Netzmaske	Netzlänge (mit Präfix)	Netzlänge (ohne Präfix)	Hostlänge	Netze	Hosts pro Netz
Klasse A	0...	0.0.0.0 – 127.255.255.255	255.0.0.0	8 Bit	7 Bit	24 Bit	128	16.777.214
Klasse B	10...	128.0.0.0 – 191.255.255.255	255.255.0.0	16 Bit	14 Bit	16 Bit	16.384	65.534
Klasse C	110...	192.0.0.0 – 223.255.255.255	255.255.255.0	24 Bit	21 Bit	8 Bit	2.097.152	254
Klasse D	1110...	224.0.0.0 – 239.255.255.255	Verwendung für Multicast-Anwendungen					
Klasse E	1111...	240.0.0.0 – 255.255.255.255	Reserviert für Forschung					

(Auf E Klassen werden wir nicht eingehen)

2.4.1.2. CIDR

Die Klasseneinteilung ist jedoch veraltet! Sie wird jedoch in LAN der Einfachheit meist genutzt.
Prinzipiell kann nämlich der Host bzw. Netzanteil variabel sein und muss nicht dem Schema 255.255.255.0 (C) bzw. 255.255.0.0. (B) oder 255.0.0.0 (A) entsprechen.
Daher wurde die CIDR-Notation **Classless Inter-Domain Routing** (CIDR) eingeführt
Hier wird an die IP-Adresse der Netzanteil mit Schrägstrich als Bitanzahl angehängt:

192.168.100.4/24 => /24 bedeutend, die ersten 24 Bits sind auf 1 gesetzt also ist dies das Netz und (192.168.100.0) und der Host hat die „Nummer“ 4.

Eine Übersicht

Notation	Adressen	Subnetzmaske dezimal	Subnetzmaske binär	Kommentar
/8	16777216	255.0.0.0	11111111.00000000.00000000.00000000	„Class A“-Größe
/9	128x65536	255.128.0.0	11111111.10000000.00000000.00000000	
/10	64x65536	255.192.0.0	11111111.11000000.00000000.00000000	
/11	32x65536	255.224.0.0	11111111.11100000.00000000.00000000	
/12	16x65536	255.240.0.0	11111111.11110000.00000000.00000000	
/13	8x65536	255.248.0.0	11111111.11111000.00000000.00000000	
/14	4x65536	255.252.0.0	11111111.11111100.00000000.00000000	
/15	2x65536	255.254.0.0	11111111.11111110.00000000.00000000	
/16	1x65536	255.255.0.0	11111111.11111111.00000000.00000000	„Class B“-Größe
/17	128x256	255.255.128.0	11111111.11111111.10000000.00000000	
/18	64x256	255.255.192.0	11111111.11111111.11000000.00000000	
/19	32x256	255.255.224.0	11111111.11111111.11100000.00000000	
/20	16x256	255.255.240.0	11111111.11111111.11110000.00000000	
/21	8x256	255.255.248.0	11111111.11111111.11111000.00000000	
/22	4x256	255.255.252.0	11111111.11111111.11111100.00000000	
/23	2x256	255.255.254.0	11111111.11111111.11111110.00000000	
/24	1x256	255.255.255.0	11111111.11111111.11111111.00000000	„Class C“-Größe
/25	128x1	255.255.255.128	11111111.11111111.11111111.10000000	
/26	64x1	255.255.255.192	11111111.11111111.11111111.11000000	
/27	32x1	255.255.255.224	11111111.11111111.11111111.11100000	
/28	16x1	255.255.255.240	11111111.11111111.11111111.11110000	
/29	8x1	255.255.255.248	11111111.11111111.11111111.11111000	
/30	4x1	255.255.255.252	11111111.11111111.11111111.11111100	
/31	2x1	255.255.255.254	11111111.11111111.11111111.11111110	
/32	1x1	255.255.255.255	11111111.11111111.11111111.11111111	einzelner Host

In einem realen Netz entfallen zwei Hostadressen
Ein Netz wird mit 0 angegeben, z. B. 192.168.100.0. Ein PC kann also niemals die Nummer 0 haben, genauso wenig kann er die Nummer 255 (192.168.100.255) haben, das diese Nummer ein Broadcastadresse ist, auf die wir hier aber nicht eingehen werden.

2.4.2. Gründe für Subnetting:

- Trennen von Netzwerken unterschiedlicher Topologie
- Trennen von Netzwerken nach Standorten, Gebäuden und Etagen
- Trennen von Netzwerken nach Abteilungen und Bereichen
- Trennen von sensitiven Bereichen vom Hauptnetz
- Trennen des Netzwerks in logische Arbeitsgruppen
- Trennen des Netzwerks zur Reduzierung des Verkehrsaufkommens

Vorteil von Subnetting:

- Flexibilität bei der Adressierung für den Administrator.
- Broadcast-Unterteilung. !!
- Höhere Sicherheit des LANs.

Für die Berechnungen
http://www.subnet-calculator.com/

bzw. CIDR
http://www.subnet-calculator.com/cidr.php

Besser für die Veranschaulichung jedoch
http://jodies.de/ipcalc

ok sind auch
http://www.subnetmask.info/
und
http://www.subnetonline.com/pages/subnet-calculators/ip-subnet-calculator.php
(hier auch rechts im Menü den Rest beachten).

2.4.3. Spezielle IP-Adressen

Private Adressen
Bestimmte IP-Adressen sind für die Nutzung im LAN vorgesehen. Diese privaten IP-Adressen stehen weltweit allen Nutzern zur Verfügung. Da eine IP-Adresse immer eindeutig sein muss, dürfen diese Adressen nicht im Internet verwendet werden. Router, welche für die Weiterleitung von IP-Paketen zuständig sind, leiten Pakete mit privater IP-Adressierung nicht weiter.

Multicast-Adressen
Bei Audio- und Videoübertragungen kommen häufig Multicast-Adressen zum Einsatz. Die Nachrichten werden von einem Punkt aus zu einer Gruppe von Geräten gesendet. Ähnlich wie beim Rundfunk.

Loopback-Adressen
Mit der Loopback-Adresse 127.0.0.1 kann die Funktionalität der eingebauten Netzwerkkarte getestet werden. Die Daten gelangen nicht ins physikalische Netz, sondern bleiben auf dem lokalen Computer.

Rundspruchadressen - Broadcasts
Die Kommunikation im Netzwerk erfordert es auch Rundspruch-Nachrichten an alle Geräte im Netzwerk zu senden. Broadcasts werden von Routern nicht an andere Netze weitergeleitet. Innerhalb eines Netzes spricht man deshalb von einer Broadcast-Domäne.

Private IP-Adressen [1]

Class A:	10.0.0.0 - 10.255.255.255	1 Netz	16 Mio Hosts pro Netz
Class B:	172.16.0.0 - 172.31.255.255	16 Netze	65534 Hosts pro Netz
Class C:	192.168.0.0 - 192.168.255.255	256 Netze	254 Hosts pro Netz

Multicast-Adressbereich [2]

Class D: 224.0.0.0 - 239.255.255.255

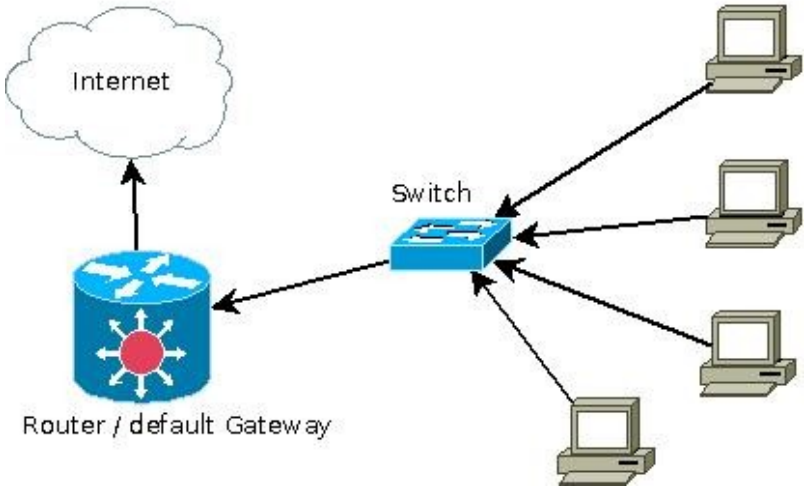
Loopback-Adressbereich [3]

Class A: 127.0.0.1

Für einige dieser speziellen Privaten-Adressen laufen Anträge um sie öffentlich freizugeben, da der IPv4 Adressraum zu klein ist. (Dazu später mehr bei Ipv6).

2.4.4. Was ist nun der Default-Gateway?

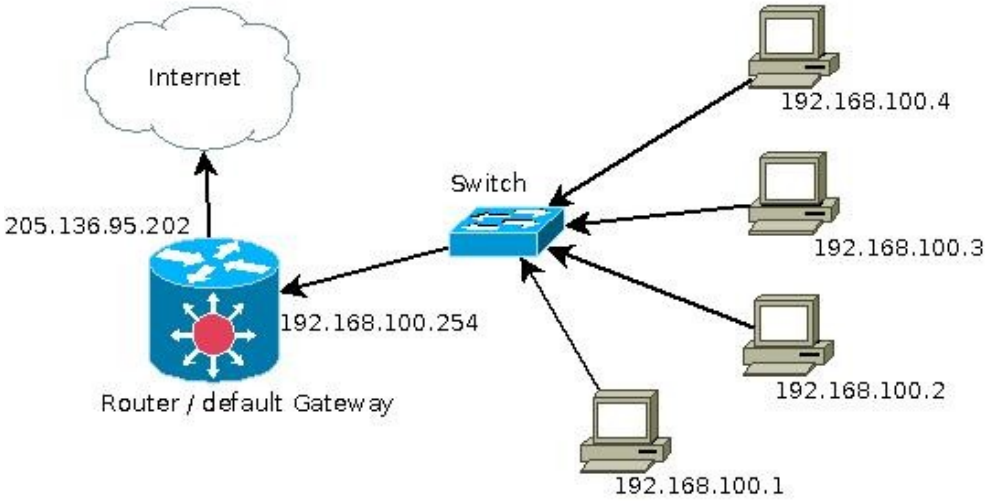
Situation: Mehrere PCs aus einem Lan wollen ins Internet



Hierfür wird ein Router / Gateway benötigt.Diese werden häufig als Schnittstelle zum Internet eingesetzt. Sie sind über eine WAN-Schnittstelle (ISDN / DSL / ...) mit dem Internet Provider verbunden. Nach dem Verbindungsaufbau wird der WAN-Schnittstelle des Routers in der Regel eine dynamische IP-Adresse aus dem Pool des Internet Service Providers zugewiesen.

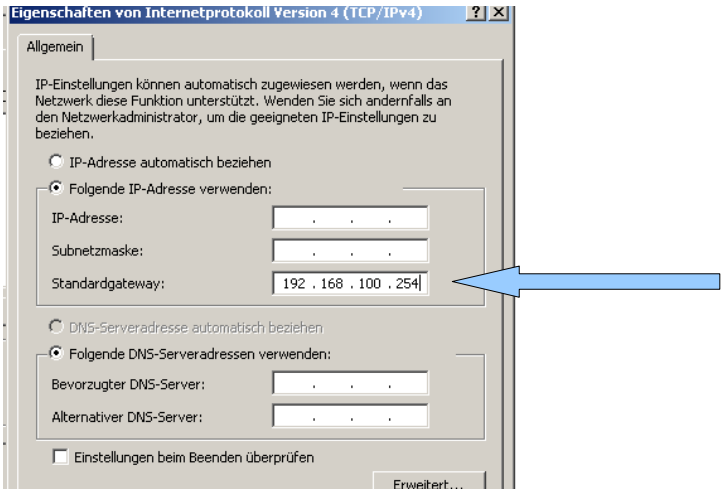
Auf der LAN-Seite ist der Router über eine Ethernet- oder FastEthernet-Schnittstelle mit dem LAN verbunden. Der Router kommuniziert mit dem LAN in der Regel über einen Switch. Die LAN-Schnittstelle wird mit einer IP-Adresse aus dem Bereich des LAN konfiguriert.

Wenn einer der PCs aus dem LAN eine URL aus dem Internet anfragt, wird die Anfrage über die LAN-Schnittstelle zur WAN-Schnittstelle des Routers und von dort an das Internet weitergegeben. Dabei wird nur die WAN-IP-Adresse des Routers als Antwortadresse übermittelt. Die eingehende Antwort wird vom Router über die LAN-Schnittstelle an den entsprechenden PC (zurück) geroutet.



2.4.4.1. Eintrag Gateway beim PC

bei Windows:



bei Linux:

Entweder mit der GUI oder
route add default gw 192.168.100.254

3. Funktionsweise NAT/PAT (Ports)
(Network-Adress-Translation / Port Adress-Translation)

Vorher müssen wir jedoch noch kurz etwas Einfügen: Ports

- jeder PC hat zwar seine IP-Adresse, gleichzeitig hat er aber auch Ports (Türchen)

- Diese Ports sind in udp und tcp Netzwerken 16 Bit groß, so dass es dezimal die Port von 0 bis 65535 gibt.

- Die Ports von 0 bis 1023 sind sogenannte privilegierte (*Well-Known*) Ports.
d. h. von der IANA (Internet Assigned Numbers Authority) einheitlich festgelegt.
- Von Port 1024 bis 49151 befinden sich die *Registered Ports*. Anwendungshersteller können bei Bedarf Ports für eigene Protokolle registrieren lassen, ähnlich wie Domainnamen. Die Registrierung hat den Vorteil, dass eine Anwendung anhand der Portnummer identifiziert werden kann, allerdings nur wenn die Anwendung auch den bei der IANA eingetragenen Port verwendet.

- Die restlichen Ports von Portnummer 49152 bis 65535 sind so genannte *Dynamic* und/oder *Private Ports*. Diese lassen sich variabel einsetzen, da sie nicht registriert und damit keiner Anwendung zugehörig sind.

Die nachfolgende Liste ist eine kleine Auswahl bekannter Ports.

Portnummer	Dienst	Beschreibung
7	Echo	Zurücksenden empfangener Daten
20	FTP-Data	Dateitransfer (Datentransfer vom Server zum Client)
21	FTP	Dateitransfer (Initiierung der Session und Senden der FTP-Steuerbefehle durch den Client)
22	SSH	Secure Shell
23	Telnet	Terminalemulation
25	SMTP, ESMTP	E-Mail-Versand
53	DNS	Auflösung von Domainnamen in IP-Adressen
80	HTTP	Webserver
110	POP3	Client-Zugriff für E-Mail-Server
143	IMAP	Client-Zugriff für E-Mail-Server
443	HTTPS	sicherer Webserver
548	AFP over IP	Datei- und Druckdienste (Mac OS und Mac OS X)
993	IMAPS	sicherer Client-Zugriff für E-Mail-Server
3050	Firebird	Zugriff auf Firebird-Datenbanken
3306	MySQL	Zugriff auf MySQL-Datenbanken
3389	RDP	Windows Remotedesktopzugriff, Windows Terminal Services
5432	PostgreSQL	Zugriff auf PostgreSQL-Datenbanken
8080	alternativer HTTP Port	Webserver

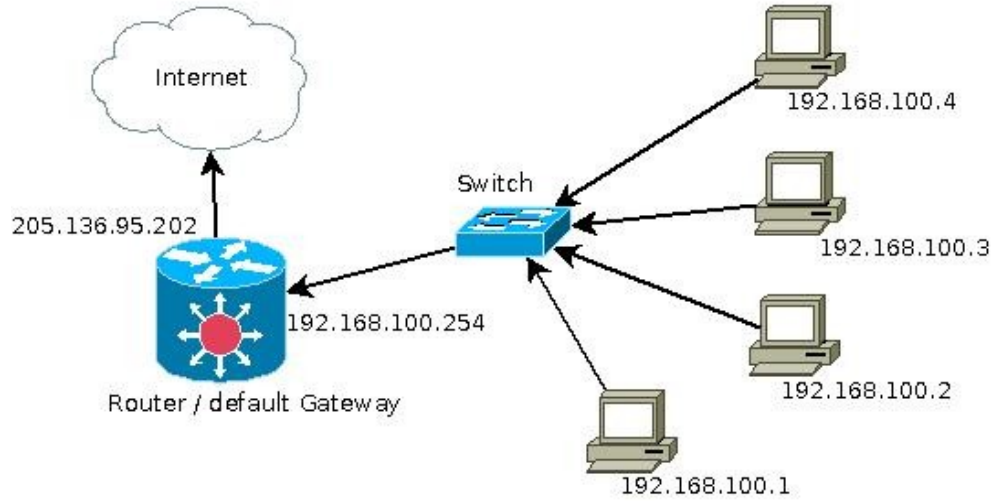
Eine Übersicht über alle Ports findet man unter:
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
PS: Jeder PC hat eine Datei „services“ in der diese Port gespeichert sind.

Man findet diese Datei unter Windows => system32 => drivers => etc => services
bei Linux direkt unter /etc/services

```
# Copyright (c) 1993-2004 Microsoft Corp.
#
# This file contains port numbers for well-known services defined by IANA
#
# Format:
#
# <service name>  <port number>/<protocol>  [aliases...]   [#<comment>]
#

echo              7/tcp
echo              7/udp
discard           9/tcp    sink null
discard           9/udp    sink null
systat           11/tcp    users               #Active users
systat           11/udp    users               #Active users
daytime          13/tcp
daytime          13/udp
qotd             17/tcp    quote               #Quote of the day
qotd             17/udp    quote               #Quote of the day
chargen          19/tcp    ttytst source       #Character generator
chargen          19/udp    ttytst source       #Character generator
ftp-data         20/tcp                        #FTP, data
ftp              21/tcp                        #FTP. control
ssh              22/tcp                        #SSH Remote Login Protocol
telnet           23/tcp
smtp             25/tcp    mail                #Simple Mail Transfer Protocol
time             37/tcp    timserver
time             37/udp    timserver
rlp              39/udp    resource            #Resource Location Protocol
nameserver       42/tcp    name                #Host Name Server
nameserver       42/udp    name                #Host Name Server
nicname          43/tcp    whois
domain           53/tcp                        #Domain Name Server
domain           53/udp                        #Domain Name Server
tftp             69/udp                        #Trivial File Transfer
http             80/tcp    www www-http        #World Wide Web
```

3.1. Wie funktioniert nun der Aufruf einer Internet-Seite bei NAT/PAT



PC1 (192.168.100.1) stellt folgende Anfrage: Ich möchte die Webseite von www.netzmafia.de betrachten.

http://www.netzmafia.de hat die IP 129.187.206.160
(Praktischer Test: Browser: http://129.187.206.160) eingeben

Schritte:
- PC1 versendet über einen freiten Port (4321) den Seitenaufruf an den Default-Gateway (denn PC1, weiß ja nicht wo dieser Web-Server ist)

- Der Router / Default-Gateway empfängt nun vereinfacht dargestellt ein Paket von 192.168.100.1:4321 und er soll dieses Paket an 129.187.206.160:80 (Web) weiterleiten.

- Der Router trägt diese Anfrage in eine Tabelle ein um sich dies zu merken.

- Nun tauscht der Router die Absender-Adresse 192.168.100.1 gegen seine eigene öffentliche Adresse 205.136.95.202 aus. (NAT)

- Dann schaut der Router nach, welchen Port er frei hat. z. B. 5555 und tauscht nun auch den Quellport 4321 gegen den 5555 Port aus (PAT)

- Die ausgetauschte IP-Adresse und den ausgetauschten Port trägt der Router wieder in seine Tabelle ein.
192.168.100.1:4321 ausgetauscht gegen 205.136.95.202:5555 Ziel 129.187.206.160:80

- Danach versendet der Router die Anfrage an den entsprechende Webserver.
(Woher der Router weiß wo und wie der Web-Server zu erreichen ist klären wir später)

- Der Web-Server antwortet und gibt dem Absender (Router) die angeforderten Informationen.
- Der Router erhält als nun ein Antwortpaket, dass an ihn selbst und an seinen Port adressiert ist.

- Er schaut nun in seine Tabelle nach
Ich erhalte ein Paket von 129.187.206.160:80 und das kommt bei mit bei 5555 rein, laut meiner Tabelle muss es an PC 192.168.100.1:4321 weitergeleitet werden.

- Der Router tauscht nun wieder im Header des Datenpakets IP-Adresse und Port aus, so dass es nun der entsprechende PC auf seinem Port 4321 die Antwort erhält.

- Zum Schluss löscht der Router den Eintrag aus seiner Tabelle

Dieser Vorgang wird also IP-Masquerading, NAT/PAT, dynamisches Source NAT genannt. Es gibt zwar noch weitere NAT-Techniken z. B. Static NAT etc. aber diese sind für uns nicht von Bedeutung.

3.1.1. Vor und Nachteile von NAT/PAT

Vorteile:
- Viele, viele PC in einem LAN erhalten über einen Router Zugang ins Internet.
- Für dieses LAN wird nur eine einzige öffentliche IP-Adresse benötigt. (Knappheit von Ipv4)
- der Router dient zugleich als Firewall da er nach außen ins Internet nur die benutzen Ports offen hält. Ein „böses“ Datenpaket gelangt somit nicht sofort zum Zielrechner sondern zum Router, und wenn der nicht weiß für wen im LAN es bestimmt ist, wirft er es einfach weg.
- eine gewisse Anonymität im LAN

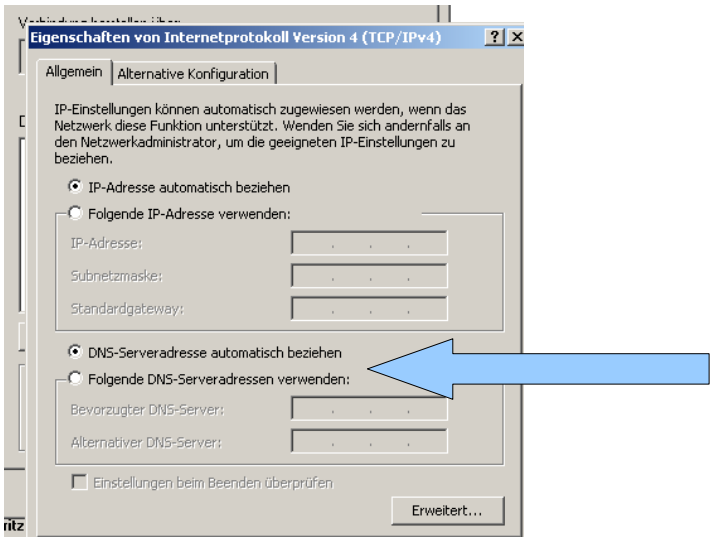
Nachteile:
- Man ist selbst von außen aus dem Internet nicht direkt erreichbar (Tauschbörsen)
- Der Router braucht Arbeitsspeicher für seine Tabelle, wenn hier 150 PC gleichzeitig surfen und jeweils viel agieren benötigt der Router entsprechend viel RAM. Home-Router stoßen hier bei 100 PC oft an ihre Grenzen. Daher gibt es billigere und teure Router.
- Probleme von Sprachpakete über den Router (Internettelefonie), da das NAT/PAT trotz QoS Zeit beansprucht (QoS bedeutet Quality of Service, Sprachpakete werden bevorzugt behandelt)
- Probleme bei der Strafverfolgung, da die Polizei zwar weiß, dass das Übel vom Router (seiner öffentlichen IP-Adresse) ausging, doch wer im LAN der Übeltäter war ist somit unklar, wenn der Router dies nicht protokolliert.

Blick auf seine Tabelle im Router (Grafisch abgewandelt, nicht mit allen Infos)

Legende : LAN | INTERNET | DMZ | Wireless | IPFire | VPN | OpenVPN

Quell-IP:Port		Ziel-IP:Port		Protokoll	Verbindung Status	Ablaufdatum (sek.)
				Alle icmp udp tcp	AlleSYN_SENTSYN_RECVESTABLISHEDFIN_WAITCLOSE_WAITLAST_ACKTIME_WAITCLOSELISTEN	
84.146.87.178	49674	192.168.10.10	444 (SNPP)	tcp	ESTABLISHED	119:59:59
84.146.87.178	49672	192.168.10.10	444 (SNPP)	tcp	ESTABLISHED	119:59:58
192.168.10.10	36348	212.162.62.43	80 (HTTP)	tcp	ESTABLISHED	112:14:35
192.168.10.10	51695	212.162.62.43	80 (HTTP)	tcp	ESTABLISHED	112:13:41
172.16.0.100	800 (MDBS_DAEMON)	172.16.100.111	15618	tcp	ESTABLISHED	112:12:19
172.16.0.100	800 (MDBS_DAEMON)	172.16.100.111	55877	tcp	ESTABLISHED	110:44:27
172.16.0.100	800 (MDBS_DAEMON)	172.16.100.111	35333	tcp	ESTABLISHED	110:29:54
172.16.0.100	800 (MDBS_DAEMON)	172.16.100.111	35597	tcp	ESTABLISHED	91:54:36
172.16.0.100	800 (MDBS_DAEMON)	172.16.100.111	64253	tcp	ESTABLISHED	91:54:06
127.0.0.1	55304	127.0.0.1	444 (SNPP)	tcp	TIME_WAIT	0:01:35
172.16.100.5	138 (NETBIOS-DGM)	172.16.255.255	138 (NETBIOS-DGM)	udp		0:00:12
84.146.87.178	49673	192.168.10.10	444 (SNPP)	tcp	CLOSE	0:00:02

4. Und was macht nun der DNS-Server?



- der User an PC möchte die Webseite von www.netzmafia.de betrachten, woher weiß nun der PC, an welche IP-Adresse er seine Anfrage stellen soll?

- Er stellt seine Anfrage an einen DNS-Server (Domain-Name-Service)

- Er richtet seine Anfrage also über Port 53 an den Nameserver 194.25.2.129 von T-online
- Dieser schaut nun in seiner Datenbank nach welche IP-Adresse die Seite www.netzmafia.de hat

- Nun gibt er dem PC die Antwort: 129.187.206.160

- Jetzt benutzt der Browser (Anwendung) diese IP-Adresse

Hinweis: Oft stellt der Router selbst eine gecacheten DNS-Server zur Verfügung. Wenn dieser nicht auflösen kann, frägt er den DNS-Server des Providers (dessen Adresse hat er bei der Einwahl erhalten), sollte der dies auch nicht wissen geht es einen DNS-Server in Frankfurt und wenn der das auch nicht weiß an einen der 13 Root-DNS-Server

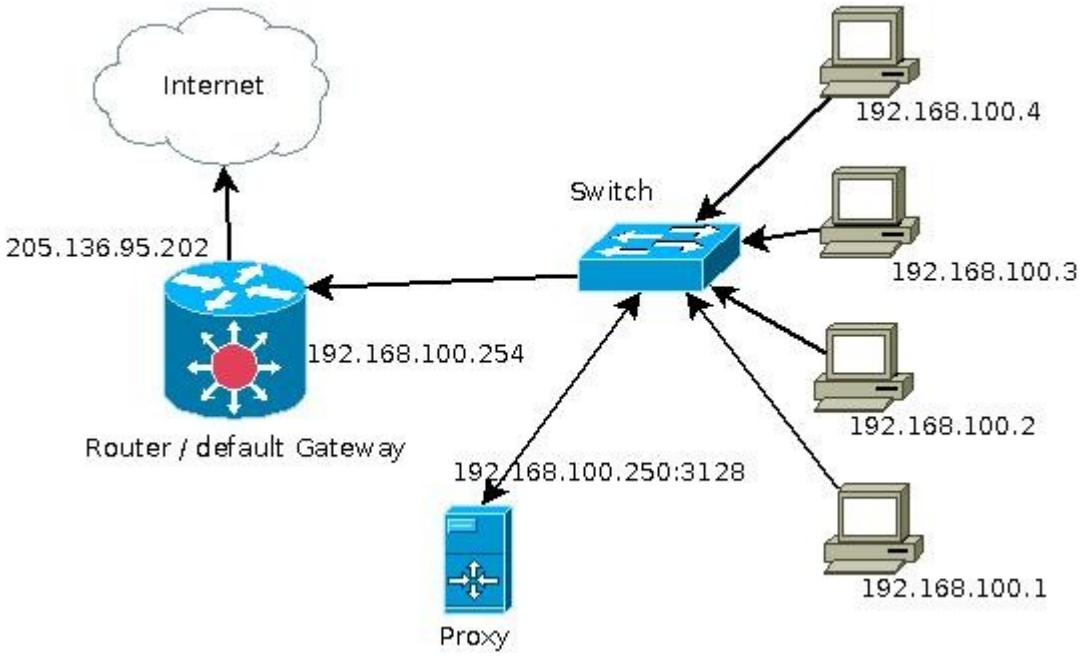
Praktisch jeder ans Internet angeschlossene Rechner bekommt einen Nameserver zugewiesen, der eindeutige Namen wie „wikipedia.org“ (die Domäne) auf technische Nummern (die IP-Adresse) übersetzen kann. Hat der Nameserver keine Information zur angefragten Adresse (in diesem Fall „org“), verweist er an die Root-Server. Dort werden die für „org“ zuständigen Nameserver abgefragt. Bei den org-Nameservern wiederum werden die für „wikipedia.org“ verantwortlichen Nameserver erfragt und dort schließlich die IP-Adresse von „wikipedia.org“.

- eine Liste der Root-DNS-Server findet man unter:
  http://de.wikipedia.org/wiki/DNS_Root_Nameserver

- Eine Liste von Nameservern findet man z. B. auf http://www.stanar.de/

- Eine Liste unzensierter (Kinderpornografie) DNS-Server findet man unter
  http://wiki.ak-zensur.de/index.php/Unzensierte_DNS_Server
  (Wie schwachsinnig ist das?)

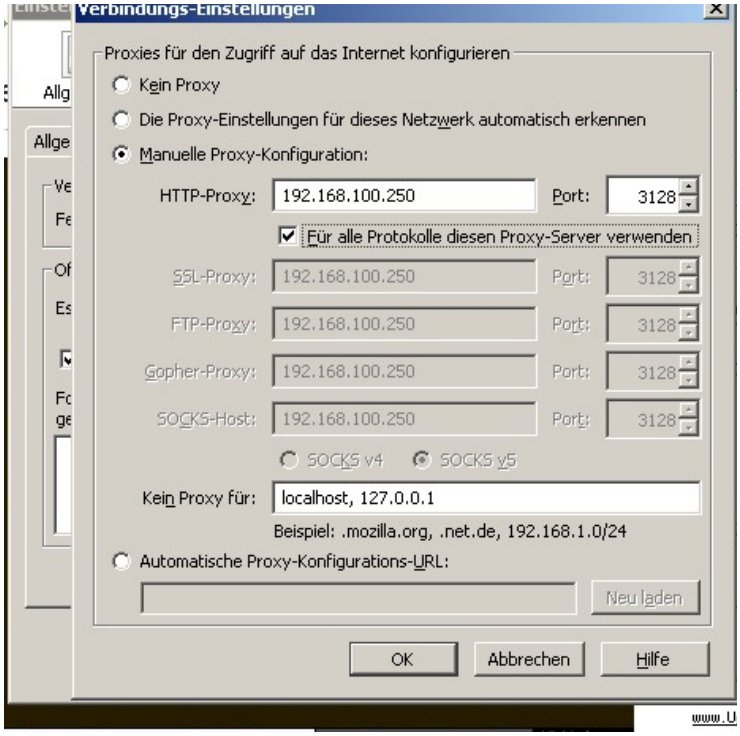
5 Und was macht nun ein Proxy?
5.1. nicht transparenter Proxy



- Es gibt Proxy-Dienste für verschiedene Applikationen: z. B. Browser, Mail, Ftp, etc.

Wir gehen hier nur auf einen Proxy für Browser ein:

- Die Netzwerkkonfiguration der PCs bleibt unverändert, die PCs können auch „Surfen“, aber wir verändern jetzt im Browser die Einstellung, dass der PC einen Proxy-Server benutzen soll.



Was passiert nun beim Surfen?

- man gibt im Browser die Adresse ein.
- Der DNS-Server wird abgefragt und die Domain aufgelöst. (Die alles geht über den Router , wie bisher)
- Der Browser kontaktiert nun den Proxy-Server und teilt ihm mit welche Seite er besuchen möchte.
- Der Proxy-Server schaut in seinem Cache nach, ob er die angeforderte Seite bereits vorrätig hat, wenn ja gibt er sie sofort an den PC, wenn nein, holt sich der Proxy selbst die Seite aus dem Internet, legt sie in seinen Cache und gibt sie dann dem PC weiter.

Warum also einen Proxy?

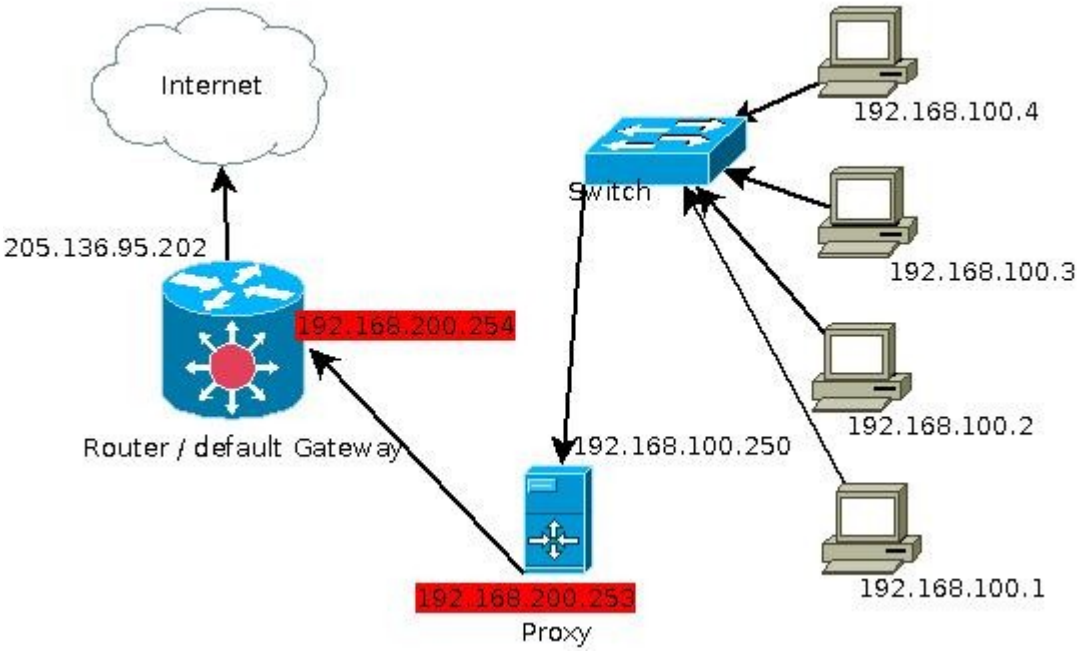
Vorteile:

-Bei langsamer Internetverbindung muss kann er bereits abgefragt Seiten aus dem Cache anbieten, interessant, wenn mehrere Leute gleichzeitig auf eine Web-Seite gehen, so wird sie nur einmal aus dem Internet geladen.

- Der Proxy kann „Filtern“
Wer darf (auch mit Benutzeranmeldung)
Wann darf man
Mit was darf man (IE, Firefox)
Wohin darf man /darf man nicht
Welche Daten / Filme/ Bilder … darf der Empfänger erhalten
usw. , auch natürlich in Kombination

Nachteil:
- ein Klick und man umgeht den Proxy!!!!!
- Alle Browser müssen konfiguriert werden!!!!
=> daher gibt gibt es noch die transparenten Proxy-Server

5.2. transparenter Proxy



Was hat sich geändert?

- der Proxy hat nun eine zweite Netzwerkkarte und ist nun in einem Netzwerk mit dem Router. (192.168.200.0)

- die einzelnen PCs müssen als default Gateway (evtl. DNS-Server) die Adresse des Proxy-Server eintragen, bzw. erhalten diese Infos von einem DHCP-Server.

- An den Browsern wird kein Proxy eingestellt (default Einstellung)

- Der Proxy dient nun auch als DNS-Proxy

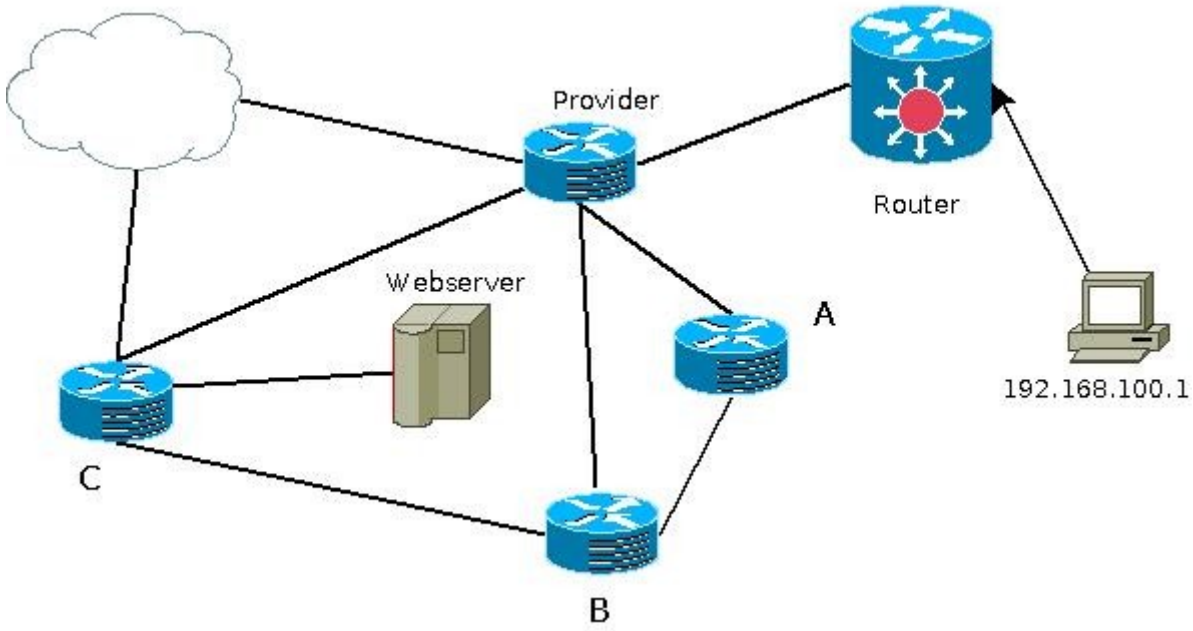
- Alle Surfaktionen, Mail-Versand, etc. müssen nun über den Proxy gehen. Daher ist dies meist ein DNS-Proxy, Web-Proxy, Mail-Proxy, Ftp-Proxy etc. in einem Paket.

Funktion: Der Proxy fängt alle Abfragen an bestimmten Ports ab und leitet sie dann an den Proxy-Dienst weiter. Jemand möchte eine Web-Seite, so geht die Anfrage beim Port 80 rein, der Kernel des Proxy leitet dies jedoch an den Port 3128 des Proxy um.

- Vorteil:
- Der Proxy lässt sich nicht mehr so leicht mit einem „Klick“ umgehen.
- Die Browser müssen nicht konfiguriert werden.

Nachteil:
- Es kann bei einem transparenten Proxy keine Benutzeranmeldung geben.
- Bestimmte Anwendungen kommen evtl. nicht ins Internet.....

6. Und wie funktioniert jetzt die Weiterleitung von Datenpaketen im Internet?



Problem: Der PC möchte den Webserver kontaktieren.

Woher weiß nun der Provider-Router, wie das Datenpaket zum Webserver gelangt? Es gibt nämlich viele Möglichkeiten:

a) Vom Provider-Router zu Router C und dann zum Webserver
b) Vom Provider-Router zu Router B von Router C und dann zum Webserver
c) Vom Provider-Router zu Router A von Router B zu Router C und dann zum Webserver
d) Vom Provider-Router zur Wolke und dann irgendwie zu Router C und dann zum Webserver

Router A hat zwei IP-Adressen
Router B hat drei IP-Adressen
Router C hat vier IP-Adressen

Jeder Router teilt dem benachbarten Router mit welche IP-Adressen (Netze) er hat bzw. er schon von Nachbar Router kennt.
Somit lernt der Provider Router nach einiger Zeit über welchen Weg er das Datenpaket verschicken kann.

- Die Router im Internet verständigen sich über sogenannte Routing-Protokolle miteinander.

Hier gibt es verschiedene Protokolle, hier möchten wir nur zwei Vorstellen:

a) das altertümliche RIP (Routing Information Protocol) => es benutzt immer nur den kürzesten Weg

b) OSPF (Open Shortest Path First) => Es entscheidet auch nach Kosten und Schnelligkeit

6.1. Eine kleine Übersicht über die gängigsten Routing-Protokolle

Abhängig davon, ob ein Router Teil eines autonomen Systems ist oder gar dessen Grenze bildet, verwendet er oftmals gleichzeitig Routing-Protokolle aus verschiedenen Klassen:

- **Interior Gateway Protocols** (**IGP**s) tauschen Routing-Informationen in einem einzelnen autonomen System aus. Häufig verwendet werden:
  - IGRP/EIGRP (Interior Gateway Routing Protocol/ Enhanced IGRP)
  - OSPF (Open Shortest Path First)
  - IS-IS (Intermediate System to Intermediate System)
  - RIP (Routing Information Protocol)
- **Exterior Gateway Protocols** (**EGP**s) regeln das Routing zwischen verschiedenen autonomen Systemen. Dazu gehören:
  - BGP (Border Gateway Protocol: seit 2002 in der Version BGP4) ist heute weltweit der De-facto-Standard.
  - EGP (mit dem alten Exterior Gateway Protocol wurden früher die Internet-Backbones verbunden. Es ist inzwischen veraltet.)
- **Ad hoc Routing-Protokolle** werden in Netzen mit wenig oder keiner Infrastruktur verwendet.
  - OLSR findet meist Verwendung im mobilen Bereich.
  - AODV findet in kleineren Netzen mit hauptsächlich statischem Traffic Verwendung.

Dabei können Routingprotokolle auch miteinander interagieren.

6.2. Und was sind nun routbare Protokolle?

Kurz: alle Protokolle auch über das Internet funktionieren:
z. B. Http, ftp, pop3, smtp, telnet, ssh um hier nur die wichtigsten zu nennen.
Das heißt die Router leiten Pakete dieser Protokolle weiter, also funktionieren diese Protokolle auch über das Internet.

ABER:
Es gibt auch nicht routbare Protokolle, diese funktionieren nur innerhalb eines LANs und sie werden nicht von einem Router weitergeleitet.
Beispiel:
smb, cifs, netbios, (typische Windows Protokolle)

7. Ipv6

7.1. Warum ein neues Protokoll?

Das alte IPv4 bietet einen Adressraum von etwas über 4 Milliarden IP-Adressen mit denen Computer (oder andere Geräte) angesprochen werden können. In den Anfangstagen des Internet als es nur wenige Rechner gab die eine IP-Adresse brauchten galt dies als mehr als ausreichend.

Viele der theoretisch 4 Milliarden IP-Adressen sind in der Praxis nicht nutzbar da sie Sonderaufgaben dienen (z.B. Multicast) oder zu den privaten Adressbereichen etc. gehören.

Als Resultat herrscht besonders in Asien heute eine Adressenknappheit der man mit NAT/PAT und der dynamischen Vergabe von Adressen begegnen muss.

Hauptsächlich wegen der Adressknappheit begann man 1995 mit den Arbeiten am neuen IPv6. Folgende Liste soll einen kurzen Überblick über die wesentlichen neuen Features von IPv6 geben.

- Vergrößerung des Adressraums von 2^{32} bei IPv4 auf 2^{128} bei IPv6
- Autokonfiguration (ähnlich DHCP) Mobile IP und automatisches Renumbering
- Services wie IPSec QoS und Multicast serienmäßig
- Vereinfachung und Verbesserung der Header (wichtig für Router)

7.2. Adressaufbau von IPv6

Eine IPv6-Adresse ist 128 bit lang (IPv4: 32 bit). Damit gibt es etwa 3 4 x 10^{38} IPv6-Adressen - für jeden Quadratmeter Erdoberfläche könnten 6 5 x 10^{23} Adressen bereitgestellt werden.

IPv6-Adressen werden nicht mehr dezimal (z.B. 80.130.234.185) sondern hexadezimal mit Doppelpunkten geschrieben:
243f:6a88:85a3:08d3:1319:8a2e:0370:7344 *(8 Blöcke)*

Wenn eine 16-bit-Gruppe den Wert 0000 hat kann sie durch einen Doppelpunkt ersetzt werden.

Wenn dann mehr als 2 Doppelpunkte aufeinander folgen würden können diese auf 2 Doppelpunkte reduziert werden solange es in der resultierenden Adresse nur einmal zwei aufeinander folgende Doppelpunkte gibt.

0588:2353::1428:57ab ist also das selbe wie
0588:2353:0000:0000:0000:0000:1428:57ab aber
3906::25de::cade wäre nicht erlaubt da zweimal zwei Doppelpunkte in der Zeichenkette vorkommen - ein Computer wüsste nicht wo mit wie vielen Nullen aufzufüllen wäre.

Die ersten 64 Bit der IPv6-Adresse dienen standardmäßig der Netzadressierung die letzten 64 Bit können zur Host-Adressierung verwendet werden - hiermit implementiert man elegant das Konzept der Netzmasken von IPv4. Man kann jedoch auch andere Netzmasken verwenden.

Die korrekte Form einer IPv6-Adresse in einer URL ist
`http://[243f:6a88:85a3:08d3:1319:8a2e:0370:7344]`

Wichtig ist hier die Schreibweise mit Klammern, da sonst der Doppelpunkt den Port signalisieren würde.

7.3. Aufteilung des IPv6-Adressraums

Man unterscheidet grob gesehen zwischen globalen Adressen (Global Scope) und lokalen Adressen (Local Scope).

Pakete mit globale Adressen werden außerhalb des lokalen Netzwerks geroutet.

Link-lokale Adressen sind nur innerhalb des lokalen Netzwerks gültig. Sie werden nicht extern, sondern nur intern geroutet.

Für private lokale Netze gibt es in IPv6 reservierte Adressbereiche (Unique Local Adressses, ULA). Sie haben eine ähnliche Funktion, wie die lokalen IPv4-Adressen. Die privaten IPv6-Adressen sind weltweit eindeutig, werden aber nicht geroutet.

7.4. Adressvergabe und Autokonfiguration

IPv6 kennt zwei verschiedene Wege, wie Clients an ihre eigene IP-Adresse kommen. Entweder über DHCPv6 oder Autokonfiguration. Letzteres hat den Nachteil, das damit nur die Kommunikation im lokalen Netz möglich ist. Standard-Gateway und DNS-Server müssen immer noch manuell konfiguriert werden oder per DHCPv6 abgefragt werden.

- Stateful Address Configuration (DHCPv6)
- Stateless Address Configuration (Autokonfiguration)

Anders als bei IPv4 müssen die IP-Adressen im lokalen Netzwerk nicht zentral vergeben werden. Die Adressvergabe erfolgt automatisch und die Stationen prüfen selbständig, ob ihre Adresse im Netz schon vergeben ist. Unter IPv6 gibt es keine Netzwerkmaske und Broadcast-Adressen mehr. Die Einrichtung eines Netzwerks ist dadurch viel einfacher.

7.5. Probleme und Vorteile

Vorteile von IPv6

- IP-Autokonfiguration anhand der MAC-Adresse der Netzwerkkarte
- schnelleres Routing
- gleiche Adresse in wechselnden Netzen
- Multicast
- Quality of Service
- Datenpakete bis 4 GByte Größe
- Keine Notwendigkeit von NAT/PAT

Vieles davon war auch mit IPv4 möglich. Doch dort wurde vieles erst nachträglich implementiert. IPv6 bringt das alles integriert mit.

Nachteil:

In Deutschland gibt es nur wenige ISP, die einen Ipv6 Zugang anbieten.
Daher kaum umgesetzt, sondern nur ins Unis zum Testen verwendet.

Schwieriger zu merkende Adressen.
Weniger Anonymität da kein NAT/PAT benötigt wird => daher sind diese PCs auch direkt vom Internet erreichbar => bedingen lokale Firewalls bzw. es müssen dir Ports wesentlich sensibler geöffnet werden, als bisher unter Windows!

Kein Benutzer wird IPv6 einsetzen, bevor nicht alle URLs darüber bequem erreichbar sind. Kein ISP wird es anbieten, bevor nicht Kunden danach drängen. Kein Server wird auf IPv6 wechseln, bevor nicht wirklich viele Kunden von einem ISP damit versorgt sind. Und keine Firma wird es ohne langjährige Tests einsetzen wollen.

GNS3 | Graphical Network Simulator
GNS3, a free powerful network simulator based on Cisco IOS
Jaganelli.de - die krankeste Hompeitsch im Intanet
Jaganelli.de - die krankeste hompeitsch im Intanet
Hide NAT vs. Masquerading - Netzwerk Forum
Hide NAT vs. Masquerading - Beitrag im Netzwerk Forum
Subnetting
Subnetting Grundlagen: Was ist Subnetting, wie geht es und warum verzweifeln so viele Schüler an Subnetting-Aufgaben.
Netzwerke und mehr
Auf www.easy-network.de dreht sich alles um Netzwerke. Von der Geschichte, bis hin zu den Topologien, von LAN bis zum WLAN findet man hier alles. Wir versuchen, Laien aber auch Fortgeschrittene das Netzwerk näher zu bringen.
Netzwerke
IPv6 - Internet Protocol Version 6
Subnetz Rechner - NETWAYS GmbH
Mit dem Subnetzrechner können Sie unterschiedliche Parameter von TCP/IP Netzen berechnen lassen
IP Masquerading, PAT und NAT
NAT (Network Address Translation), PAT (Port and Address Translation) und IP Masquerading, NAPT, 1-to-n-NAT
netzwerkgrundlagen
www.different-thinking.de - Netze, Protokolle, Sicherheit
Team Unix - Howto - Netfilter und IPTables
Das Team Unix bietet FAQs und HOWTOs für jeden. Linux, C/C++ und Datensicherheit sind Hauptthema
iptables -regel ein und ausschalten [Archiv] - linuxforen.de -- User helfen Usern
[Archiv] iptables -regel ein und ausschalten Router und Netzaufbau
Tutorial IPTables
NAT mit Linux und iptables - Tutorial (Einführung)
Linux - Wegweiser für Netzwerker
Linux-Router/-Server im Eigenbau -- Routing- und Firewall-Konfiguration
Ip Assignment, Per Capita
Under IPv4 there are 4,294,967,296 possible IP addresses - each of which may be assigned to a device or computer on the internet. 4 billion addresses equates to slightly less that two thirds of an IP address per person on the planet. As you may imagine, the IP addresses are not distributed evenly around the world - they are assigned to individual countries by Regional Internet Registries such as ARIN and RIPE. We take a look at how that information breaks down per person in each country.
Ein Bild unserer Zeit: Globale IP-Adressierung | Sajonara.de - Internetmagazin
Das Internet Protokoll (engl. Internet Protocol, kurz IP) ist die Grundlage für alles das, was der Laie mit dem Internet in Verbindung bringt. Aus diesem Grund
IP-Adresse – Wikipedia
http://alp.dillingen.de/schulnetz/curriculum/
Private IP-Adresse – Wikipedia
Classless Inter-Domain Routing – Wikipedia
Netzmaske – Wikipedia
Netzklasse – Wikipedia
SubnetOnline.com - IP Subnet Calculator
IP Subnet Calculator: with an IP address and subnetmask you can calculate the number of hosts, start IP and end IP of your range, network and broadcast address and bits user for networks and hosts.

Network Address Translation – Wikipedia
Proxy (Rechnernetz) – Wikipedia
Search Results - Cisco Systems
IPv6
Peter Bieringer's Linux-Section: IPv6
    Linux IPv6 Information
Linux IPv6 HOWTO (de)
IPv6 - Theorie
Routing – Wikipedia
schild-ipv6lan.pdf (application/pdf-Objekt)
SCHNEIDER-IPv6council_2.pdf (application/pdf-Objekt)
http://www.fefe.de/ct/ipv6.txt
Einführung in IPv6 - NJH-Wiki
Protokolle - heise Netze
IPv6 für kleine Netze
Wann kommt IPv6 auf Lieber Linux
    Wann kommt IPv6 - Eintrag zu den Themen DNS, IPv4, IPv6, ISP, LAN, NAT, Tunnel bei Lieber-Linux

Praktische Übungen:

1. Wir betrachten unsere Rechnerkonfiguration mit

ipconfig

2. Wir pingen unseren Rechner mit
ping 127.0.0.1

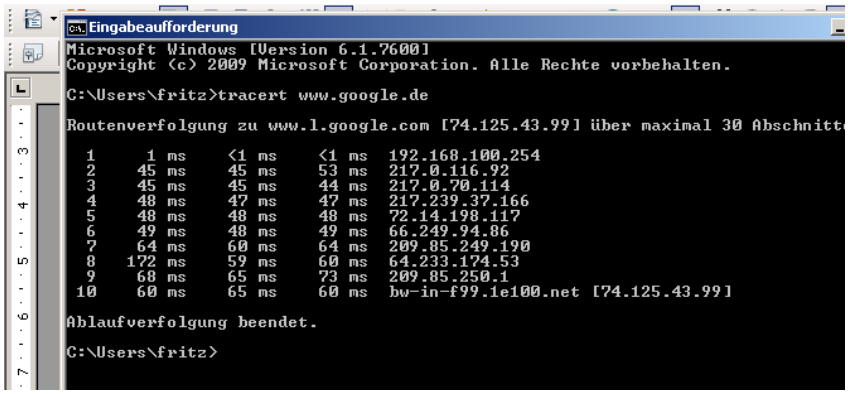
3. Wir pingen den Nachbar PC mit
ping w.x.y.z

4. Wir ändern uns Subnetmask und pingen
pc1 128.168.100.1/24
pc2 192.168.100.2/16

5. Wir fragen den DNS -Server
Man kann so einen DNS-Server auch manuell anfragen mit dem Befehl
nslookup
bzw.
nslookup www.netzmafia.de

6. Routenverfolgung:

1. Wir verwenden den Befehl: a) Windowse: tracert www.google.de
b) Linuxe: traceroute www.google.de
=> man sieht, dass das Datenpaket den PC verlässt und welche Router es durchläuft,



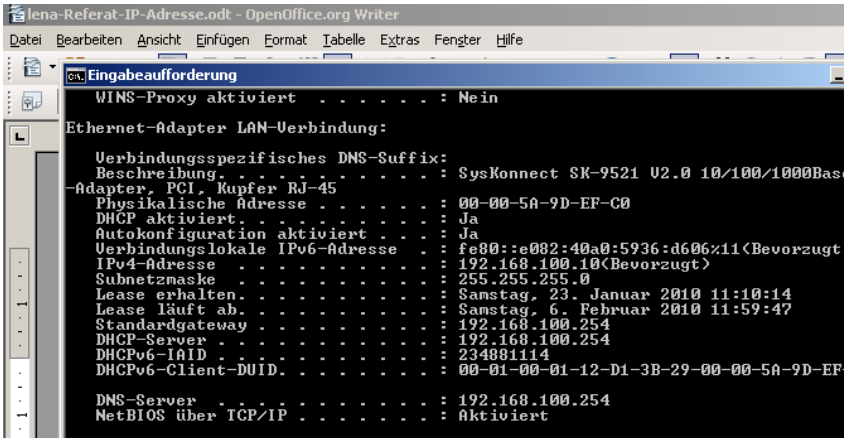
interessant ist für uns hier nur der default Gateway

Alle diese Einträge:
IP-Adresse
Subnetzmaske
default Gateway
DNS-Server
und noch vieles mehr
kann auch der DHCP-Server an einen anfragenden PC übermitteln.

7. Übung:
Wir lassen uns vom DHCP-Server alles geben und überprüfen mit

a) Windowse: ipconfig /all
b) Linux: ifconfig und route -n und cat /etc/resolv.conf (bei Linux sieht man diese Infos nicht komplett)

Hinweis: der Befehlt ipconfig /release verwirft alle Einträge, die er von einem DHCP-Server erhalten und der Befehl ipconfig /renew macht dann eine erneute Anfrage beim DHCP-Server (bei Linux war es dhclient)



Erweiterte Übung:
Wir schalten den DHCP-Server aus und machen eine Anfrage beim DHCP-Server.
Ergebnis: wir erhalten eine APIPA-Adresse

8. Welche Ports sind offen?
netstat

bzw.
netstat /?