CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

System- und Netzwerk-administration

CloudCommand GmbH chr.schumacher@gmx.tm

Adressierung

Was sind Protokolle

- Ein Netzwerkprotokoll (auch Netzprotokoll) ist ein Kommunikationsprotokoll für den Austausch von Daten zwischen Computern bzw. Prozessen, die in einem Rechnernetz miteinander verbunden sind (verteiltes System).
- Die Vereinbarung besteht aus einem Satz von Regeln und Formaten (Syntax), die das Kommunikationsverhalten der kommunizierenden Instanzen in den Computern bestimmen (Semantik).
- Der in einem Protokoll beschriebene Aufbau eines Datenpaketes enthält für den Datenaustausch wichtige Informationen über das Paket wie beispielsweise:
    - dessen Absender und Empfänger, damit Nicht-Empfänger das Paket ignorieren

Was sind Protokolle

  - den Typ des Pakets (beispielsweise Verbindungsaufbau, Verbindungsabbau oder reine Nutzdaten)
  - die Paketgröße, die der Empfänger zu erwarten hat
  - bei mehrteiligen Übertragungen die laufende Nummer und Gesamtzahl der Pakete
  - eine Prüfsumme zum Nachvollziehen einer fehlerfreien Übertragung
- Diese Informationen werden den Nutzdaten als Header vorangestellt oder als Trailer angehängt.

Geschichte TCP

- Anfang der siebziger Jahre von der amerikanischen Behörde DARPA (Defence Advanced Research Projects Agency) als Standardprotokoll für das ARPANET entwickelt.

Der Entwicklungsgedanke:

- weg von einer festen leitungsgebundenen Kommunikation
- hin zur paketorientierten offenen Kommunikation
- unabhängig von Hardware /Übertragungstechnik
- Pakete sollen durch intelligente Vermittler Stationen (Router) auch bei einem teilweise zerstörten Kommunikations-Netz, immer noch sicher ans Ziel zu kommen

Geschichte TCP

- Insgesamt fünf Versionen wurden entwickelt: TCP v1, TCP v2, das aufgesplittete TCP v3/IP v3 und danach das stabile TCP/IP v4
- TCP/IP v6 ist das neueste Protokoll

- Übrigens: IPv5 gibt es nicht. Diese Nummer war ursprünglich für das Internet Stream Protocol v2 reserviert, die Entwicklung wurde aber eingestellt zu Gunsten von IPv6.

Die IP Adresse

- IP steht für Internet Protocol (Internet steht für Interconnected Network).
- Die IP Adresse identifiziert einen Teilnehmer / Knoten im Netzwerk.

Was haben eine Telefonnummer und eine IP Adresse gemeinsam?

Die IPv4 Adresse

Aufbau einer IP Adresse:

- Aus Sicht der Anwender:
  150.122.5.230

- Was der Rechner sieht:
  10010110 01111010 00000101 11100110

Binäres Zahlensystem

Stellenwert:	$Basis^5$	$Basis^4$	$Basis^3$	$Basis^2$	$Basis^1$	$Basis^0$
Binär/Dual (2)	2^5	2^4	2^3	2^2	2^1	2^0
	2x2x2x2x2	2x2x2x2	2x2x2	2x2	1x2	1
Nennwert	32er	16er	8er	4er	2er	1er
mögl. – Ziffernwerte 0,1	1	0	1	1	0	1

128	64	32	16	8	4	2	1
1	1	1	1	0	0	0	0

- 128 + 64 + 32 + 16 + 0 + 0 + 0 + 0 = 240
- Die dezimale Zahl für die duale $1111\,0000_2$ ist also 240_{10}

Die IPv4 Adresse

Der Aufbau einer IP Adresse:

- 150.122.5.230
- 10010110 01111010 00000101 11100110

Eine IP Adresse besteht immer aus einem Netz- und einem Host-Anteil.

Vergleichbar mit einer Telefonnummer: Vorwahl und Rufnummer

150	100	50	100
Netz (N)	Netz (N)	Host (H)	Host (H)

IP-Adress-Klassen

Class A	Netz	Host	Host	Host
Class B	Netz	Netz	Host	Host
Class C	Netz	Netz	Netz	Host

IP-Adress-Klassen

Wo steht die erste 0?

	128	64	32	16	8	4	2	1
Class A	**0**	x	x	x	x	x	x	x
Class B	1	**0**	x	x	x	x	x	x
Class C	1	1	**0**	x	x	x	x	x

- An erster Stelle - Class A - Adresse.
- An zweiter Stelle - Class B - Adresse.
- An dritter Stelle - Class C - Adresse

IP-Adress-Klassen

- **Class A:** 0000 00002 – 0111 11112 = 000_{10} – 127_{10}
- **Class B:** 1000 00002 – 1011 11112 = 128_{10} – 191_{10}
- **Class C:** 1100 00002 – 1101 11112 = 192_{10} – 223_{10}

IP-Adress-Klassen

Mögl. Anzahl	1. Byte	2. Byte	3. Byte	4. Byte
Class A	0 - 127	0.0.1 - 255.255.254 = **16.777.214** Hosts / Netz		
Class B	128 - 191	0-255	0.1 - 255.254 = **65.534** Hosts / Netz	
Class C	192 - 223	0-255	0-255	1 - 254 **= 254** Hosts /Netz
Class D	224 - 239	Verwendung für Multicast-Anwendungen (Router – Router)		
Class E	240 - 255	reserviert (zur Entwicklung)		

Subnetzmaske

- Ein zweiter Parameter zusätzlich zur IP-Adresse
- Eine 32 Bit große Maske, die dezimal angegeben wird z.B. 255.255.0.0
- Gibt an, wie viele Bits in der IP-Adresse den Netzanteil ausmachen, und wie viele für die Hosts benutzt werden.
- Die Netzmasken aller zusammengehörigen Rechner im selben IP-Netz, sollten gleich konfiguriert sein.

Subnetzmaske

Netzanteil: duale 1

Hostanteil: duale 0

Class A Netzmaske dual:

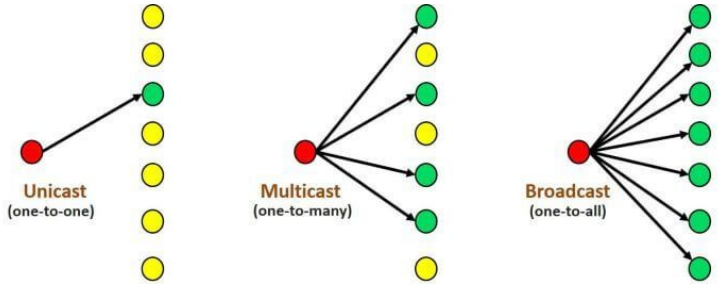
- 1111 1111 . 0000 0000 . 0000 0000 . 0000 0000

Dezimal:

- 255.0.0.0 Class A (Standard) Netz Maske
- 255.255.0.0 Class B (Standard) Netz Maske
- 255.255.255.0 Class C (Standard) Netz Maske

Reservierte und Spezielle IP Adressen

- **Netzadresse:** Alle Hostbits auf dual 0 z.B.:150.100.0.0
- **Broadcast:** Alle Hostbits auf dual 1 z.B.:150.100.255.255
- **Unicast**
- **Multicast**



Reservierte und Spezielle IP Adressen

- **Loopback Adresse:** Netz 127.0.0.0 z.B.:127.0.0.1
- **default Route** in Routingtabellen: Alle Netzwerkbits auf 0, also 0.0.0.0
- **Globaler Broadcast:** Alle Netzwerk Bits auf 1 z.B.: 255.255.255.255

Subnetting

- **Subnetting:** das Bilden von Unternetzen (Subnetze/ Subnets) um ein Class A, B – oder C besser verwaltbar zu machen.
- Um Subnetze adressieren und bilden zu können opfert der Administrator / Systemarchitekt einen Teil der IP-Adresse der eigentlich für Hosts reserviert ist.
- immer mit dem höchst wertigsten Host-Byte und Host-Bit anfangen
- Die Bits für Subnetze müssen zusammenhängend sein.
- In der Subnetzmaske ist jede duale 1 im ursprünglichen Host Bereich ein Subnetz-Bit.
- jede duale 0 im ursprünglichen Host Bereich weiterhin ein Host-Bit

Subnetting

dezimal	128	64	32	16	8	4	2	1
128	1	0	0	0	0	0	0	0
192	1	1	0	0	0	0	0	0
224	1	1	1	0	0	0	0	0
240	1	1	1	1	0	0	0	0
248	1	1	1	1	1	0	0	0
252	1	1	1	1	1	1	0	0
254	1	1	1	1	1	1	1	0
255	1	1	1	1	1	1	1	1

CIDR - Classless Inter Domain Routing

- Mit CIDR entfallen die starren Netzklassen (Class A – Class D).
- Durch die zusätzliche Angabe einer frei wählbaren Netzmaske (Suffix) wird jetzt die IP-Adresse in den neuen Netzwerk- und Hostteil aufgeteilt.
- Das Suffix wird einfach an die IP-Adresse angehängt, getrennt durch einen Schrägstrich. z.B.: 10.17.5.100/16
- Die „CIDR Notation“ 10.17.5.100/16 entspricht somit der Adresse:
    - 10.17.5.100 mit der Netzmaske 255.255.0.0

Sonderform:

- Das Suffix /32 adressiert kein Netz/Subnetz, sondern gibt immer nur einen einzelnen Host an.

Subnetting Übung

Gegeben:

- Netz: IP 192.168.168.0
- Netzmaske: 255.255.255.0
- (Oder anders geschrieben: 192.168.168.0/24)

Aufgabe:

- Das vorhandene Netz in 4 Subnetze unterteilen.

Subnetting Übung

Schritt 1:

- Damit ein Netz in kleinere Subnetze unterteilt werden kann, soll der Netzanteil um bestimmte Anzahl von bits in der Netzmaske erweitert werden.
- Im ersten Schritt wird also diese Anzahl von bits berechnet.
- Die Anzahl der notwendigen bits ist von der Anzahl der notwendigen Subnetze abhängig.

Anzahl von bits :	1	2	3	4	5	6	7	8	...
Anzahl der Subnetze :	2	4	8	16	32	64	128	256	...

Subnetting Übung

Schritt 1:

- Mit 1 bit können 2^1 = 2 Subnetze aufgebaut werden.
  - Es sind aber 4 Subnetze notwendig.
- Mit 2 bits können wir 2^2=4 Subnetze aufbauen.
  - Der Netzteil muss also um 2 bits erweitert werden.

Subnetting Übung

Zwischenschritt:

- Den Hostanteil in Binärzahl umrechnen.
- Hier werden nur die Oktette in die Binärzahl umgerechnet, die in der Netzmaske nicht gleich als 255 sind. → (In diesem Beispiel: 255.255.255.0)

- IP-Adresse: 192.168.168.0
- Netzmaske: 255.255.255.0
  - 192.168.168.00000000
  - 255.255.255.00000000

Subnetting Übung

Schritt 2:

- Den Netzanteil um 2 bits erweitern.
- IP-Adresse: 192.168.168.00000000
- Netzmaske: 255.255.255.00000000
    - 192.168.168.00000000
    - 255.255.255.11000000

- Der Netzanteil wurde um 2 bits in der Netzmaske erweitert. (Von links nach rechts)
    - Dadurch verschiebt sich die Grenze zwischen dem Hostanteil und Netzanteil nach rechts.

Subnetting Übung

Schritt 3:

- Ist nun der Netzanteil um 2 bits erweitert, haben wir automatisch die Subnetzadresse vom 1. Subnetz:
  - IP-Adresse: 192.168.168.00000000
  - Netzmaske: 255.255.255.11000000
- Der Hostanteil besteht aus 6 bits (farbig markiert).

- Das heißt jedem Subnetz stehen 26 = 64 IP Adressen zur Verfügung:
  - **1x:** für Netz-ID
  - **62x:** für Hosts (Host-IP-Range)
  - **1x:** für Broadcast

Subnetting Übung

Schritt 4:

- Das letzte Oktett von der Subnetzadresse wieder Dezimalzahl umrechnen.
  - IP-Adresse: 192.168.168.00000000
  - Netzmaske: 255.255.255.11000000

  - IP-Adresse: 192.168.168.0
  - Netzmaske: 255.255.255.192

Hilfsmittel

Dezimalzahl	Binärzahl
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110
255	11111111

Subnetting Übung

Schritt 5:

- Broadcast vom 1. Subnetz berechnen.
- Im Broadcast werden alle Hostbits auf 1 gesetzt.

- 192.168.168.00000000
  - 192.168.168.00111111

Subnetting Übung

Schritt 6:

- Das letzte Oktett von Broadcast in Dezimalzahl umrechnen:
- 192.168.168.00111111 → 192.168.168.63

Schritt 7:

- Subnetzadresse und Broadcast vom 1. Subnetz

Subnetzadresse/ Netz ID:	**Host-IP-Range:**	**Broadcast:**
192.168.168.0	192.168.168.1 - 192.168.168.62	192.168.168.63

Subnetting Übung

Schritt 8:

- Erhöht man die Broadcast IP um 1, bekommt man die Subnetzadresse vom nächsten Subnetz

Subnetting Übung

Schritt 9:

- Die IP Adresse um 63 (62 Host-Range-IPs +1 Broadcast IP) erhöhen = Broadcast: 192.168.168.64 + 63 = 127

Subnetzadresse/ Netz ID:	Host-IP-Range:	Broadcast:
192.168.168.0/26	192.168.168.1 - 192.168.168.62	192.168.168.63
192.168.168.64/26	192.168.168.65 - 192.168.168.126	192.168.168.127
192.168.168.128/26	192.168.168.129 - 192.168.168.190	192.168.168.191
192.168.168.192/26	192.168.168.193 - 192.168.168.254	
192.168.168.255		

Magic Numbers

1. Interessantes Oktett der IP und der Subnetzmaske finden und markieren. (Das Oktett vor dem 0er Oktett bzw das letzte Oktett, wenn kein 0er Oktett vorhanden)
2. Bekannte Daten schon mal hinschreiben bei SN und BC (Die Oktette bei denen die SM 255 oder 0 ist).
3. Magic Number errechnen (256 – interessantes Oktett der SM).
4. Herausfinden, wie oft die MN ganzzahlig in das interessante Oktett der IP passt und das Ergebnis von MN x Ganzzahl beim SN eintragen.
5. BC errechnen – Interessantes Oktett von SN + MN – 1

Magic Numbers

Beispiele:

IP: 189.178.33.17	CIDR /20 = 11111111.11111111.11110000.00000000
SM:255.255.240.0	MN= 256 – 240 = 16
SN: 189.178.32.0	BC: 189.178.47.255
IP: 199.38.22.99	CIDR /23 = 11111111.11111111.11111110.00000000
SM: 255.255.254.0	MN=256 – 252 = 2
SN: 199.38.22.0	BC: 199.38.23.255

Private IP Adressen

	Netz Adressbereich	Anzahl Netze gemäß Netzklasse
Class A	**10.0.0.0**	**1** privates Netz mit 16.777.214 Adressen
Class B	**172.16.0.0** **172.17.0.0** **172.18.0.0** ... bis **172.31.255.255**	**16** private Netze mit jeweils 65.534 Adressen
Class C	**192.168.0.0** **192.168.1.0** **192.168.2.0** ... bis **192.168.255.0**	**256** private Netze mit jeweils 254 Adressen

APIPA (local link)

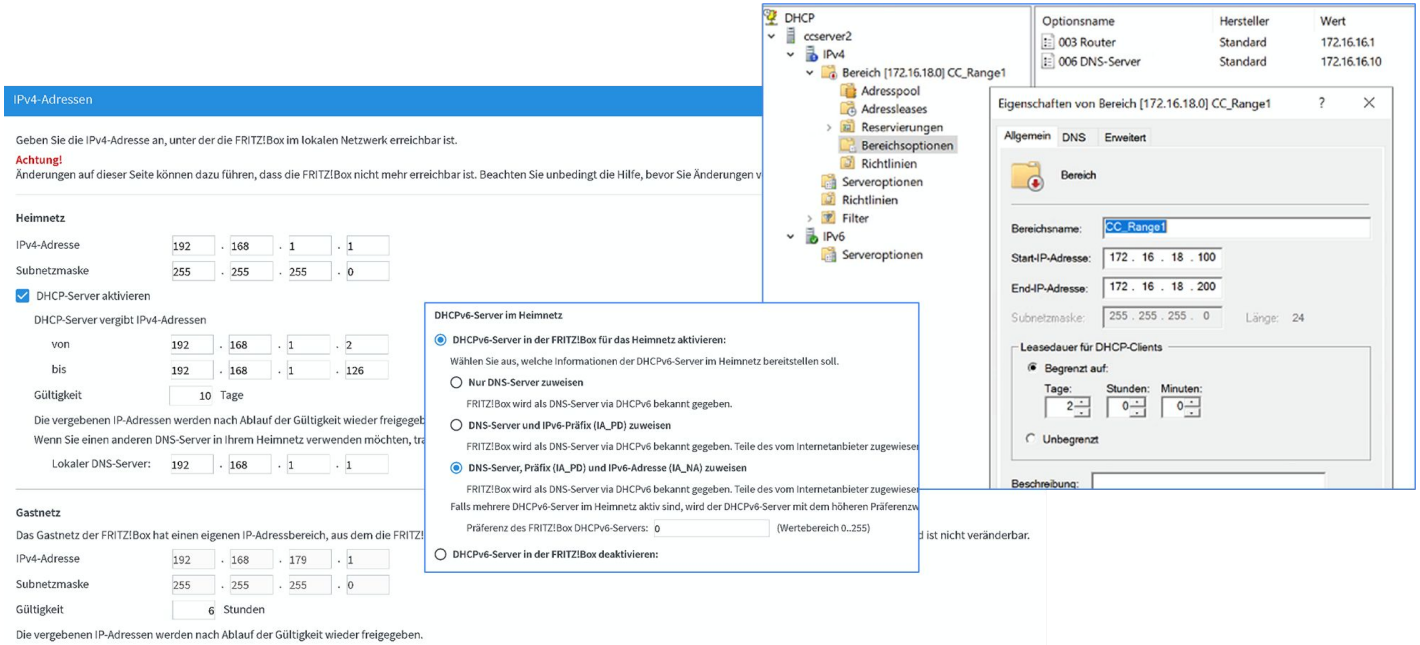
- automatisch Auswahl einer privaten IP-Adresse ohne einen IP Adress-Server (DHCP-Server).
- In der Microsoft Welt unter dem Namen APIPA (Automatic Private IP Addressing) bekannt.
- Verwendet den Class B Adressbereich 169.254.0.0
- Nur für sehr kleine Netze praktikabel (max. 10 – 20 Hosts), die kein Zugriff auf andere Netze oder dem Internet benötigen, da man kein Standardgateway eintragen kann.

Hinweis: „Diese Verbindung verfügt über eine eingeschränkte Konnektivität“ / bzw. „Kein Internet“

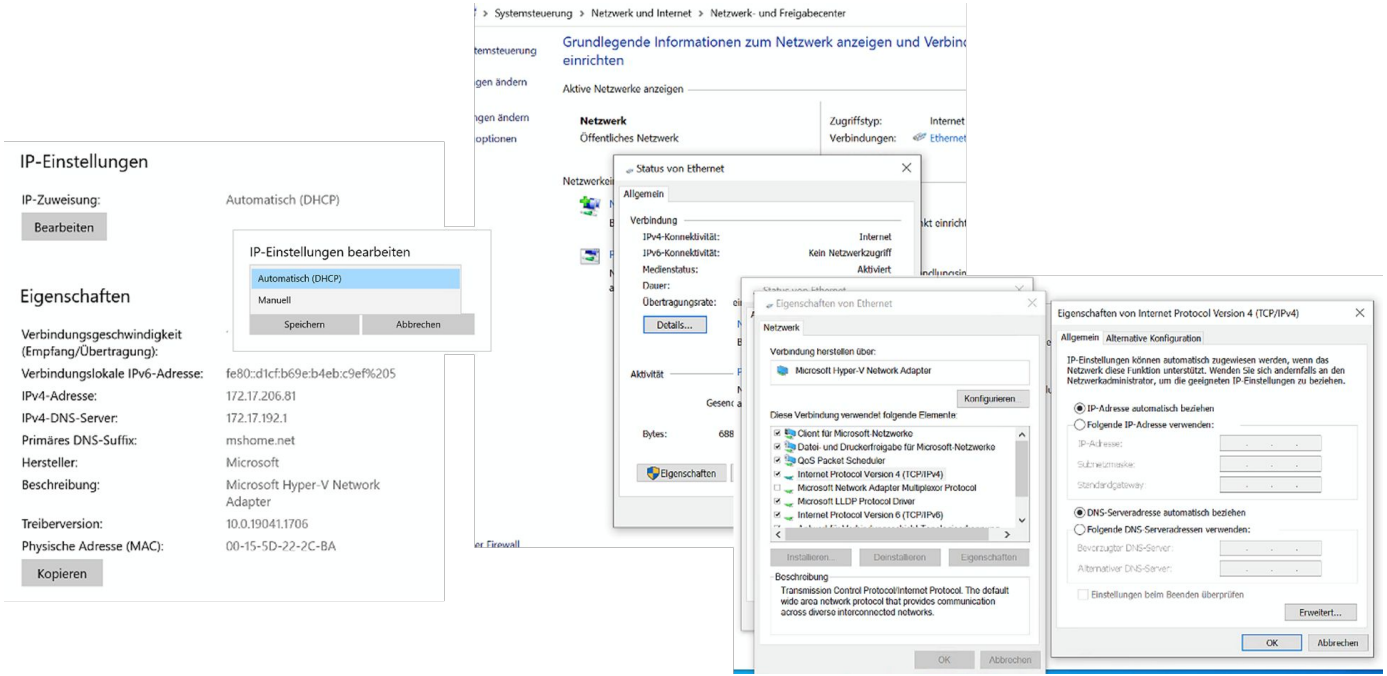
Automatische IP-Adress-Konfiguration

- Mittels APIPA (link local)
- Mit Hilfe eines DHCP Server
  - zentrale Client-Server Lösung
  - Dynamic Host Configuration Protokoll Server, oder einfach DHCP Server.
  - notwendigen Minimalangaben sind: IP-Adressbereich und Subnetzmaske
  - Zusätzliche Angaben können sein: Standard Gateway (Router), DNS Server, Domain Name, ...

DHCP-Server


IPv4-Adressen
Geben Sie die IPv4-Adresse an, unter der die FRITZ!Box im lokalen Netzwerk erreichbar ist.
Achtung!
Änderungen auf dieser Seite können dazu führen, dass die FRITZ!Box nicht mehr erreichbar ist. Beachten Sie unbedingt die Hilfe, bevor Sie Änderungen v
Heimnetz
IPv4-Adresse 192 . 168 . 1 . 1
Subnetzmaske 255 . 255 . 255 . 0
DHCP-Server aktivieren
DHCP-Server vergibt IPv4-Adressen
von 192 . 168 . 1 . 2
bis 192 . 168 . 1 . 126
Gültigkeit 10 Tage
Die vergebenen IP-Adressen werden nach Ablauf der Gültigkeit wieder freigegeb
Wenn Sie einen anderen DNS-Server in Ihrem Heimnetz verwenden möchten, tra
Lokaler DNS-Server: 192 . 168 . 1 . 1
Gastnetz
Das Gastnetz der FRITZ!Box hat einen eigenen IP-Adressbereich, aus dem die FRITZ!
d ist nicht veränderbar.
IPv4-Adresse 192 . 168 . 179 . 1
Subnetzmaske 255 . 255 . 255 . 0
Gültigkeit 6 Stunden
Die vergebenen IP-Adressen werden nach Ablauf der Gültigkeit wieder freigegeben.
DHCPv6-Server im Heimnetz
DHCPv6-Server in der FRITZ!Box für das Heimnetz aktivieren:
Wählen Sie aus, welche Informationen der DHCPv6-Server im Heimnetz bereitstellen soll.
Nur DNS-Server zuweisen
FRITZ!Box wird als DNS-Server via DHCPv6 bekannt gegeben.
DNS-Server und IPv6-Präfix (IA_PD) zuweisen
FRITZ!Box wird als DNS-Server via DHCPv6 bekannt gegeben. Teile des vom Internetanbieter zugewiese
DNS-Server, Präfix (IA_PD) und IPv6-Adresse (IA_NA) zuweisen
FRITZ!Box wird als DNS-Server via DHCPv6 bekannt gegeben. Teile des vom Internetanbieter zugewiese
Falls mehrere DHCPv6-Server im Heimnetz aktiv sind, wird der DHCPv6-Server mit dem höheren Präferenzw
Präferenz des FRITZ!Box DHCPv6-Servers: 0 (Wertebereich 0..255)
DHCPv6-Server in der FRITZ!Box deaktivieren:
DHCP
ccserver2
IPv4
Bereich [172.16.18.0] CC_Range1
Adresspool
Adressleases
Reservierungen
Bereichsoptionen
Richtlinien
Serveroptionen
Richtlinien
Filter
IPv6
Serveroptionen
Optionsname Hersteller Wert
003 Router Standard 172.16.16.1
006 DNS-Server Standard 172.16.16.10
Eigenschaften von Bereich [172.16.18.0] CC_Range1
Allgemein DNS Erweitert
Bereich
Bereichsname: CC_Range1
Start-IP-Adresse: 172 . 16 . 18 . 100
End-IP-Adresse: 172 . 16 . 18 . 200
Subnetzmaske: 255 . 255 . 255 . 0 Länge: 24
Leasedauer für DHCP-Clients
Begrenzt auf:
Tage: 2 Stunden: 0 Minuten: 0
Unbegrenzt
Beschreibung:

DHCP am Windows PC



Aufbau der IP-Vergabe mittels DHCP

- Client sendet eine Broadcast-Nachricht (mit seiner MAC-Adresse) an den verfügbaren DHCP-Server.
  - Discover → an den Server
- Der DHCP-Server antwortet mit einem Vorschlag für eine IP-Adresse.
  - Offer → an den Client
- Diesen nimmer der Client an.
  - Request → an den Server
- Der Server bestätigt das ganze nochmal und sendet alle weiteren Optionen an den Client
  - Acknowledge → an den Client

DHCP Lease

- Jede per DHCP verteilte Adresse enthält eine sog. Lease-Time, also eine Gültigkeitszeit
- Client: nach 50% seiner Leasedauer erneuter Versuch beim alten DHCP Server
- Ist der Server nicht verfügbar ist, behält der Client trotzdem weiter seine Adresse.
- Bei 87.5 Prozent Leasedauer, letzter Versuch zu erneuern.

DHCP Lease

- Wenn die Lease völlig abgelaufen ist, dann muss der Client die IP-Adresse aufgeben.
- Waren alle Versuche also erfolglos, dann beginnt alles von vorn und der Client versucht irgendeinen DHCP-Server zu erreichen um eine gültige IP-Adresse zu bekommen.
- Dann bekommt er entweder eine neue Adresse aus dem Bereich des neuen Servers, oder gibt es keinen anderen Server, so bekommt er evtl. eine APIPA Adresse

Die IPv6 Adresse

Die IPv6 Adresse

- Anstelle der 32-Bit-Adressen von IPv4 verwendet IPv6 128- Bit-Adressen.
- Dieser größere IPv6-Adressraum stellt 340 Sextillionen (3,4 × 1038) Adressen zur Verfügung.
  - 340.282.366.920.938.463.463.374.607.431.768.211.456

- IPv4 nur 4 Milliarden (4.294.967.296)

Die IPv6 Adresse

- **128-Bit-Adresse im Binärformat:**

```
00100000000000010000110110111000001111
11110101001000000000000000000000
00000000000000000000000000000000
00000000110100111001110001011010
```

- **128-Bit-Adresse unterteilt in 16-Bit-Einheiten:**

```
0010000000000001  0000110110111000
0011111110101001  0000000000000000
0000000000000000  0000000000000000
0000000011010011  1001110001011010
```

- **Die einzelnen 16-Bit-Blöcke konvertiert in HEX (base 16):**

```
2001:0DB8:3FA9:0000:0000:0000:00D3:9C5A
```

Verkürzte Schreibweise

- **Original:**

  2001:0DB8:3FA9:0000:0000:0000:00D3:9C5A

- **1. Vorangestellte 0 weglassen:**

  2001:DB8:3FA9:0:0:0:D3:9C5A

- **2. Ganze 0 Blöcke weglassen:**

  2001:DB8:3FA9::D3:9C5A

Unterscheidung von IPv6 Adresse

IPv6 definiert momentan drei Typen von Adressen:

- **globale Adressen (global addresses):**
  - 2000 – 3FFF
- **eindeutige lokale Adressen (unique local addresses):**
  - FD00 :: /64
- **verbindungslokale Adressen (link-local addresses):**
  - FE80:

- **Loopback:**
  - ::1
- Broadcast gibt es nicht mehr! Wird durch Multicast ersetzt.
  - FF…:

Unterscheidung von IPv6 Adresse

Öffentlich	Privat	Automatischen Privaten IP Adressen
Verwendung im Internet (Vollständiges Routing)	Verwendung im lokalen Netz (Privat & Unternehmen) (Kein Internet-Routing)	Verwendung im lokalen Netz ohne separate IP Verteil-Dienste (DHCP) (kein Routing)
Alles was nicht „reserviert“ oder privat ist 0.0.0.1 – 9.255.255.255 11.0.0.1-126.255.255.255 128.0.0.1-169.253.255.255 169.255.0.0-172.15.255.255. ……	10.0.0.0 172.16.0.0. – 172.31.0.0 192.168.0.0 – 192.168.255.0	169.254.0.0
Verwaltung durch IANA Internet Assigned Numbers Authority	Verwaltung durch den lokalen Administrator	Verwaltung durch den Host-OS selbst

Unterscheidung von IPv6 Adresse

Unicast:	Spricht einen Host im Netzwerk an
Broadcast:	Spricht alle Hosts im Subnetz an
Multicast (Class D):	224.0.0.0 - 239.255.255.255
Loopback:	127.0.0.0
Default Route:	0.0.0.0
Globale Broadcast:	255.255.255.255
Forschung (Class E):	240.0.0.0 - 255.255.255.254

IPv6 Fun

Netzwerke benennen mit IPv6:

- FD00:
  - ACDC
  - CAFE
  - C1A0
  - FACE
  - BOOC
  - AFFE
  - ...

Übergang zu IPv6

- IPv6 hat ein anderes Headerformat als IPv4
- Router, die nicht IPv6 kompatibel sind, können den IPv6-Header nicht auswerten.
- Schicht-2-Protokolle wie Ethernet sind nicht betroffen
- Schicht-2-Switches und -Hubs müssen nicht aufgerüstet zu werden
- Übergangstechnologien wie
    - ISATAP
    - 6to4
    - Teredo

erlauben es, IPv6 in einer Routing Infrastruktur einzusetzen, die eigentlich nur IPv4 unterstützt.

Transportprotokolle

TCP - Transmission Control Protocol

- Sorgt für den problemlosen Transport der IP-Pakete
- Im Gegensatz zu den IP-Paketen bezeichnet man die Einheiten der Transportschicht als „Segmente“
- Transportprotokoll auf OSI Schicht 4
- Verbindungsorientiert

UDP – User Datagram Protocol

- Sorgt für den schnelleren Transport der IP-Pakete (aber unsicherer)
- Die Transporteinheiten werden 'UDP-Datagramme' oder 'User Datagramme' genannt
- Transportprotokoll auf OSI Schicht 4
- Verbindungslos

Ports

Sind wie Türen zwischen Schicht 4 und Schicht 5

- 16 Bit groß. Bis zu 65535 TCP-Verbindungen möglich
- 0 bis 1.023 (well known ports) empfohlene Standard Ports, fest vergeben
- 1.024 bis 49.151 (registered ports) sind zur Registrierung freigegeben
- Port-Nummern ab 49.152, (dynamic and private ports) können frei belegt werden, sofern sie gerade von keinem anderen Dienst belegt sind

Typische Ports

Portnummer	Protokoll	Bedeutung
20	FTP (Daten)	File Transfer Protocol
21	FTP (Befehle)	
22	SSH	Secure Shell
23	Telnet	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name System
80	HTTP (Proxy-Server)	
88	Kerberos	Kerberos
110	POP3	Post Office Protocol Version3
119	NNTP	Network News Transfer Protocol
137-139	NetBIOS	NetBIOS Name/Datagram/Session- Service

Typische Ports

Portnummer	Protokoll	Bedeutung
143	IMAP	Internet Message Access Protocol
161	SNMP	Simple Network Management Protocol
389	LDAP	Lightweight Directory Access Protocol
443	HTTPS	Hyper Text Transfer Protocol Secure
445	SMB	Server Message Block
520	RIP	Routing Information Protocol
631	IPP	Internet Printing Protocol
1701	L2TP	Layer 2 Tunneling Protocol
1723	PPTP	Point to Point Tunneling Protocol
3389	RDP	Remote Desktop Protocol
9100	TCP/IP Druckdienst	Der Standard Port für den TCP/IP Druckdienst

Sockets

Die IP-Adresse in Verbindung mit der Portnummer definiert einen Socket.

- Dadurch können u.U. spezielle Dienste direkt angesprochen werden
- Die Schreibweise für einen Socket ist:
  - IP-Adresse : Portnummer
  - 10.100.5.1:8080

Weiter Protokolle

<table>
<tr><th>OSI Layer</th><th>TCP/IP Schicht</th><th>Internet (UNIX)</th><th colspan="2">Microsoft</th><th>Novell</th><th>Apple</th></tr>
<tr><td>7</td><td rowspan="4">Anwend-ungen</td><td rowspan="3">HTTP, FTP, SMTP, POP, IMAP, Telnet, DNS, NTP, NNTP, RDP, SNMP, LDAP, LPR, IPP,</td><td colspan="2">SMB</td><td rowspan="4">NCP</td><td rowspan="6">Apple Talk</td></tr>
<tr><td>6</td><td rowspan="3">NetBIOS (NBT)</td><td rowspan="5">NetBIOS NetBEUI</td></tr>
<tr><td>5</td></tr>
<tr><td colspan="2">Ports</td></tr>
<tr><td>4</td><td>Transport</td><td colspan="2">TCP, UDP</td><td>SPX</td></tr>
<tr><td>3</td><td>Internet</td><td colspan="2">IPV4, IPV6, ICMP, RIP, OSPF</td><td>IPX</td></tr>
<tr><td>2</td><td rowspan="2">Netzzugang (Hardware)</td><td colspan="4" rowspan="2">MAC Adresse, ARP, RARP, CSMA-CD, PPP, Ethernet, WLAN, Token Ring, Arcnet, FDDI, DSL,</td></tr>
<tr><td>1</td><td>Local Talk</td></tr>
</table>

NAT - Netzwerkadressübersetzung

- NAT ermöglicht unter anderem die gleichzeitige Verwendung einer öffentlichen Adresse durch mehrere Hosts.
- Bei jedem Verbindungsaufbau durch einen internen Client wird die interne Quell-IP-Adresse durch die öffentliche IP-Adresse des Routers + ein freier Port ersetzt.
- Diese Zuordnung wird in der Session-Table (NAT-Table) des Routers gespeichert.
- Anhand der gespeicherten Informationen kann der NAT-Router dann das jeweilige Antwort-Datenpaket dem richtigen Client wieder zuordnen.

NAT - Netzwerkadressübersetzung

Quelle	Ziel
192.168.0.2:49701	198.51.100.1:80
192.168.0.3:50387	198.51.100.1:80
192.168.0.4:49152	198.51.100.1:23

Router
==========>
NAT

Quelle	Ziel
203.0.113.2:49701	198.51.100.1:80
203.0.113.2:50387	198.51.100.1:80
203.0.113.2:49152	198.51.100.1:23

SMB – Server Message Block

- Kommunikationsprotokoll für Datei-, Druck- und andere Serverdienste in Microsoft Netzwerken
- Nicht konfigurierbar
- SMB und seine Einstellmöglichkeiten verbergen sich zumeist hinter solchen Microsoft Diensten wie „Client für Microsoft Netzwerke“, „Datei und Druckfreigabe“, „Netzwerk-Umgebung“, „Netzwerk und Freigabecenter“, …
- von Open Source „Samba“ verwendet, um Windows-Systemen den Zugriff auf Ressourcen von Unix-basierten Systemen zu ermöglichen und umgekehrt.
- Aktuell in der Version 3 verfügbar
    - SMBv1 gilt heutzutage auch als unsicher und sollte nicht mehr genutzt werden

NBT - NetBOIS over TCP/IP

NetBIOS (stark veraltet)

- Network Basic Input Output System
- OSI-Schicht 3 bis hin zur Schicht 5
- NetBIOS Namen bis zu 15 Zeichen lang

NBT

- Anwendungsorientiertes Protokoll der OSI-Schicht 5
- ermöglicht, den auf der Programmierschnittstelle NetBIOS aufbauenden Programmen, das Netzwerkprotokoll TCP/IP zu verwenden.
- Nur noch zur abwärts Kompatibilität erforderlich

NetBEUI – NetBIOS Extended User Interface

- NetBIOS Extended User Interface
- OSI-Schicht Schicht 3
- Früheres Standard Protokoll in einfachen Microsoft Netzen
- Hostname ist unter Windows der „Computername“
- Er darf für NetBEUI 15 Zeichen nicht überschreiten.
- Dieser Name darf auch nur ein einziges Mal vorkommen!
- Nicht routingfähig

AppleTalk

- Eine Gruppe von proprietären Netzwerkprotokollen (von Schicht 2 bis Schicht 7)
- „Plug and Play“ Netzwerk, von Apple Computer, Ende 1983 entwickelt
- AppleTalk teilte ein Gesamtnetz in mehrere Teilnetze den sogenannten Zonen ein. Innerhalb dieser Zonen, lagen die einzelnen Knoten wie Rechner, Server, Drucker, etc.
- Angesichts der weiten Verbreitung von IP-basierten Netzwerken wurde AppleTalk ab Mac OS X 10.6 von Apple aufgegeben.
- Teiles des AppleTalk, wie AFP (Apple Filling Protocoll), wird noch für den Datenaustausch in Homogenen Umgebungen genutzt, auch wenn dies durch SMB2 ersetzt wurde.

Bonjour

- Immer noch aktuelles Protokoll zur Implementierung eines sog. Zeroconfig-Systems in einer Apple-Umgebung
- Wird u.a. von Safari, iTunes, AirPrint genutzt
- Frei zugänglich und kann sogar auf Windows Systemen installiert werden

Was sollte ich auf jeden Fall behalten

- Auf OSI-Layer-3-Ebene ist das Internet Protokoll (IP) in den Versionen 4 und 6 (IPv4 und IPv6)
- Auf Ebene 4 befinden sich das TCP und UDP Protokoll
- Bei IPv4 wird zwischen privaten (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) und öffentlichen Adressen unterschieden, diese werden im Internet nicht geroutet.
- Aufgrund der Adressknappheit wurde zum einen NAT entwickelt und später IPv6 entwickelt
- Ports werden verwendet, um Prozessen/Diensten Datenpakete zuzuordnen (z.B. 80 → HTTP, 22 → SSH, 445 → SMB etc.)

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm