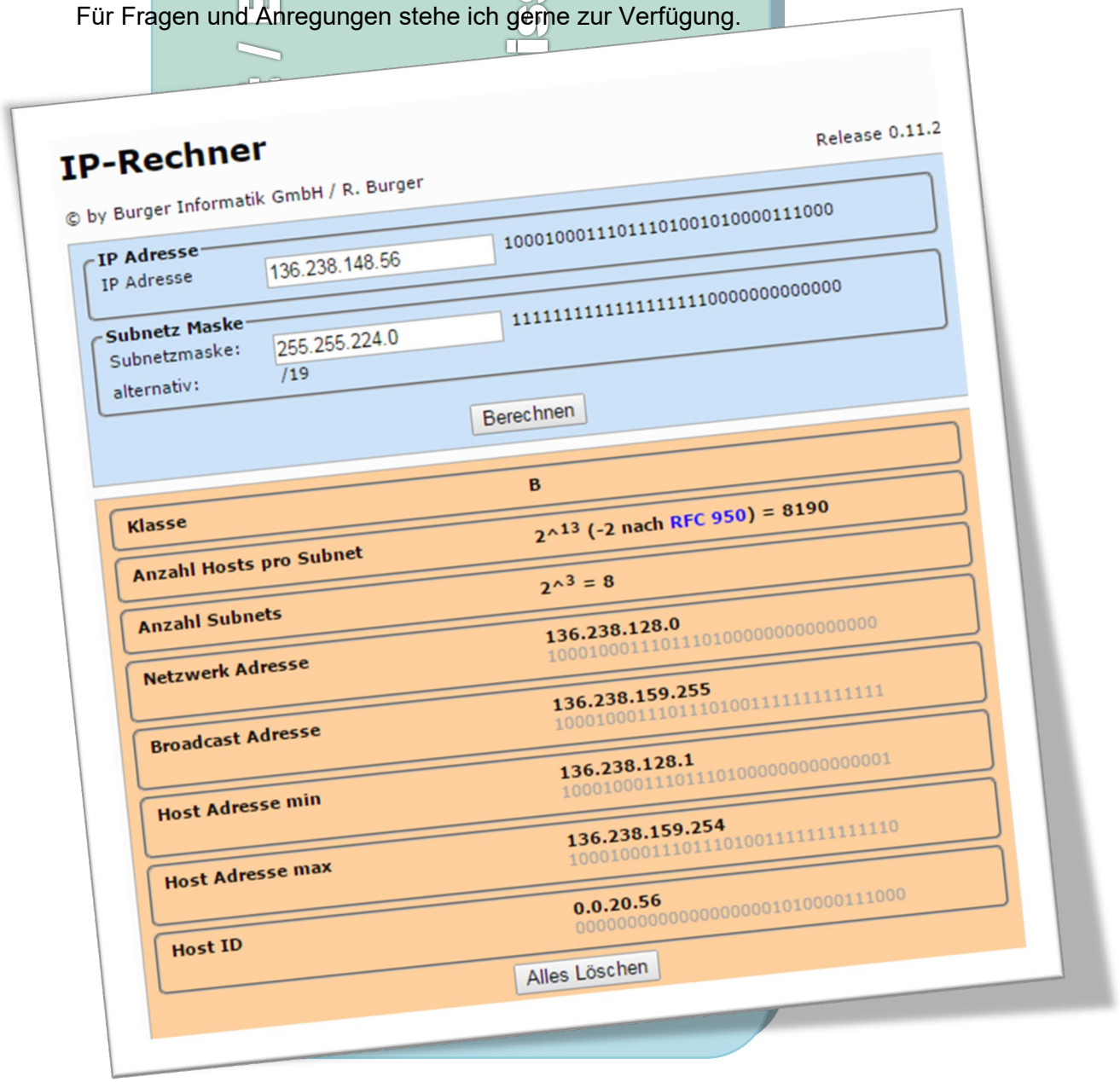
IP-Rechnen kann so einfach sein!

BUCH: Netzwerktechnik - IP-Rechnen kann so einfach sein von R. Burger
(Draft Version 0.11b, Oktober 2019)

Einleitung

Es gibt viele IP-Rechner im Internet, verschiedene Seiten, wo beschrieben wird, wie man Binär rechnet und dennoch stelle ich fest, dass sehr viele Interessierte, Informatiker und Leute die es werden wollen, sich das Vorgehen nicht merken können oder es (noch) nicht richtig verstehen.
Aufgrund dieser Erkenntnis und meiner langjähriger Tätigkeit als Ausbildner und Dozent an verschiedenen Schulen unterschiedlichen Niveaus habe ich eine Methode entwickelt, welche vielen Lernenden und Studierenden eine Hilfe sein kann.
Die folgenden Seiten zeigen auf, wie man einfach IP-Rechnen kann.
Weitere Kapitel über allgemeine Netzwerkgrundlagen, IP-Konzepte, sinnvolle Dimensionierung, Routing etc. werden auch beschrieben, sind in dieser Version jedoch noch im Draft / Aufbau.

Für Fragen und Anregungen stehe ich gerne zur Verfügung.



Inhaltsverzeichnis

Grundlagen

Erst mal ein paar Informationen als Grundwissen:
Wir arbeiten mit IP V4. IP V4 ist 32bit gross (aufgeteilt in 4 Oktetten zu 8 Bit) (siehe Abbildung 1: Aufteilung Netzwork und Hosts) und kann dezimal oder binär dargestellt werden:

Binär / Dezimal umrechnen

Um mit IP-Adressen rechnen zu können, muss verstanden werden, wie man vom dezimalen System ins Binäre umrechnen kann und umgekehrt.
Hier ein Beispiel:

172.16.1.150 ist in Binär: 10101100.00001000.00000001.10010110

Dezimal in Binär

1.Die gegebene Zahl durch 2 dividieren
2.Den Rest der Division notieren
3.Falls das Ergebnis nicht 0 ist, Schritt 1 und 2 wiederholen

Zahl	Quotient	**Rest**
172:2	86	0
86:2	43	0
43:2	21	1
21:2	10	1
10:2	5	0
5:2	2	1
2:2	1	0
1:2	0	1

Den Rest jetzt von unten nach oben gelesen ist die Binärzahl aus 172 also: 10101100

Binär in Dezimal

Das erste Oktett schauen wir uns mal genauer an:

Bit-Nr	8	7	6	5	4	3	2	1
172 in Binär	1	0	1	0	1	1	0	0
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
ergibt	128		32		8	4		

Dort wo in der zweiten Reihe eine 1 steht, rechnen wir die Zahl aus, welche daraus resultiert. Das erste Bit von links (Bit-Nr 8) entspricht 2^7. Das ergibt 128. Da beim 2. Bit (Bit-Nr 7) eine 0 steht, müssen wir nichts rechnen. Beim 3. Bit (Bit-Nr 6) steht wieder eine 1, also rechnen wir 2^5. Usw. Jetzt müssen wir nur die Resultate addieren und haben das Resultat im Dezimalsystem:
128+32+8+4=172

IP Version 4 und 6

Von IP V4 zu IP V6 ist ein grosser Schritt passiert. Nicht nur, dass die Adressgrösse von v4 mit 32Bit auf 128 Bit bei v6 angehoben wurde, auch wird IP v6 in HEX dargestellt. Alle weiteren Änderungen werden in einem späteren Kapitel beschrieben (Verweis).
Die folgenden Seiten beschreiben IP v4. Das Kapitel IPv6 startet auf Seite 46.

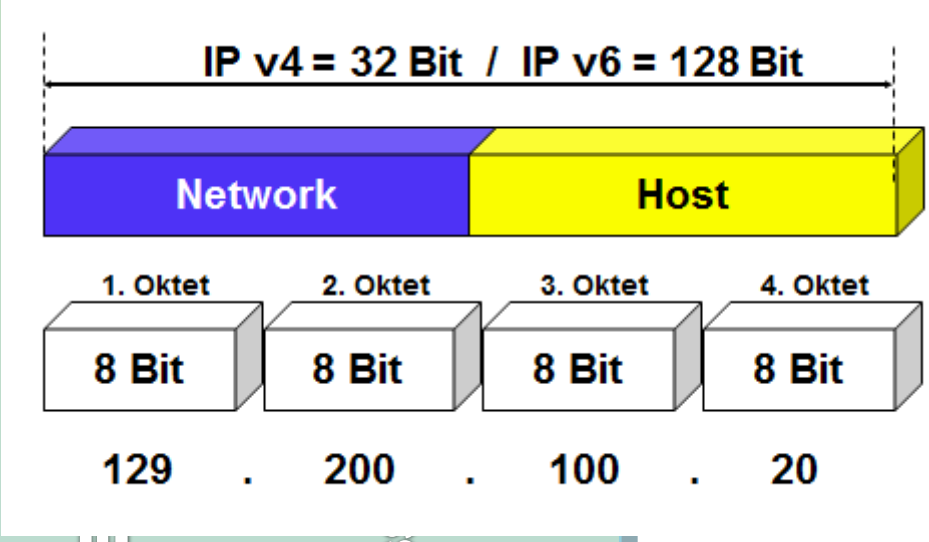


Abbildung 1: Aufteilung Netzwork und Hosts

Die IP-Adresse ist in einen Netzwerkteil und einen Hostteil unterteilt. Vergleichbar mit der Telefonnummer 041 / 123 45 67 wobei die Vorwahl 041 der Netzwerkadresse (blau) entspricht und die Telefonnummer 123 45 67 dem Hostteil (gelb).

Netzwerkklassen

Massgebend für die Netzwerkklasse ist nicht die Netzmaske wie oft angenommen, sondern das erste Oktett einer Netzwerkadresse!

Schauen wir von der IP-Adresse das erste Oktett genauer an, sehen wir, dass die ersten Ziffern bei der Darstellung in Binär massgebend sind für die Zuordnung der Klassen.
Ist die erste Ziffer eine 0 handelt es sich um die Klasse A
Ist die erste Ziffer eine 1 und die Zweite eine 0, sind wir in der Klasse B
Und so weiter:

Dezimal 1.Oktett	Binär-darstellung	Klasse	Maske	VLSM	Bereich	#Hosts	#Netze
0 – 126	0xxxxxxx	A	255.0.0.0	/8	0.0.0.0 - 126.255.255.255	16‘777‘216	128
128 - 191	10xxxxxx	B	255.255.0.0	/16	128.0.0.0 - 191.255.255.255	65‘536	16‘384
192 - 223	110xxxxx	C	255.255.255.0	/24	192.0.0.0 - 223.255.255.255	256	2‘097‘152
224 - 239	1110xxxx	D			224.0.0.0 - 239.255.255.255	Verwendung für Multicast-Anwendungen	
240 - 255	11110xxx	E			240.0.0.0 - 255.255.255.255	reserviert (für zukünftige Zwecke)	

Tabelle 1: Aufstellung der Klassen bei IPv4

127.0.0.0 – 127.255.255.255 ist für localhost für Loopback-Devices
(Bei IPv6 wird für den gleichen Effekt die Notation ::1 verwendet.)

Grafische Darstellung der Netzwerkklassen

Um zu ermitteln, zu welcher Klasse eine IP-Adresse zuzuordnen ist, können wir dies auch mit dem Kreis darstellen. Sind im ersten Oktett die IP-Adresse zwischen 0 und 126, befindet sich die IP-Adressen in der Klasse A, also der blaue Bereich (127 ist ja bekanntlich local-host).
Ist die IP-Adresse des ersten Oktetts zwischen 128 und 191 > Klasse B (grüner Bereich).
Ist die IP-Adresse des ersten Oktetts zwischen 192 und 223 > Klasse C (roter Bereich).

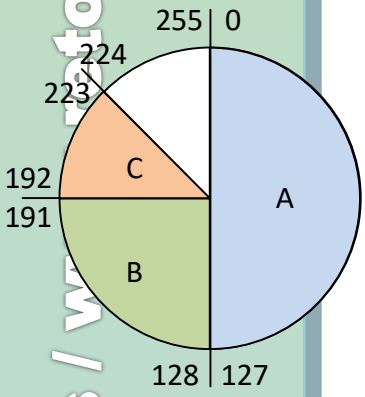


Abbildung 2: Andere Darstellung für die Zuordnung der Klassen

Beispiel:
Die IP-Adresse 136.238.144.12. Die Zahl im ersten Oktett ist die 136. Diese wird demnach im grünen Bereich des obigen Kreises eingetragen und ist somit eine Adresse aus der Klasse B.

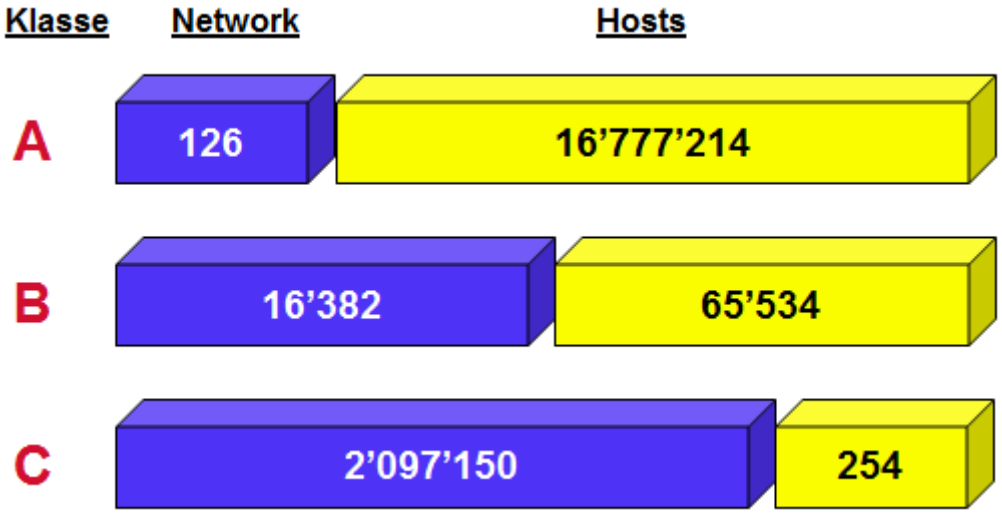


Abbildung 3: Anz. Netze pro Klasse & Hosts

In diesem Bild werden nur die nutzbaren IP-Adressen und nutzbaren Netzwerke aufgezählt. Darum unterscheiden sich die Zahlen der vorherigen Tabelle.

Variable Length Subnet Mask

… gelöscht!

Abschnitt wird neu überarbeitet!!

Classless Inter-Domain Routing / CIDR

… gelöscht!

Abschnitt wird neu überarbeitet!!

Private Ranges

Aus jeder Klasse gibt es einen Bereich, der vom Internet her nicht geroutet wird (RFC1918). Diese Adressen dürfen beliebig genutzt werden. Die Verantwortung für die Richtigkeit bleibt beim jeweiligen Administrator.

Klasse A	10.0.0.0 – 10.255.255.255	1 Klasse A Netze
Klasse B	172.16.0.0 – 172.31.255.255	16 Klasse B Netze
Klasse C	192.168.0.0 – 192.168.255.255	256 Klasse C Netze

Tabelle 2: Private IP-Adressbereiche

Shared Address

Wegen des Adressmangels und zunehmender Konflikte bei den oben genannten IP-Adressbereichen wurde ein weiterer Bereich zur mehrfachen Verwendung freigegeben. Dieser Bereich 100.64.0.0/10 (RFC 6598) ist speziell für Internetdienstanbieter zur Verwendung mit CGNAT resp. Carrier-grade NAT (CGN) vorgesehen.

Link Local

Weiterhin hat der Adressraum 169.254.0.0/16, der gemäss RFC 5735 als Link Local ausgezeichnet ist, eine ähnliche Sonderstellung. Mittels Zeroconf bzw. Automatic Private IP Addressing (APIPA) können Endgeräte automatisch eine IP-Adresse aus diesem Bereich verwenden.

IPv6

Das IPv6-Pendant heißt Unique Local Addresses. Aufgrund des größeren Adressraums nutzt man dort 40 Bit der Netzadresse als zufällig gewählten Identifikator. Dieser soll die Wahrscheinlichkeit der Einmaligkeit eines privaten Netzes erhöhen, um Adresskonflikte bei Zusammenschluss von privaten Netzen zu vermindern.

Subnetmaske

Mit der Subnetmaske lässt sich errechnen, wie gross der Hostanteil einer IP-Adresse ist. In anderen Worten, von wo bis der IP-Adressbereich innerhalb des Netzes, oder Subnetzes geht.

Klasse	Address Range	Subnetmaske
A	1 126 . 0 0 . 0 0 . 0 0	255.0.0.0
B	128 191 . 0 255 . 0 0 . 0 0	255.255.0.0
C	192 223 . 0 255 . 0 255 . 0 0	255.255.255.0
D	224.0.0.0 to 239.255.255.254	

Abbildung 4: Klassen und dessen Standardmaske

IP-Rechnen nach Burger

Bemerkung: Ich erlaube mir diese Methode so zu nennen, da ich diese Methode selber entwickelt und durch jahrelanges Dozieren verfeinert habe.

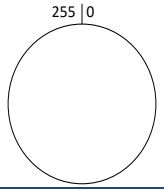
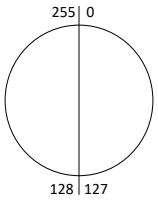
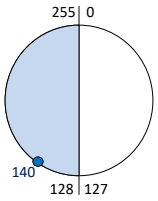
Wir haben z.B. folgende Ausgangslage:

192.168.1.140 mit der **Maske 255.255.255.128**

Ist bei einem Oktett die Zahl weder 0 noch 255, so nennen wir das ein „angeschnittenes“ Oktett, wie dies beim 4. Oktett in obigem Beispiel der Fall ist.
Schauen wir uns die Maske genauer an können wir diese in Binär wie folgt schreiben:
11111111.11111111.11111111.10000000.
Es sind also 25Bits der Maske gesetzt, was auch als alternative Schreibweise, manchmal auch als Präfixlänge oder VLSM/Classless Routing (variable-length subnet mask) oder Classless Inter-Domain Routing (CIDR) genannt.

Wenn wir nur das angeschnittene Oktett der Maske anschauen, sehen wir, dass ein Bit gesetzt wird.
Somit wird das vierte Oktett einmal geteilt.

Das können wir auch grafisch darstellen:

Ein ungeteiltes Oktett können wir als einen Kreis (Zirkel) von 0 -255 darstellen:	
Ist nun ein Bit im angeschnittenen Oktett gesetzt, wird der Kreis einmal geteilt:	
Der vorgegebenen IP-Adresse (192.168.1.140) entnehmen wir, dass das 4 Oktett die 140 ist. In unserem Kreis ist also die 140 auf der eingefärbten Seite. Nun können wir schon einiges aus der Zeichnung herauslesen: Erste IP-Adresse unseres IP-Ranges (IP-Bereiches) im 4 Oktett ist die 128 und die letzte die 255.	

Jetzt setzen wir die Zahlen zusammen und das ergibt folgendes Resultat:

IP-Adresse:	192.168.1.140
Netzmaske:	255.255.255.128
Alternative Schreibweise:	/25
Netz-ID:	192.168.1.128
Broadcastadresse:	192.168.1.255

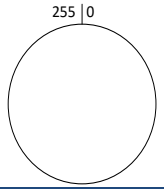
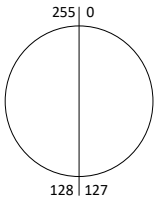
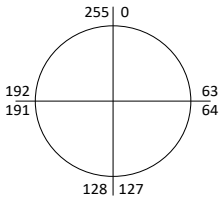
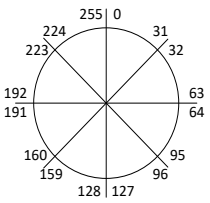
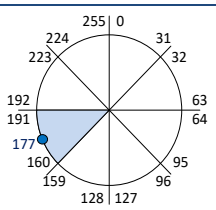
Wir machen ein weiteres Beispiel, um dies genauer zu veranschaulichen:

Als Ausgangslage nehmen wir **172.20.177.50** mit der **Maske 255.255.224.0**

Das angeschnittene Oktett (also weder 255 noch 0) ist das dritte Oktett mit der Zahl 224. 224 kann mit 11100000 in Binär geschrieben werden. Die 3 Bits vom dritten Oktett werden also den 16 vorangehenden Bits zusammen gezählt:
11111111.11111111.11100000.00000000
Die Maske hat also 19 Bits gesetzt, was also auch als /19 geschrieben werden kann.
Drei Bits im angeschnittenen Oktett heisst also, dass der Kreis dreimal halbiert werden muss, oder genauer gesagt wird der komplette Kreis in 8 Segmente geteilt zu 32 Bits resp. zu 32 Adressen.

1Bit:	halbiert	2x 1/2	à 128 Bits
2Bit:	gevierteilt	4x 1/4	à 64 Bits
3Bit:	geachtelt	8x 1/8	à 32 Bits
4Bit:	in 16 Teile	16x 1/16	à 16 Bits
5Bit:	in 32 Teile	32x 1/32	à 8 Bits
6Bit:	in 64 Teile	64x 1/64	à 4 Bits
7Bit:	in 128 Teile	128x 1/128	à 2 Bits

Grafisch dargestellt sieht das wie folgt aus:

Ein ungeteiltes Oktett können wie als einen Kreis von 0 -255 darstellen:	
Ist nun ein Bit im angeschnittenen Oktett gesetzt, wird der Kreis einmal geteilt:	
Sind zwei Bits im angeschnittenen Oktett gesetzt, wird der Kreis noch einmal geteilt:	
Und bei drei Bits im angeschnittenen Oktett wird der Kreis nochmals geteilt, also total 3x halbiert. Das macht dann 8 Segmente zu 32 Adressen.	
Der vorgegebenen IP-Adresse (172.20.177.50) entnehmen wir, dass das 3 Oktett die 177 ist. In unserem Kreis ist also die 177 im eingefärbten Segment. Auch hier können wir vieles direkt aus der Zeichnung heraus lesen:	

Die erste IP-Adresse unseres IP-Ranges (IP-Bereiches) im 3 Oktett ist die 160 und die letzte die 191.	

Jetzt setzen wir die Zahlen zusammen und das ergibt folgendes Resultat:

IP-Adresse:	172.20.177.50
Netzmaske:	255.255.224.0
Alternative Schreibweise:	/19
Netz-ID:	172.20.160.0
Broadcastadresse:	172.20.191.255

Grundregel zur Überprüfung
Wir können durch einen Kontrollcheck prüfen, ob unsere Berechnungen auch stimmen:

- Die Netz-ID ist im gebrochenen Oktett immer eine **gerade** Zahl
- Die Broadcast-Adresse ist im gebrochenen Oktett immer eine **ungerade** Zahl

Kleinere Aufteilungen

Wenn die Netzwerkmaske im Oktett noch kleinere Segmente verlangt, können wir das kaum mehr mit dem Kreis darstellen. Der Kreis hilft uns jedoch für eine weitere Methode:

Beispiel mit 140.190.201.80 / 22

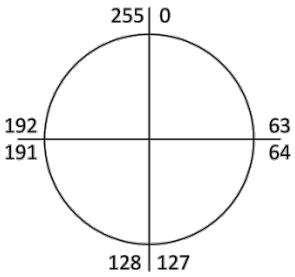
Die Subnetmaske aus dem Beispiel mit /22 heisst also 255.255.252.0.
Wir suchen das geschnittene / gebrochene Oktett in der Maske und finden das an der dritten Stelle. Wir schauen uns das dritte Oktett genauer an:

Die 252 wird binär als 11111100 dargestellt. Es sind also sechs Bits auf 1 gesetzt.
Wir gehen also wie gewohnt vor:

1. Bit bedeutet 1x teilen	halbieren
2. Bit bedeutet 2x teilen	vierteln
3. Bit bedeutet 4x teilen	achteln
4. Bit bedeutet 8x teilen	sechzehn Teile
5. Bit bedeutet 16x teilen	zweiunddreissig Teile
6. Bit bedeutet 32x teilen	64 Teile

Nun können wir unseren Kreis kaum so zeichnen, dass diese 64 Teile erkennbar sind. Also gehen wir wie folgt vor:
6 Bit ergeben 64 Teile in unseren Bereich von 0-255 (das macht 256 Informationen oder Zustände). Also teilen wir diese 256 durch 64 und erhalten die 4. Das heisst, dass wir jetzt mit im dritten Oktett vierer-Schritte machen. 0-3, 4-7, 8-11, usw.
Unsere IP-Adresse heisst 140.190.201.80. Da das dritte Oktett das geschnittene ist, interessiert uns im Moment nur das dritte Oktett der IP-Adresse, also die 201.

Wir könnten nun eine Tabelle aufstellen und von 0 starten:
0 – 3
4 – 7
8 – 11
12 – 15
Etc. bis wir den Bereich einschliessen wo die Zahl 201 vorkommt.



Da wir aus vergangenen Übungen die bekannten Zahlen wie 0, 64, 128, 192, 255 kennen, starten wir von der Zahl, die der 196 am nächsten ist. Das wäre also die 192.
Wir zählen also die Viererschritte ab 192 und sehen bereits nach der dritten Aufzählung, dass die 201 zwischen 200 und 203 liegt.

192 – 195
196 – 199
200 – 203
204 – 207
…

Vertiefung

Anzahl nutzbaren Hosts

Oft interessiert uns, wie viele IP-Adressen im gegebenen Bereich angesprochen resp. verwenden werden dürfen. Dies kann auch einfach anhand der Subnetzmaske / Netzwerkmaske errechnet werden.
Dazu schauen wir die Netzmaske an. Sind, wie in obigem Beispiel 19 Bits gesetzt müssen also 13 Bis mit 0 gesetzt werden, damit wir auf 32 Bit in der Maske kommen.
Diese 13 setzen wir als Exponent (Hochzahl) zur Basis 2. > 2^{13}. Da wir jedoch die erste Adresse (Netz-ID) und die letzte Adresse (Broadcast-Adresse) nicht nutzen dürfen (nach RFC 950) sieht die Rechnung nun so aus: 2^{13} -2

Anzahl gleicher Subnetze

Möchten wir wissen, wie viele gleich grosser Subnetze zur Verfügung stehen, müssen wir die Differenz der aktuellen Netzwerkmaske zur Maske, welche unsere IP-Adresse in der ungeteilten Grösse hat (also ohne Subnetze) rechnen und also Exponent zur Basis zwei setzen.

Beispiel:
172.20.177.50 / 19
172 kommt aus dem B-Netz und hat im Normalfall 16 Bits in der Maske. Nun haben wir 19Bits gesetzt, was zu 16 eine Differenz von 3 macht. Setzen wir also diese 3 als Exponent zur Basis 2.
2^3 ergibt 8. Wir haben also 8 gleich grosse Netze zur Verfügung.

Natürlich können wir nachdem wir eines dieser 8 Netze genutzt haben, die weiteren noch kleiner unterteilen oder mischen. Es muss aber immer darauf geachtet werden, dass die Teilungen möglich sind!

Subnetze und Supernetze

Ein Subnetz verkleinert ein Netz. Wenn wir ein A-Klasse Netz mit der IP-Adresse 10.0.0.0/8 haben, werden wir dieses kaum so einsetzen, sondern in mehrere kleinere Netze aufteilen. Wenn wir also ein Netz kleiner machen, als die Standardmaske der Klasse es vorsieht, nennen wir das Subnetz oder Subnetieren.
Der andere Fall ist, wenn wir z.B. zwei nebeneinanderliegende C-Netze zu einem grösseren Netz zusammenfassen wollen. Das nennen wir Supernetze.
Wir haben beispielsweise 192.168.0.0/24 und 192.168.1.0/24 und möchten diese zwei als eines mit 512 Hosts nutzen, dann vergrössern wir ein Standardnetz. Dieser Vorgang nennt man Supernetz oder Superneting. Neu sieht dann unser Beispiel so aus: 192.168.0.0/23

Host-ID

Die Host-ID ist eine rein rechnerische ID, die ich all die vielen Jahre kaum in der Praxis gebraucht habe. Die Host-ID ist quasi die Telefonnummer ohne Vorwahl, also die IP-Adresse ohne Netz-ID. Gerechnet wird das auch genauso. Man rechnet die IP-Adresse minus die Netz-ID und bekommt die Host-ID

Beispiel:

IP-Adresse		172	20	177	50
Netz-ID	-	172	20	160	0
Host-ID		0	0	17	50

Die Host-ID ist also 0.0.17.50 resp. 17.50
Die Nullen links können weggelassen werden.

Komplette Aufgabe

Schliesslich lassen sich alle nötigen Daten errechnen:

- IP-Adresse
- Subnetzmaske
- Alternative Schreibweise / VLSM / CIDR
- Klasse
- Anzahl Host im Subnetz
- Anzahl gleichgrosse Subnetze (bei gleicher Maske)
- Netz-ID
- Broadcast-Adresse
- Host-ID

Beispiele

Zur Kontrolle der folgenden Aufgaben kann der Online IP-Rechner von www.reto-burger.ch benutzt werden. Dieser zeigt die Resultate jeweils Binär und Dezimal an.

Als Ausgangslage nehmen wir folgende Daten:
10.200.100.50 mit 255.192.0.0

Genauer Ablauf / Vorgehen:
Das „angeschnittene" Oktett ist in diesem Fall das zweite, also die 192. Die 192 wird binär mit 11000000 dargestellt. Es sind also zwei Bits gesetzt.

VLSM
Für die alternative Schreibweise resp. VLSM rechnen wir die 8 Bits der Maske aus dem ersten Oktett dazu und erhalten die /10.

CIDR
Bei CIDR führte man als neue Notation so genannte Suffixe ein. Das Suffix gibt die Anzahl der 1-Bits in der Netzmaske an. Diese Schreibform, z. B. 172.17.0.0/17, ist viel kürzer und im Umgang einfacher als die Dotted decimal notation wie 172.17.0.0/255.255.128.0 und ebenfalls eindeutig.

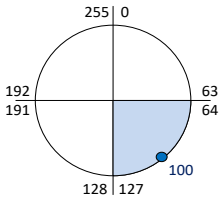
Bei IPv6 ist die Notation gleich wie beim CIDR in IPv4 und besteht aus IPv6-Adresse und Präfixlänge (z. B. 2001:0DB8:0:CD30::1/60).

Klasse
Die Zahl aus dem ersten Oktett zeigt uns, aus welcher Klasse die IP-Adresse stammt. 10 ist also gemäss den Ausführungen auf Seite 5 (Netzwerkklassen) aus der Klasse A.

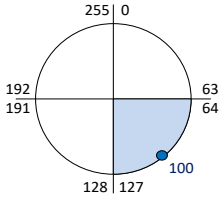
Anzahl (#) Host im Subnetz
Dazu zählen wir die nicht gesetzten Bits (0) der Subnetzmaske oder ziehen von 32 die aus VLSM gefundenen 10 Bits ab. Die Zahl 32 kommt daher, dass total 32Bits in der Subnetzmaske möglich sind. Das ergibt 22. Diese nehmen wir als Exponent zur Basis 2 und das ergibt $2^{22.}$ Da wir die Netz-ID und Broadcastadresse nicht nutzen dürfen, zählen wir noch 2 ab und das ergibt unser Resultat für die Anz. Host im Subnetz: 2^{22} -2.

Anzahl (#) gleichgrosse Subnetze
Hierzu brauchen wir wiederum die Subnetzmaske. Gesetzt sind 10 Bits. Da die IP-Adresse aus der Klasse A stammt, wissen wir, dass normalerweise 8 Bits in der Maske definiert werden. Die Differenz der gesetzten 10 Bits zu den aus der Klasse A stammenden 8 Bits gibt 2. Diese 2 nehmen wir als Exponenten zur Basis 2 was das Resultat für die Anzahl gleichgrosser Subnetze ergibt: 2^2.

Netz-ID
Dazu können wir wieder unseren IP-Kreis (IP-Zirkel) verwenden:

Im angeschnittenen Teil der Maske sind 2 Bits gesetzt. Wir halbieren also unseren Kreis 2x: 1.mal: in 2 Teile 2.mal: in 4 Teile Nun haben wir unseren IP-Kreis in vier Segmente unterteilt und können aus der IP-Adresse herauslesen, in welchen der Segmente wir uns befinden. Die Zahl aus der IP-Adresse im angeschnittenen Teil ist 100 und passt also in das zweite (eingefärbte) Segment. Wir können jetzt bereits die Netz-ID herauslesen, da es sich dabei aus der kleinsten Zahl handelt. Die 64 ist also die Netz-ID.	

Broadcast-Adresse
Auch dazu können wir wieder unseren IP-Kreis (IP-Zirkel) verwenden:

Den obigen Kreis können wir auch hier verwenden und direkt die Zahl herauslesen für die Broadcastadresse: 127	

Host-ID
Wir rechnen die Differenz der IP-Adresse zur Netz-ID und erhalten dann die Host-ID:

IP-Adresse		10	100	100	50
Netz-ID	-	10	64	0	0
Host-ID		0	36	100	50

Die Host-ID ist also 36.100.50

Lösung:

IP-Adresse	10.100.100.50
Subnetzmaske	255.192.0.0
VLSM	/10
Klasse	A
# Host im Subnetz	2^{22} -2
# gleichgrosse Subnetze	2^{2}
Netz-ID	10.64.0.0
Broadcast-Adresse	10.127.255.255
Host-ID	0.36.100.50

Klassisches IP-Rechnen (binär)

Wir nehmen wieder die bereits verwendeten IP-Adressen und Masken für die Berechnung im binären System.
172.20.177.50 / 19
Binär dargestellt sieht das wie folgt aus:

172	20	177	50
1010 1100	0001 0100	1011 0001	0011 0010
255	255	224	0
1111 1111	1111 1111	1110 0000	0000 0000

Nehmen wir zur vereinfachten Darstellung die Dezimalzahlen aus der Tabelle.
Wenn wir nun die erste Reihe mit der zweiten Reihe mit AND verknüpfen erhalten wir in der dritten Reihe die Netz-ID

1010 1100	0001 0100	1011 0001	0011 0010
1111 1111	1111 1111	1110 0000	0000 0000
1010 1100	0001 0100	1010 0000	0000 0000
172	20	160	0

Um die Broadcastadresse zu errechnen, macht man den gleichen Vorgang wie für die Netz-ID (auch mit dem AND-Operator). Es wird dann im Resultat überall eine 1 geschrieben, wo in der Maske eine 0 steht. Das ergibt automatisch die Broadcast-Adresse.

1010 1100	0001 0100	1011 0001	0011 0010
1111 1111	1111 1111	1110 0000	0000 0000
1010 1100	0001 0100	1011 1111	1111 1111
172	20	191	255

NAT Network Adress Translation

Wir unterscheiden zwischen sNAT und dNAT

Source-NAT

PAT

Destination-NAT

NAT-T NAT-Traversal

Portweiterleitung

Kapitel noch in Arbeit

Netzwerke dimensionieren

Nehmen wir an, dass wir ein grösseres Netzwerk komplett neu definieren dürfen / sollen.
LAN A soll 600 Hosts[1] beinhalten.
Wenn wir nun 192.168.0.0 /24 mit 256 Hosts (-2) als Ausgangslage haben, brauchen wir noch ein zweites solches Netz, was wir in dem Falle als Supernetz benennen:
192.168.0.0 /23

Auch hier können wir wieder ganz normal unsere Erkenntnisse vom IP-Rechnen holen und errechnen folgendes:

Netz-ID:	192.168.0.0	(ist gegeben)
Netzwerkmaske:	255.255.254.0	(entspricht /23)
Broadcastadresse:	192.168.1.255	(wird errechnet)

Also haben wir 256 Adressen vom Netz 192.168.0.x und weitere 256 Adressen vom Netz 192.168.1.x.

Da wir als Anzahl Hosts immer die Nullen der Netzwerkmaske zählen gibt es bei /23 neun Nullen > 2^9 ergibt 512. Wenn wir am Schluss noch zwei abzählen, erhalten wir 510 brauchbare IP-Adressen.

Wenn wir also sparsam mit unseren IP-Adressen umgehen wollen, müssen wir zuerst mal ein Konzept erstellen oder erhalten mit den Vorgaben, wie viele IP-Adressen in den jeweiligen Teilnetzen gebraucht werden.

Notizen: Immer mit den grössten Teilnetzen beginnen….

Achtung: Theorie und Praxis!!

Übungsbeispiel auf der folgenden Seite

Netzwerke verdoppeln mit der Ausgangslage von /24 (255.255.255.0)

/24	256 Hosts	8 Bits auf 0 (in der Netzwerkmaske)
/23	512 Hosts	9 Bits auf 0
/22	1024 Hosts	10 Bits auf 0
/21	2048 Hosts	11 Bits auf 0
/20	4096 Hosts	12 Bits auf 0
etc		

Netzwerke halbieren mit der Ausgangslage von /24 (255.255.255.0)

/24	256 Hosts	8 Bits auf 0 (in der Netzwerkmaske)
/25	128 Hosts	7 Bits auf 0
/26	64 Hosts	6 Bits auf 0
/27	32 Hosts	5 Bits auf 0
/28	16 Hosts	4 Bits auf 0
/29	8 Hosts	3 Bits auf 0
/30	4 Hosts	2 Bits auf 0
etc		

Kapitel noch in Arbeit

[1] Mit Hosts meinen wir hier nicht nur PCs sondern auch Drucker, Server, Mobile-Devices, etc. Also alles Geräte, die in dem LAN kommunizieren müssen oder dürfen.

Beispiel

Gegeben / Ausgangslage:

LAN	Basis	Anzahl Hosts
LAN 1	172.20.0.0	260 Hosts
LAN 2	10.0.0.0	300 Hosts
LAN 3	10.0.0.0	28 Hosts
LAN 4	10.0.0.0	60 Hosts
LAN 5	172.20.0.0	1800 Hosts
LAN 6	172.20.0.0	900 Hosts
DMZ	172.21.0.0	20 Hosts
TL	192.168.0.0	
ISP ext.	213.200.1.94	

>>> GW hat die höchste mögliche IP-Adresse

Ges :

- Netz-ID
- Netzwerkmaske / Alternative Schreibweise
- Broadcast-Adresse
- Gateway

Bitte vervollständigen Sie die Tabelle:

LAN	Netz-ID	Netzwerkmaske	Alt. Schreibw.	Broadcast-Adresse	Gateway
1			/		
2					
3					
4					
5					
6					
DMZ					
TL					
ISP					

Musterlösung:

Wir beginnen pro Basis mit dem grössten Netz. Als Vorbereitung wurden bei der Tabelle (Ausgangslage) jene LAN's mit der gleichen Farbe markiert, welche zusammengehören, resp. die gleiche Basis haben.

LAN	Netz-ID	Netzwerkmaske	Alt. Schreibw.	Broadcast-Adresse	Gateway
1	172.20.12.0	255.255.254.0	/23	172.20.13.255	172.20.13.254
2	10.0.0.0	255.255.254.0	/23	10.0.1.255	10.0.1.254
3	10.0.2.64	255.255.255.224	/27	10.0.2.95	10.0.2.94
4	10.0.2.0	255.255.255.192	/26	10.0.2.63	10.0.2.62
5	172.20.0.0	255.255.248	/21	172.20.7.255	172.20.7.254
6	172.20.8.0	255.255.252.0	/22	172.20.11.255	172.20.11.254
DMZ	172.21.0.0	255.255.255.224	/27	172.21.0.31	172.21.0.30
TL	192.168.0.0	255.255.255.252	/30	192.168.0.3	192.168.0.2
ISP	213.200.1.92	255.255.255.252	/30	213.200.1.95	213.200.1.94

Zur Kontrolle hilft Ihnen der Online IP-Rechner: www.ip-rechner.ch

DMZ: Demilitarisierte Zone
TL: Transit LAN (direkte Verbindung zwischen zwei Router > /30)

IP Konzepte

Es macht Sinn, sich bereits vor der Implementation eines Netzwerkes Gedanken zu machen, wie man die IP-Adressen im Netzwerk optimal verteilen kann. Hier gibt es nicht ein „Richtig“ oder „Falsch“.
Hier ein Beispiel, wie man die IP-Adressen aufteilen könnte:

192.168.0.0 / 24	
192.168.0.0 – 192.168.0.19	Server, NSAs
192.168.0.20 – 192.168.0.29	*Reserve*
192.168.0.30 – 192.168.0.49	Printer, Plotter
192.168.0.50 – 192.168.0.79	VoIP-Geräte
192.168.0.80 – 192.168.0.99	*Reserve*
192.168.0.100 – 192.168.0.199	DHCP / Clients
192.168.0.200 – 192.168.0.219	*Reserve*
192.168.0.220 – 192.168.0.239	Switches (Mgnt)
192.168.0.240 – 192.168.0.249	AccessPoints
192.168.0.250 – 192.168.0.253	weitere Router
192.168.0.254	Default-Gateway / Firewall

Mögliche weitere Geräte die zu berücksichtigen sind:

- CNC-Systeme
- Roboter
- Barcodelesegeräte
- MDE (Mobile Daten Erfassung)
- Zeiterfassungssysteme
- Zutrittskontrollen
- Webcams
- Überwachungs- Sicherheitssysteme
- Alarmanlagen
- Klima- und Heizanlagen
- Brandschutz-Systeme
- Solaranlagen
- Mobile-Devices, Smart-Phones
- Beamer
- KVM
- USV, UPS
- Haustechnik, Gebäudetechnik
- NAS
- Etc.

Diese Liste kann beliebig erweitert werden.

Namenskonzepte

Genauso macht es auch Sinn, ein Namenskonzept für User, Gruppen, Domains, Computer, Server, etc. zu definieren. Finde ich im Netzwerk ein Gerät, welches unnötigen Traffic macht, so sehe ich sehr schnell, was und wo das Gerät ist.
Idealerweise ist aus dem Namen zu entnehmen: Firmenname, Geräteart / Typ, Etage/Zimmer/Location, durchnummerierte Erweiterung.
zB: LABWS15612:
LAB: Labor, WS: Workstation, Zimmer: 156, Systemnummer:12

Routing

Die Kommunikation kann nur innerhalb eines Subnetzes stattfinden.
Um ausserhalb des Subnetzes zu kommunizieren, ist es nötig zu routen. Routen bedeutet, Datenpakete aus einem Subnetz in ein nächstes Subnetz weiterzuleiten. Generell unterscheiden wir zwischen drei Verfahren: **Defaultrouting, Dynamisches Routing und Statisches Routing**.

Es wird noch von weiteren Verfahren gesprochen wie:

- Statisches Routing
- Zentralisiertes Routing
- Isoliertes Routing
  - Delta Routing
  - Broadcast Routing
  - Hot Potato
  - Backward Learning, verteiltes adaptives Routing > dynamisches Routing
- Verteiltes adaptives Routing
- Distance Vector Routing
- Link State Routing
- Hierarchisches Routing
- Routing im Internet
  - Intradomain-Routing
  - Interdomain-Routing

Default Routing

Alles was nicht bekannt ist, wird an das Gerät weitergeleitet, welches als Defaultrouting resp. Standardgateway eingetragen ist. Wir vergleichen das gerne mit Verkehrstafeln, die den Weg von A nach B weisen. Kommen wir in einer grösseren Stadt an eine Kreuzung, finden wir oft das Verkehrssignal „Alle Richtungen“ oder Autobahn ohne genaue Zielangaben.

Beim Defaultrouting ist es das gleiche Prinzip. Der Defaultrouter ist jener, der uns den Weg zu weiteren Netzwerken oder zum Internet / Internetprovider zeigt.
In einer Routingtabelle wird das Defaultrouting wie folgt dargestellt:

Netz-ID	Maske	Gateway	Schnittstelle
0.0.0.0	0.0.0.0	x.x.x.x (nächster Router)	z.z.z.z (lokale Schnittstelle)

Netz-ID 0.0.0.0 mit der Maske 0.0.0.0 (/0) ist also deren Broadcastadresse die 255.255.255.255. Das heisst, dass damit der komplette IP-Bereich von 4'294'967'296 IP-Adressen abgedeckt ist.

Dynamisches Routing

Beim dynamischen Routing finden die gerouteten Pakete den Weg selber dank den aktivierten Routingprotokollen. Die unterschiedlichen Routingprotokolle haben unterschiedliche Eigenheiten und Einstellungsmöglichkeiten. Nachfolgende Tabelle zeigt einen kurzen Überblick:

Protokoll	Metric	Algorithmus IG / EG	Verwendung
RIP Routing Information Protokoll	Hops	DistanceVector Interior Gateway	Kleine Netzwerke (Limite von 15 hops) LAN
IGRP Interior Gateway Routing Protokoll	Bandbreite Zuverlässigkeit Auslastung	DistanceVector Interior Gateway	Grusse Netzwerke
OSPF Open Shortest Path First	Kombinationen	LinkState Interior Gateway	Grosse Netzwerke mit AS
E-IGRP Enhanced Interior Gateway Routing Protokoll	Kombinationen	LinkState Interior Gateway	Grosse Netzwerke mit AS
BGP Border Gateway Protokoll	AS System Count Delaystatus, Kosten	Exteriour Gateway	Sehr grosse Netzwerke. Nachfolger von EGP

Tabelle 3: Routing Protokolle mit Kurzbeschreibung

Der Begriff Hop (Hopser) bezeichnet einen Netzknoten wie ein Router oder ein Computer welcher routet. Die Anzahl Hops wird auch für die Errechnung der TTL (Time to Live) gebraucht, welche verhindert, dass Pakete im endlos weiterlaufen. Die TTL hat 8 Bits (ein Oktett) und hat somit maximal 255 Hops, die es durchlaufen kann. Nach jedem Hop wird das TTL um eins reduziert. Dienstprogramme wie tracert (traceroute) nutzen diese Technik auch.

Vergleich Routing- vs Routed- Protokolle

Routing Protokolle

RIP
IGRP
E-IGRP
OSPF
RIPX
BGP
…

Routed Protokolle

IP (TCP/IP)

XNS	Xerox
DECnet	DEC
LAT	DEC
SNA	IBM
NetWare / NCP	Novell
IPX/SPX	Novell
AppleTalk	Apple
Banyan Vines	**V**irtual **I**ntegrated **N**etwork **S**ervice (Abgeleitet von XNS)

Nicht routbare Protokolle

NetBEUI / NETBIOS
Das Protokoll NetBEUI ist ein kleines, schnelles und effizientes Protokoll, entwickelt von Microsoft und ist für die Kommunikation und für Anwendungen auf nur einem Segment gedacht (bis 15 max. 30 Systeme).

Statisches Routing

Statisches Routing oder manuelles Routing bezeichnen wir die Einstellung an einem Router oder System, wenn wir die Routingwege manuell konfigurieren.

Dieses Verfahren ist nicht adaptiv, sehr einfach und kommt daher häufig zum Einsatz. Jeder Knoten (entspricht einem Router) unterhält eine Tabelle mit einer Zeile für jeden möglichen Zielknoten resp. Zielnetzwerk. Eine Zeile enthält Einträge, welche die beste, zweitbeste usw. Übertragungsleitung für dieses Ziel ist, zusammen mit einer Gewichtung (Metrik). Vor der Weiterleitung eines Paketes wird der entsprechende Eintrag aus der Tabelle gewählt und auf eine der möglichen Leitungen (Schnittstellen) gegeben. Die Gewichtung spiegelt hier die Wahrscheinlichkeit wider, dass diese Leitung gewählt wird.

An einem Windows-PC kann ich die Routingtable / Routing Tabelle mit den folgenden Befehlen anschauen:

```
route print
```

oder

```
netstat -r
```

Beispiel unter Windows:

```
===========================================================================
Schnittstellenliste
 21...02 80 37 ab 00 00 ......HP hs2340 HSPA+ Mobile Broadband Module Network Adapter
 14...08 11 96 bc 00 1d ......Microsoft Virtual WiFi Miniport Adapter
 13...08 11 96 cd 00 1c ......Intel(R) Centrino(R) Advanced-N 6205
 10...e4 11 5b ef 00 10 ......Intel(R) 82579LM Gigabit Network Connection
  1...........................Software Loopback Interface 1
 18...00 00 00 00 00 00 00 e0 Microsoft-ISATAP-Adapter #2
 22...00 00 00 00 00 00 00 e0 Microsoft-ISATAP-Adapter #3
 23...00 00 00 00 00 00 00 e0 Microsoft-ISATAP-Adapter #4
 19...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 24...00 00 00 00 00 00 00 e0 Microsoft-ISATAP-Adapter #6
===========================================================================

IPv4-Routentabelle
===========================================================================
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway    Schnittstelle Metrik
          0.0.0.0          0.0.0.0     10.10.0.254       10.10.0.117     20
       10.10.0.0      255.255.255.0   Auf Verbindung       10.10.0.117    276
     10.10.0.117   255.255.255.255   Auf Verbindung       10.10.0.117    276
     10.10.0.255   255.255.255.255   Auf Verbindung       10.10.0.117    276
        127.0.0.0        255.0.0.0   Auf Verbindung         127.0.0.1    306
        127.0.0.1  255.255.255.255   Auf Verbindung         127.0.0.1    306
  127.255.255.255  255.255.255.255   Auf Verbindung         127.0.0.1    306
        224.0.0.0        240.0.0.0   Auf Verbindung         127.0.0.1    306
        224.0.0.0        240.0.0.0   Auf Verbindung       10.10.0.117    276
  255.255.255.255  255.255.255.255   Auf Verbindung         127.0.0.1    306
  255.255.255.255  255.255.255.255   Auf Verbindung       10.10.0.117    276
===========================================================================
Ständige Routen:
  Keine

IPv6-Routentabelle
===========================================================================
Aktive Routen:
 If Metrik Netzwerkziel            Gateway
  1    306 ::1/128                  Auf Verbindung
 13    276 fe80::/64                Auf Verbindung
 13    276 fe80::3bbf:68a1:cd97:8047/128
                                    Auf Verbindung
  1    306 ff00::/8                 Auf Verbindung
 13    276 ff00::/8                 Auf Verbindung
===========================================================================
Ständige Routen:
  Keine
```

Tabelle 4: Routing unter Windows

Routing-Tabelle einer Firewall:

```
Router> show ip route
Flags: A - Activated route, S - Static route, C - directly Connected
       O - OSPF derived, R - RIP derived, G - selected Gateway
       ! - reject, B - Black hole, L - Loop

IP Address/Netmask    Gateway          IFace          Metric    Flags    Persist
=============================================================================
0.0.0.0/0             0.0.0.0          ge2_ppp        0         ASG      -
10.10.0.0/24          0.0.0.0          ge1            0         ACG      -
10.150.0.0/24         0.0.0.0          ge7            0         ACG      -
10.190.0.0/24         0.0.0.0          ge4            0         ACG      -
127.0.0.0/8           0.0.0.0          lo             0         ACG      -
192.168.3.0/24        0.0.0.0          ge5            0         ACG      -
192.168.4.0/24        0.0.0.0          ge6            0         ACG      -
200.3.242.161/32      0.0.0.0          ge2_ppp        0         ACG      -
Router>
```

Tabelle 5: Routing unter Zyxel USG

Beispiele und Übungen für statisches Routing

In folgendem Beispiel haben wir ein Netzwerk mit drei Routern, einem Internetzugang und mehreren Teilnetzen.

Als Vorgabe erhalten wir folgende Angaben:

LAN A:	172.16.0.0 /23	512 Host (-2)
LAN B:	172.16.0.0 /24	256 Host (-2)
LAN C:	172.16.0.0 /22	1024 Host (-2)
LAN D:	172.16.0.0 /25	128 Host (-2)
LAN E:	172.16.0.0 /24	256 Host (-2)
LAN F:	172.16.0.0 /26	64 Host (-2)
Transit-LAN:	172.30.0.0 /30	4 Host (-2)
DMZ:	192.168.0.0 /27	32 Host (-2)

Der Default Gateway hat immer die höchste IP-Adresse.
Der ISP (Internet Service Provider) hat als Gateway 213.222.78.2 und gibt ihnen als statische IP-Adresse 213.222.78.1

Definition Transit-LAN
Ein Transit-LAN ist eine Verbindung zwischen zwei Router ohne dass weitere Geräte darin angeschlossen werden. Somit braucht es in einem Transit-LAN nur 4 IP-Adressen, also zwei nutzbare IP-Adressen.

Lösung:
Damit wir so wenige IP-Adressen wie möglich verbrauchen, sortieren wir die Bereiche der Grösse nach. Das grösste LAN zuerst und dann geht es weiter mit dem zweitgrössten LAN u.s.w.

LAN C:	172.16.0.0 /22	172.16.0.0	bis	172.16.3.255	1024 Host (-2)
LAN A:	172.16.0.0 /23	172.16.4.0	bis	172.16.5.255	512 Host (-2)
LAN B:	172.16.0.0 /24	172.16.6.0	bis	172.16.6.255	256 Host (-2)
LAN E:	172.16.0.0 /24	172.16.7.0	bis	172.16.7.255	256 Host (-2)
LAN D:	172.16.0.0 /25	172.16.8.0	bis	172.16.8.127	128 Host (-2)
LAN F:	172.16.0.0 /26	172.16.8.128	bis	172.16.8.191	64 Host (-2)
Transit-LAN:	172.30.0.0 /30	172.30.0.0	bis	172.30.0.3	4 Host (-2)
DMZ:	192.168.0.0 /27	192.168.0.0	bis	192.168.0.31	32 Host (-2)

Wir haben nun folgenden Netzwerkplan:

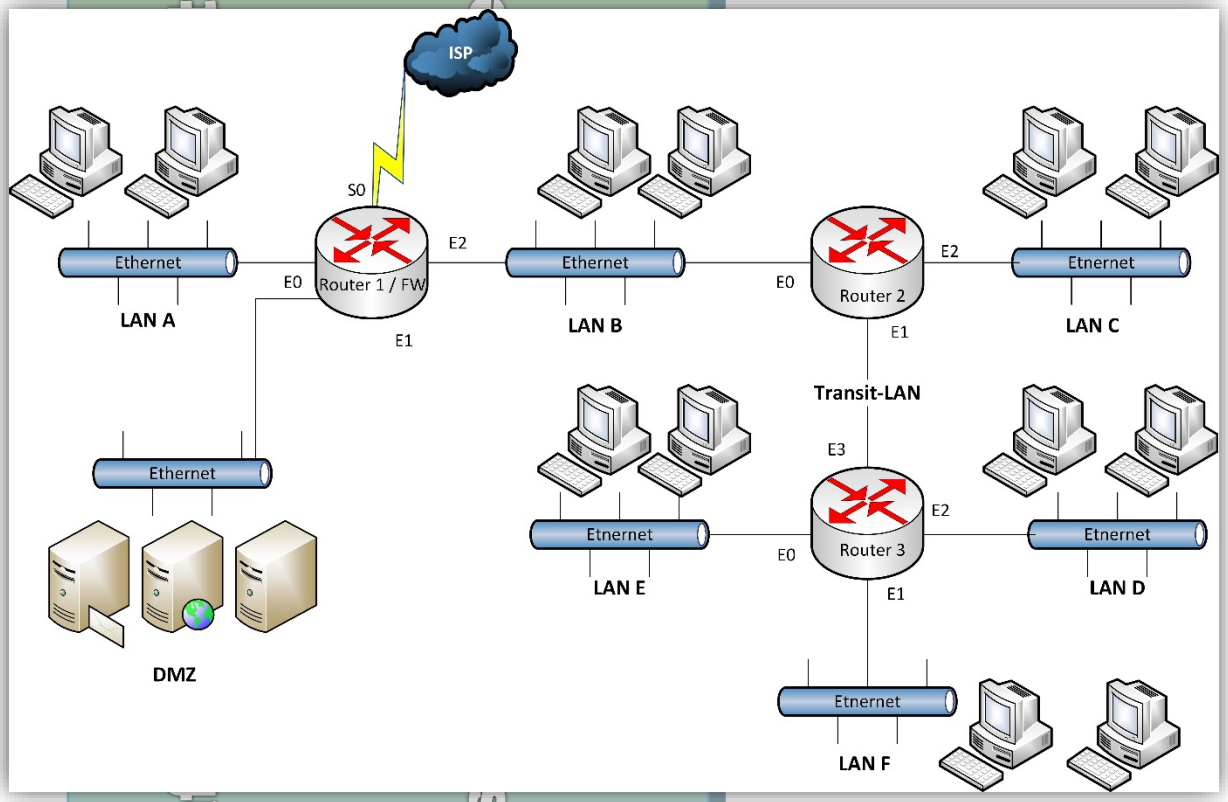


Abbildung 5 - Netzwerkplan für Routing

Folgende Regeln gilt es zu beachten:

- Das Netzwerkziel entspricht der Netz-ID
- Die Netzwerkmaske übernehmen wir von der errechneten Liste (oben)
- Ist das Zielnetz direkt am Router, dann ist der Gateway gleich der Schnittstelle
- Ist das Zielnetz nicht direkt am Router, ist der Gateway der nächste Router, den man vom Router wo wir die Routingtabelle machen direkt ansprechbar ist.
- Die Schnittstelle ist immer ein Ausgang am Router der aktuellen Routingtabelle (Beschriftet mit E0, E1, E2, S0, etc.)

Somit ergeben sich folgenden drei Routing-Tabellen:

Router 1

-	Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle
DGW	0.0.0.0	0.0.0.0	213.222.78.2	213.222.78.1
LAN A	172.16.4.0	255.255.254.0	172.16.5.254	172.16.5.254
LAN B	172.16.6.0	255.255.255.0	172.16.6.254	172.16.6.254
LAN C	172.16.0.0	255.255.252.0	172.16.6.253	172.16.6.254
LAN D	172.16.8.0	255.255.255.128	172.16.6.253	172.16.6.254
LAN E	172.16.7.0	255.255.255.0	172.16.6.253	172.16.6.254
LAN F	172.16.8.128	255.255.255.192	172.16.6.253	172.16.6.254
TL	172.30.0.0	255.255.255.252	172.16.6.253	172.16.6.254
DMZ	192.168.0.0	255.255.255.224	192.168.0.30	192.168.0.30

Tabelle 6 - Routingtabelle R 1

DGW steht für Default-Gateway / Default Routing
TL steht für Transit-LAN

Router 2

-	Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle
DGW	0.0.0.0	0.0.0.0	172.16.6.254	172.16.6.253
LAN A	172.16.4.0	255.255.254.0	172.16.6.254	172.16.6.253
LAN B	172.16.6.0	255.255.255.0	172.16.6.253	172.16.6.253
LAN C	172.16.0.0	255.255.252.0	172.16.3.254	172.16.3.254
LAN D	172.16.8.0	255.255.255.128	172.30.0.2	172.30.0.1
LAN E	172.16.7.0	255.255.255.0	172.30.0.2	172.30.0.1
LAN F	172.16.8.128	255.255.255.192	172.30.0.2	172.30.0.1
TL	172.30.0.0	255.255.255.252	172.30.0.2	172.30.0.2
DMZ	192.168.0.0	255.255.255.224	172.16.6.254	172.16.6.253

Tabelle 7 - Routingtabelle R 2

Router 3

-	Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle
DGW	0.0.0.0	0.0.0.0	172.30.0.2	172.30.0.1
LAN A	172.16.4.0	255.255.254.0	172.30.0.2	172.30.0.1
LAN B	172.16.6.0	255.255.255.0	172.30.0.2	172.30.0.1
LAN C	172.16.0.0	255.255.252.0	172.30.0.2	172.30.0.1
LAN D	172.16.8.0	255.255.255.128	172.16.8.126	172.16.8.126
LAN E	172.16.7.0	255.255.255.0	172.16.7.254	172.16.7.254
LAN F	172.16.8.128	255.255.255.192	172.16.8.190	172.16.8.190
TL	172.30.0.0	255.255.255.252	172.30.0.1	172.30.0.1
DMZ	192.168.0.0	255.255.255.224	172.30.0.2	172.30.0.1

Tabelle 8 - Routingtabelle R 3

VPN - Virtual Private Network

VPN steht für „Virtual Private Network“ oder „virtuelles privates Netz“. Dabei geht es um eine verschlüsselte Kommunikation zwischen zwei Punkten über das öffentliche Internet.

VPNs nutzen eine öffentliche Infrastruktur wie das Internet, um Systeme zu einem virtuellen Netzwerk zu verbinden, das ähnlichen Anforderungen an Vertraulichkeit und Sicherheit genügt, wie das LAN

Klassische VPN-Techniken
- PPTP
- IPSEc

Neuere VPN-Techniken
- SSL-VPNs
- OpenVPN
- Zero-Configuration VPNs

Alternativ: Provider VPNs z.B. mit MPLS auf Layer 2, meist ohne Verschlüsselung

Vertraulichkeit und Integrität

Starke Authentifizierung: Nur die Guten kommen rein
Starke Verschlüsselung: Wer nicht drin ist, sieht nur Kauderwelsch
Starke Authentisierung:
Eindeutig feststellbar, wer was „gesagt“ hat
VPNs brauchen starke Kryptographie

Point-to-Point Tunneling Protocol

Stammt von Microsoft
Nur Remote Access
Vorteile:
- Bei allen Windows-Versionen dabei
- Einfach zu benutzen

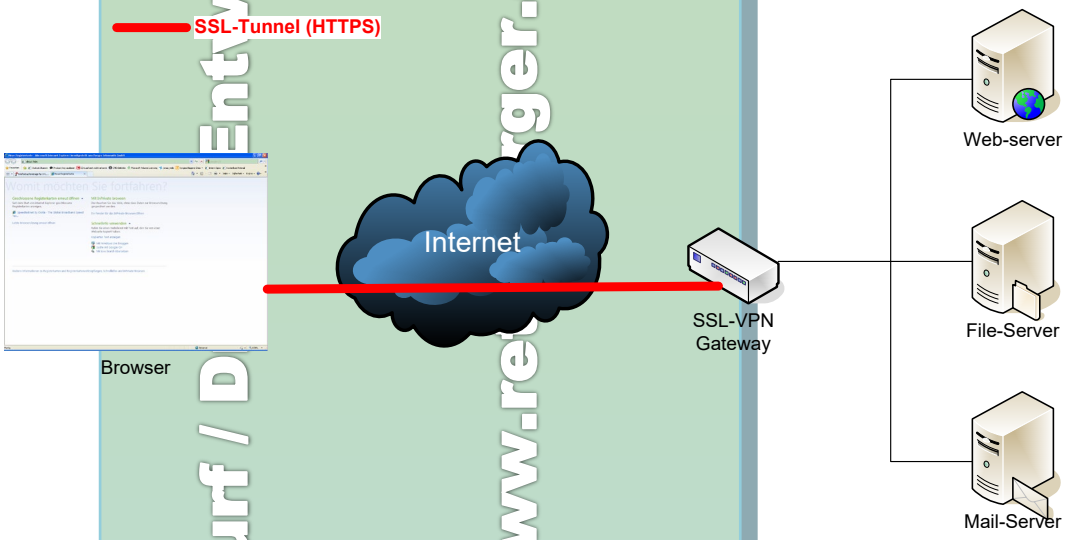
Nachteil: ……..

IP Security – kurz IPSec

Erweiterung des IP-Protokolls (für IPv6)
Familie von Protokollen und Standards
Der Standard für VPNs
Ursprünglich zur Koppelung von Netzen
Auch RAS (mit spez. Client Software)
Bei Microsoft in Kombination mit L2TP
Erweiterung wie NAT-T, Dead-Peer-Detection usw.

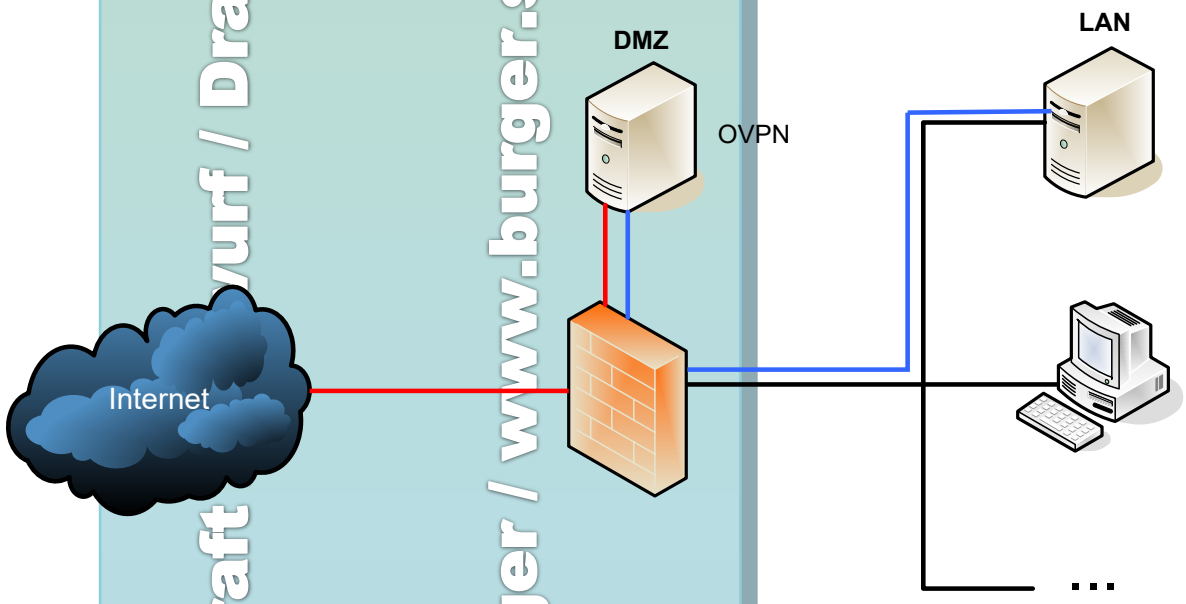
IPSec ist nach wie vor der De-Facto-Standard für VPNs.
Wenn man es richtig macht, ist es das sicherste Protokoll.
…aber eigentlich will man es zumindest für RAS nicht mehr benutzen müssen.

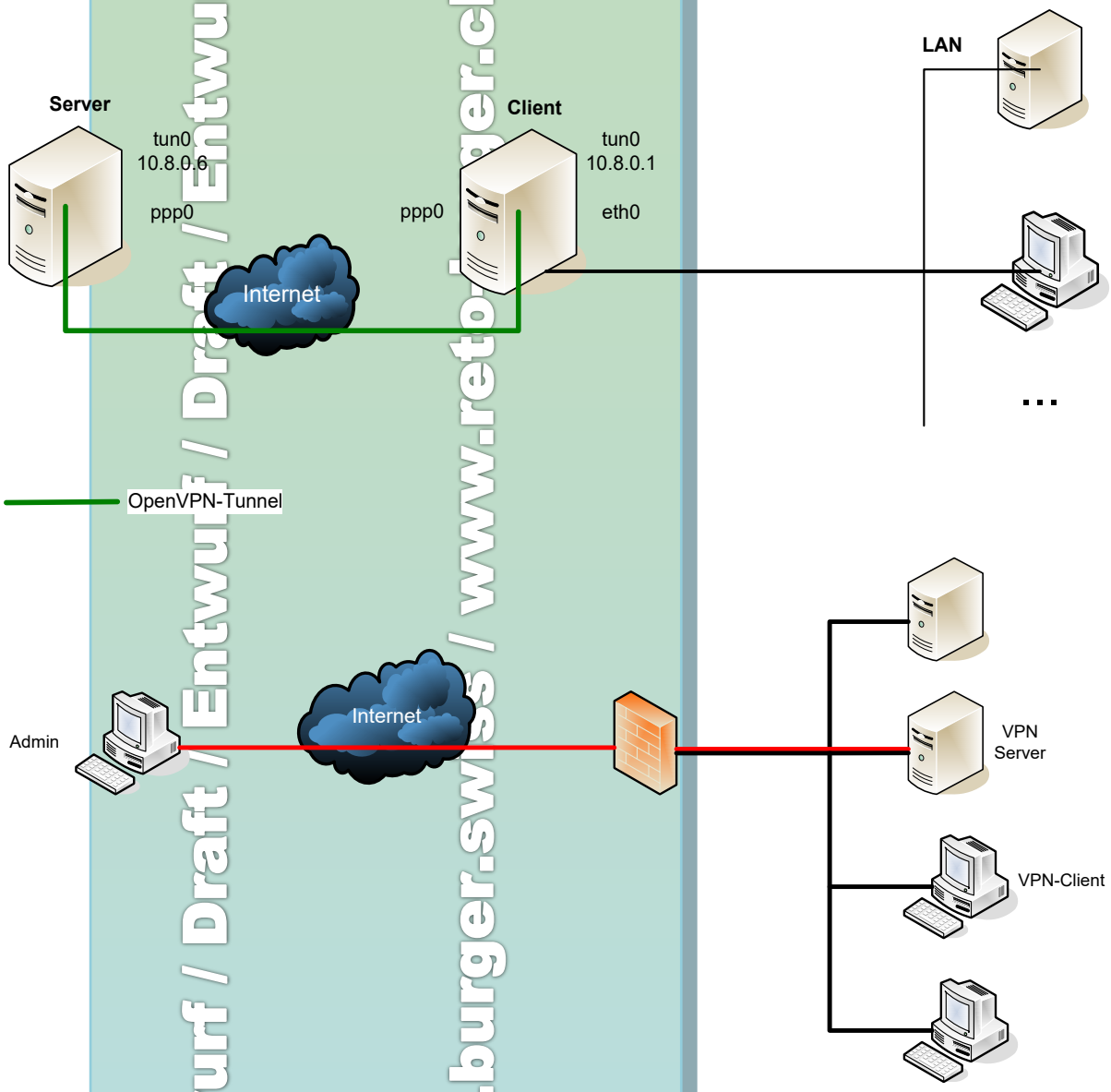
SSL-VPN



Keine oder zumindest einfache Client Installation. Jeder Browser kann es und mehr braucht man nicht (unbedingt)
Einfach zu wartende Appliances auf Server-Seite
Mobiler Zugang mit PDAs, BlackBerries usw.
SSL ist eine etablierte, stabile, bewährte Technik für Authentifizierung und Verschlüsselung
Flexible, feingranulare Zugriffssteuerung möglich

OpenVPN



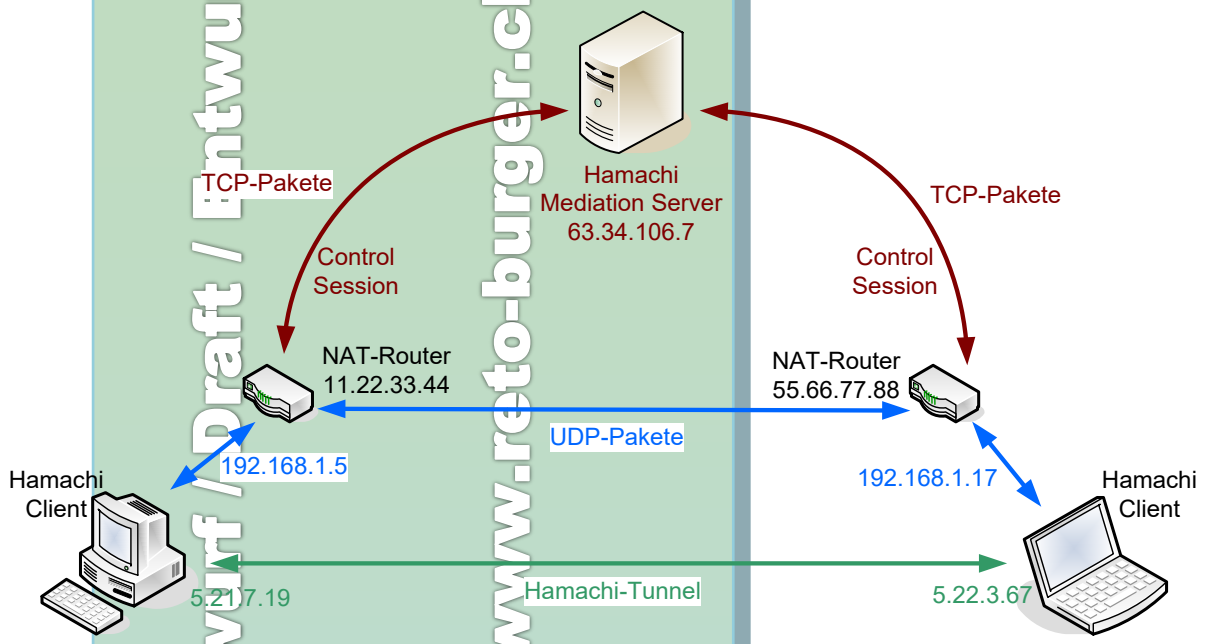


Vorteile

Nachteile

Hamachi

Bekannt aus der Gamer-Szene.



Übersicht

	PPTP	IPSec	SSL-VPN	OpenVPN
Authentifizierung	Passwort	Zertifikat/ Passwort	Passwort	Zertifikat
Protokolle	IP, IPX	IP	HTTP	IP
Transparenz	++	++	-	+
Policy-Enforcement	-	+	++	-
Plattformen	-	+	++	+
Mobilität	-	-	++	+
Management	-	+	+	-
Sicherheit	-	+	+ / ++	++

VPN Einsatzmöglichkeiten

Wir kennen folgende Möglichkeiten:

- Host to Host
- Host to Site
- Site to Site

Host to Host

Host to Site

Site to Site

Fazit zu VPN

Bei richtiger Einstellung ist VPN sehr sicher. Mit den vielen Varianten die es gibt, bei denen man beliebig viele und fast beliebig grosse Daten via Cloud-Lösungen austauschen kann, werden VPN's immer weniger gefragt. Dropbox, OneDrive, SharePoint etc. bieten sehr sichere Technologien um Daten über das öffentliche Netz auszutauschen.
Auch im Bereich der Fernwartung von Systemen wird heute statt eine VPN-Lösung zu alternativen wie TeamViewer zurückgegriffen, welche sehr einfach zu installieren und konfigurieren sind und dennoch als sehr sicher gelten (sofern richtig konfiguriert und sichere Passwörter hinterlegt sind).

CMD – Befehle für‘s Netzwerk

Befehl	Parameter	Info
Ping		
	-a	Zeigt Namensauflösung an
	-n 1	Macht zum Host nur ein Ping (nur eine Echoanforderung)
	-w 5	Zeitlimit in Millisekunden für die einzelne Antwort
tracert (traceroute)		
	-d	Unterdrückt Namensauflösung
ipconfig		
	/all	Zeigt alle Einstellungen der lokalen Netzwerkeinstellungen aller Adapter an
	/flushdns	Lokaler DNS-Cache löschen
arp		
	-a	ARP-Tabelle anschauen
	-s	Neuen Eintrag setzen
	-d	Statischen Eintrag löschen
route print		Zeigt die Routingtabelle an
netstat		
	-r	Wie route print
telnet		
nslookup		Für Abfragen verschiedener DNS-Einstellungen
finger		Ist eigentlich ein alter Befehlt, welcher aber mit den neusten Systemen noch unterstützt wird.

Tabelle 9: CMD Netzwerkbefehle

Natürlich haben viele der oben aufgeführten Befehle noch viele weitere Parameter. Die oben erwähnten sind jene, die in der Regel am häufigsten gebraucht werden.
Tabelle noch im Aufbau!

DNS

Domain Name System (auch Domain Name Server und Domain Name Service genannt) ist ein hierarchischer, (de)zentraler Verzeichnisdienst für Namensauflösung von IP-Adressen und umgekehrt.

DNS kann mit folgenden Eigenschaften beschrieben werden:
- Dezentrale Verwaltung
- Eindeutigkeit der Namen
- Beliebige Erweiterbarkeit
- Namensraums in hierarchischer, baumförmiger Struktur

DNS Aufbau und Begriffe

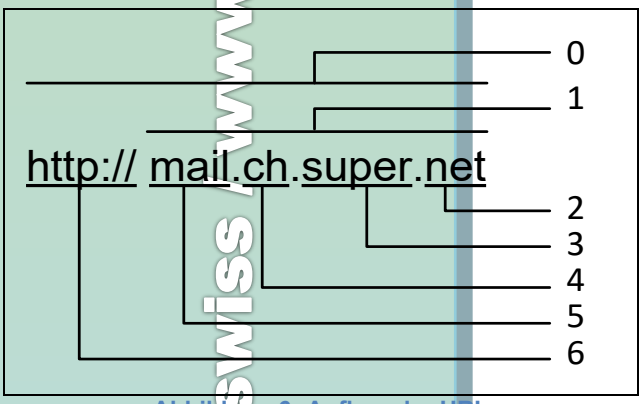


Abbildung 6: Aufbau der URL

0. URL / Uniform Resource Locator
1. FQDN / Fully Qualified Domain Name
2. TLD Top Level Domain
3. Domain
4. Subdomain
5. Host
6. Schema / URL-Zugriffsmethode (für die URI) (Doppelpunkt gehört dazu)

URI: Uniform Resource Identifier
URL: Uniform Resource Locator
URN: Uniform Resource Name

Die beiden slashes (//) nach http: sind eigentlich funktionslos und müssten nicht eingegeben werden. Das hat sich im Verlauf der Jahre einfach so festgeankert, dass es heute normal wurde, dies so einzugeben.

TLD

Die **T**op **L**evel **D**omain ist die oberste Hierarchie im Aufbau des DNS. Dem übergeordnet sind nur noch die Rootserver, welche auf die TLDs verweisen.

Hier gibt es folgende Gruppen:
- Länder-Kürzel nach ISO
- Generische Kürzel
- test

- infrastructure
- sponsored
- generic-restricted

Kapitel noch im Aufbau

Domain

Die Domain kann (fast) frei definiert werden. Ein paar Einschränkungen gibt es:
….
Kapitel noch im Aufbau

DNS Abfragen

Nslookup
Zeigt Informationen an, die Sie zur Diagnose der DNS-Infrastruktur (Domain Name System) verwenden können. Bevor Sie dieses Befehlszeilenprogramm verwenden, sollten Sie sich mit der Funktionsweise von DNS vertraut machen. Das Befehlszeilenprogramm Nslookup steht nur zur Verfügung, wenn Sie TCP/IP installiert haben.

Syntax

```
nslookup [-Unterbefehl ...] [{ZuSuchenderComputer| [-Server]}]
```

Beispiele:
Zeigt alle Einträge der Zone / Domäne ithelp.ch an:

```
nslookup -ty=any ithelp.ch
  oder
nslookup -type=any ithelp.ch
  oder
nslookup -querytype=any ithelp.ch
  oder
nslookup -ty=all ithelp.ch
```

Die Abfrage lautet: nslookup –type=“xxx“ domain. Statt –type= kann auch –ty= eingegeben werden. Für „xxx“ können folgende Einträge gemacht werden:

A ->	Gibt die Host-IP-Adresse an.
AAAA ->	Gibt die Host-IP-Adresse IPv6 an.
ALL, ANY ->	Alle Datentypen.
CNAME ->	Gibt einen kanonischen Namen für einen Alias an.
GID ->	Gibt einen Gruppenbezeichner eines Gruppennamens an.
HINFO ->	Gibt den Computerprozessor und die Betriebssystemart an.
MB ->	Gibt einen Mailbox-Domänennamen an.
MG ->	Gibt ein Mailgruppenmitglied an.
MINFO ->	Gibt Mailbox- oder Maillisten-Informationen an.
MR ->	Gibt den Mailumbenennungs-Domänennamen an.
MX ->	Gibt den Mail-Exchanger an.
NS ->	Gibt einen DNS-Namenserver für die benannte Zone an.
PTR ->	Gibt einen Hostnamen an, falls es sich bei der Abfrage um eine IP-Adresse handelt, sonst den Zeiger auf andere Informationen.
SOA ->	Gibt den Autoritätsursprung für eine DNS-Zone an.
TXT ->	Gibt die Textinformationen an. Wird gerne für SPAM-Schutzeinstellungen gebraucht.

UID -> Gibt die Benutzerkennung an.
UINFO -> Gibt die Benutzerinformationen an.
WKS -> Beschreibt einen bekannten Dienst.

Beispiele:
Gesucht sind die SOA-Einträge der Domain google.ch welche auf dem Server mit der IP-Adresse 8.8.8.8 gespeichert (oder im Cache) sind.

```
> nslookup -ty=soa google.ch 8.8.8.8
```

Antwort:

```
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Nicht autorisierende Antwort:
google.ch
        primary name server = ns2.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 1580684
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

Gesucht sind die DNS-Einträge für den Mailserver der Domain admin.ch vom Server welcher in der lokalen IP-Konfiguration eingestellt ist (myserver.mydomain.local):

```
> nslookup -ty=mx admin.ch
```

Antwort:

```
Server:  myserver.mydomain.local
Address:  10.10.0.1

admin.ch        MX preference = 10, mail exchanger = mailgate2.admin.ch
admin.ch        MX preference = 10, mail exchanger = mailgate1.admin.ch
admin.ch        nameserver = ins2.admin.ch
admin.ch        nameserver = ins3.admin.ch
admin.ch        nameserver = ins1.admin.ch
mailgate1.admin.ch      internet address = 162.23.32.31
mailgate2.admin.ch      internet address = 162.23.32.32
ins1.admin.ch   internet address = 162.23.37.16
ins2.admin.ch   internet address = 162.23.37.160
ins3.admin.ch   internet address = 212.103.72.85
```

DHCP

DHCP-Relay-Agent

WINS

Nächste Themen:

Leitungsvermittelte Dienste
Paketvermittelte Dienste
ATM, etc.

Das OSI-Referenzmodell

(Open System Interconnect, Kapselung nach unten)

7. Anwendungsschicht (Application Layer)

- keine normierten Protokolle
- Servicefunktionen wie SQL möglich
- BSP: NFS(Fileservices), EDI- oder X-Windows-Fkt

6. Darstellungschicht (Presentation Layer)

- Daten werden den konkreten Anforderungen angepasst
- Kodierung der Datentypen
- Transformieren von Datenstrukturen
- Wechsel von Zeichensätzen (maschinenabhängig)
- Kompression und Verschlüsselung
- Protokolle: XDR

5. Sitzungsschicht (Session Layer)

- Bedeutet Nutzung eines Systems oder Teilsytems für einen bestimmten Anwender oder Aufgabe
- Koordiniert Aufnahme, Durchführung und Beendigung der Verbindung
- Zuständig für Auf- Abbau und Überwachung der Verbindung
- BSP : Login Procedur eines Benutzers Verwaltung von Speicher und Prioritäten
- Protokolle: LU6.2 oder RPC (UNIX)

4. Transportschicht (Transport Layer)

- Schnittstelle zwischen Kommunikationsnetzwerk unterhalb und Applikation oberhalb
- Trägt Verantwortung für für die Zuverlässigkeit der Übertragung
- Aufteilung der Netzwerkressourcen an die Applikationen (Multiplexen)
- Protokolle:
  - Verbindungslos
  - Verbindungsorientiert
- Application Programming Interface (API) möglich (SOCKET von UNIX)
- Protokoll: TCP, UDP(TCP/IP),TP0-TP4

3. Vermittlungsschicht (Network Layer)

- Betrifft das ganze Netzwerk
- Vermittlung und Wegleitung der Netzknoten (Routing)
- Segmentation der Informationen in Pakete und Datenflusskontrolle auf Paketebene
- Bei Empfang zusammenstellen der Pakete und Weiterlieferung der Pakete als Information an die Transportschicht
- Protokoll: X.25, IP (Inernet Protokoll (TCP/IP)),
  ISO/OSI 8473, 9574 (ISO/OSI Protokoll)

2. Sicherungsschicht (Link Layer)

- Aufteilung, wenn nötig, in Infoblöcke von x*100-4KB
- Zusammenfassen in einer Struktur (Frames)
- Übermittlung nur an die gleiche Empfängerschicht
- Verantwortlich für den Datentransfer über den physikalischen Kanal
- Zuständig für:
  - Synchronisation
  - Adressieren der angeschlossenen Stationen
  - Teilweise die Flusskontrolle
  - Detektion von Übertragungsfehlern
  - Behebung von Übertragungsfehlern
  - Parameteraustasch
- eher softwareorientiert

- Netzwerkkarten des PC unterstützen normal die ersten beiden Layer
- Dienste:
  - unbestätigte verbindungsunabhängige Dienste
  - bestätigte verbindungsunabhängige Dienste
  - Verbindungsorientierte Dienste
- Protokoll: Ethernet (IEEE802.3),Tokenring(IEEE802.5) FDDI, HDLC, SDLC

1. Bitübertragungsschicht (Physical Layer)

- Regelt Austausch einzelner Bits über das Übertragungsmedium
- Geregelt werden:
  - Übertragungsgeschwindigkeit
  - Bitcodierung
  - Übermittlungsmodus (Duplex, Halb duplex)
  - Anschlussart

Welche Aktivkomponenten gehören zu welchem OSI-Layer?

Begriff Passiv- und Aktivkomponenten:

Passivkomponenten:
Als passive Netzwerkkomponenten wird das Material bezeichnet, das ohne jegliche Stromversorgung auskommt. Dazu zählen insbesondere: Leitungen, Kabel und Patchkabel, Anschlussdosen, Stecker und Buchsen. Baugruppen, die lediglich passive Bauelemente enthalten (also Widerstände, Kondensatoren usw.) wie z. B. die DSL-Splitter, werden meistens auch dieser Gruppe hinzugerechnet.

Aktivkomponenten:
Aktive Netzwerkkomponenten sind alle Geräte, die aktiv Signale verarbeiten bzw. verstärken können. Sie benötigen dazu eine Stromversorgung. Zu dieser Gruppe gehören Hubs und Switches, Router, Bridges, Firewalls und Session Border Controller. Ein Bestandteil eines Computers kann ebenfalls eine Netzwerkkomponente sein, z. B. Netzwerkkarte und ISDN-Karte.

OSI-Layer	Geräte	Geräte	OSI-Layer
Layer 7	Proxy	Gateway Firewall	Layer 7
Layer 6			Layer 6
Layer 5			Layer 5
Layer 4	L4-Switch		Layer 4
Layer 3	Router L3-Switch AccessPoint		Layer 3
Layer 2	Bridge Switch Modem AccessPoint		Layer 2
Layer 1	Repeater Hub NIC		Layer 1

Tabelle 10: OSI-Layer und Geräte

Der Gateway arbeitet primär in den Layern 3-7.
Da der Gateway jedoch auch als Medienkonverter (Layer 1) oder als Brücke zwischen verschiedenen Netzwerk-Topologien (Ethernet zu Tockenring oder xDSL etc.) (Layer 2) eingesetzt werden kann, wird et oft auch allen 7 OSI-Layern zugeordnet.

Einführung in IPv6

Kapitel in Arbeit

Glossar

Abkürzung	Ausgeschrieben	Beschreibung
CMD	Command	Windows Eingabeaufforderung
DHCP	Dynamic Host Configuration Protokoll	Zuweisung der Netzwerkkonfiguration an Clients durch einen Server
DNS	Domain Name System	Beantwortung von Anfragen zur Namensauflösung
FQDN	Fully Qualified Domain Name	Bsp. www.reto-burger.ch
FTP	File Transfer Protokoll	Ermöglicht den Datenaustausch über das Internet zwischen Client und Server
FTPS	File Transfer Protokoll Sesure	FTP über SSL oder FTP over TLS
HTTP	HyperText Transfer Protocol	Protokoll zur Datenübertragung an den Webbrowser
HTTPS	HyperText Transfer Protocol Secure	http mit SSL zur sicheren Datenübertragung des http
ICMP	Internet Control Message Protocol	Zum Austausch von Informations- und Fehlermeldungen. Bekannter Befehl: ping
OSI-Modell	Open Systems Interconnection Model	Referenzmodell für Netzwerkprotokolle als Schichtenarchitektur dargestellt mit 7 Schichten / 7 Layer
SFTP	SSH File Transfer Protocol	FTP über SSH
SMTP	Simple Mail Transfer Protokoll	Protokoll zum Austausch vom E-Mails in Computernetzwerken
SNMP	Simple Network Management Protocol	Protokoll zur Überwachung, Fernsteuerung und Fehler-benachrichtigung von Netzwerkkomponenten
SSL	Secure Sockets Layer	Ist die alte Bezeichnung von TLS
TLD	Top Level Domain	Bsp.: .com, .ch, .info, .net, .org. u.v.m.
TLS	Transport Layer Security	weitläufiger bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL). Bezeichnung TLS seit Version 3.0 hybrides Verschlüsselungs-protokoll zur sicheren Daten-übertragung im Internet
UNC	Uniform Naming Convention	(auch Universal Naming Convention) Bsp.: \\server1\freigabe oder \\10.10.0.1\austausch\dokus-free
URI	Uniform Resource Identifier	einheitlicher Bezeichner für Ressourcen Bsp.: http:
URL	Uniform Resource Locator	Bsp.: http://www.reto-burger.ch
WINS	Windows Internet Naming Service	Eine Umsetzung des Netzwerkprotokolls NetBIOS over TCP/IP durch Microsoft

Tabelle 11: Glossar

Verzeichnisse / Index

Abbildungsverzeichnis

Tabellenverzeichnis

Index

Autor:

Reto Burger, Eidg. dipl. Informatik Ingenieur HTL / FH, dipl. Berufsfachschullehrer mit Jahrgang 1968 aus Sempach (Schweiz).

Reto Burger ist Prüfungsexperte, Validator für Abschlussprüfungen in der Zentralschweiz, Lehrer und Dozent an verschiedenen Technikerschulen, Gewerbe- und Berufsschulen und an Hochschulen in der deutschsprachigen Schweiz.

Weiter ist Burger für die Modulentwicklung verschiedener ÜK's Verantwortlich und auch als Autor tätig. Burger war mehrere Jahre in der Kurskommission des VFI's engagiert und ist selber Lehrmeister.
Er hat für I-CH bei mehreren Netzwerk- und Systemtechnik–Module im Aufbau aktiv mitgearbeitet und war verantwortlich für verschiedene Module für die Ausbildung des Berufes gesamtschweizerisch.

Autor von:

- IP-Rechnen kann so einfach sein!
- Netzwerkgrundlagen
- Regular Expressions
- Rund um das Backup
- WLAN Sicherheit
- Firewalls und wie setze ich sie ein

Rechte

Garantie

Alle in diesem Stoff enthaltenen Berechnungen, Daten und Fakten wurden nach bestem Wissen erstellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschliessen. Aus diesem Grund sind die im vorliegenden Stoff enthaltenen Informationen mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Referenzen

Im Internet

www.burger.swiss
www.reto-burger.ch
www.bsi.de
usw.

In Literatur

Danke
Wenn Ihnen die Dokumentation gefallen hat, dürfen Sie das gerne mit einem kleinen Betrag via PayPal zeigen. paypal@burger.swiss Danke.