

Netzwerk und TCP / IP Grundlagen

ppedv AG

Daniel Rerich

Vorstellung

- Ihr Trainer:

Daniel Rerich

danielr@ppedv.de

- Kurse bei ppedv:
 - JavaScript, HTML und CSS – Jump Start
 - Responsive Design
 - Netzwerktechnik



Vorab

- Kursablauf
 - Zeiten: 09:00 bis 17:00 Uhr
 - Pausen: 10:30, 12:30, 15:30
- Parken
- Räumlichkeiten
- Vorstellungsrunde
 - Hintergrund, Motivation und Vorkenntnisse
- Slides und Anleitungen später online verfügbar
- !! Bei Fragen bitte sofort melden !!



Agenda

- Netzwerkprotokolle und Protokollsammlungen
 - ISO / OSI
 - TCP / IP
- Netzwerkgeräte
- IP
- VLAN
- DNS
- DHCP
- VPN

Netzwerkprotokolle und Protokollsammlungen

ISO / OSI Modell

- OSI-Modell = Open Systems Interconnection Model
 - „7 Schichten Modell“

• A pplication	Anwendung
• P resentation	Darstellung
• S ession	Sitzung
• T ransport	Transport
• N etwork	Netzwerk
• D ata Link	Daten / Verbindungsebene
• P hysical	Bit / Übertragungsschicht

Merksatz !

Please Do Not Throw
Salami Pizza Away

ISO /OSI Modell

Application / Anwendung

- Layer 7
- Schnittstelle zu den Anwendungen
- Zuständig für Dateneingabe und –ausgabe
- Protokolle / Anwendungen
 - http
 - Webbrowser

ISO /OSI Modell

Presentation / Darstellung

- Layer 6
- Wandelt systemabhängige Darstellung (ASCII) in unabhängige Form (ASN 1 – Abstract Syntax Notation One)
- Zuständig auch für Kompression & Verschlüsselung

ISO /OSI Modell

Session / Sitzung

- Layer 5
- Zuständig für Prozesskommunikation
- Synchronisiert den Datenaustausch
- Setzt „Check Points“ zum Fortsetzen der Verbindung bei Abbruch
- Protokolle z.B.
 - RPC

ISO /OSI Modell

Transport

- Layer 4
- Zuständig für Segmentierung und „Stau Vermeidung“
- Datensegment (SDU-Service Data Unit)
- Zuteilung an Ports
- Beispiel Protokolle:
 - TCP
 - UDP

ISO / OSI Modell Network

- Layer 3
- Schaltet die „Verbindungen“
- Kümmert sich um die „Wegsuche“ (Routing)
- Arbeitet mit folgenden Adressstypen
 - IP
 - NSAP (ISDN-Nummer)
- Beispiel Protokolle:
 - IP
 - ICMP

ISO / OSI Modell

Data / Verbindungsschicht

- Layer 2
- Teilt den Bitdatenstrom in Frames auf
- Fügt und Prüfsummen hinzu und überprüft diese
- Zuständig für Datenflusskontrolle
- Nutzt:
 - LLC
 - MAC (Media Access Control)

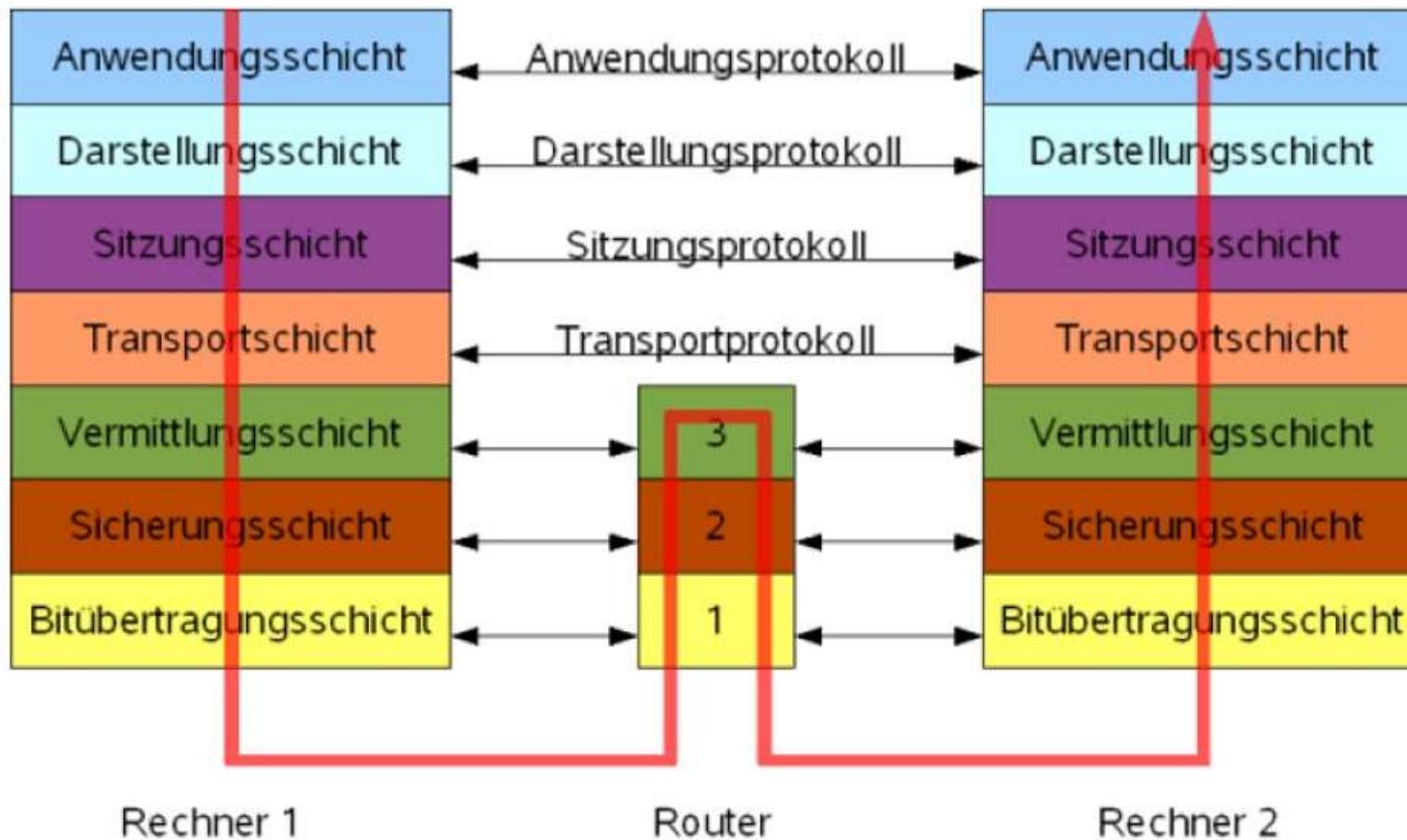
ISO / OSI Modell

Physical / Bit- oder Übertragungsschicht

- Layer 1
- Zuständig z.B. auch für das Multiplexing
- Übertragung der Daten über ein Medium z.B.:
 - Elektrisch
 - Optisch
 - Elektromagnetisch
 - Schall

ISO / OSI Modell

Verbindung



ISO / OSI im Vergleich zu TCP / IP

ISO / OSI	TCP / IP (DoD)
Application	
Presentation	Application
Session	
Transport	Transport
Network	Internet
Data Link	Link
Physical	

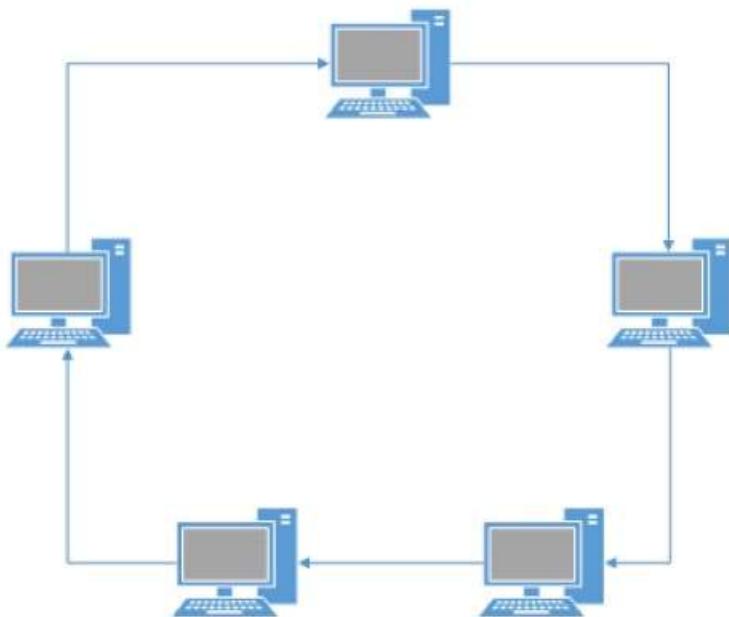
Netzwerkgeräte / Topologien

ISO OSI Layer	Geräte	Hub	Switch	Router
Layer 1		X		
Layer 2			X	
Layer 3			(X)	X
Layer 4				
Layer 5				
Layer 6				
Layer 7				

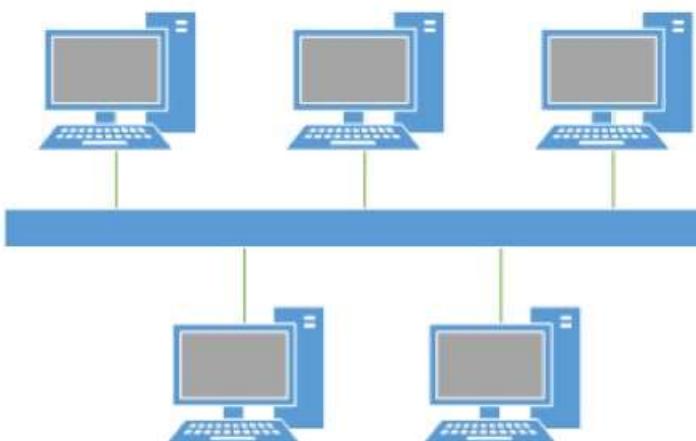


Topologien

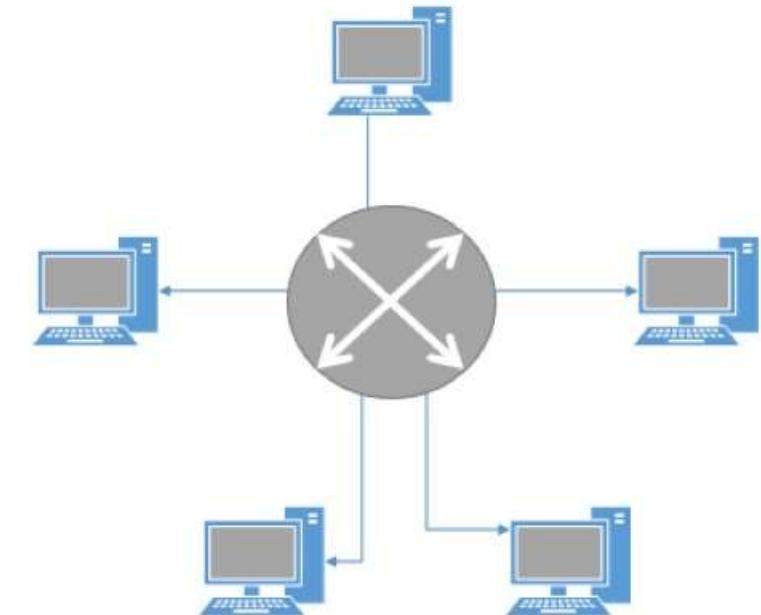
Token Ring



Bus



Stern

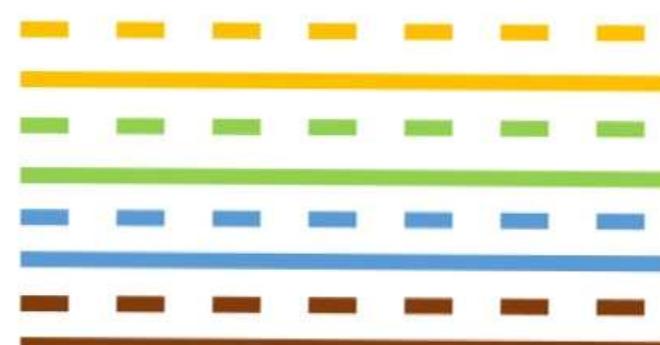


Kabelbelegung Patchkabel

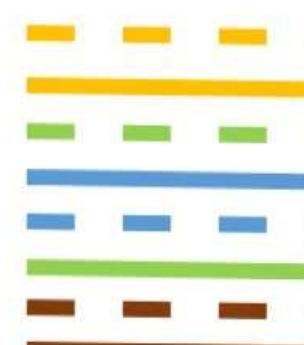
Stecker A



Kabel

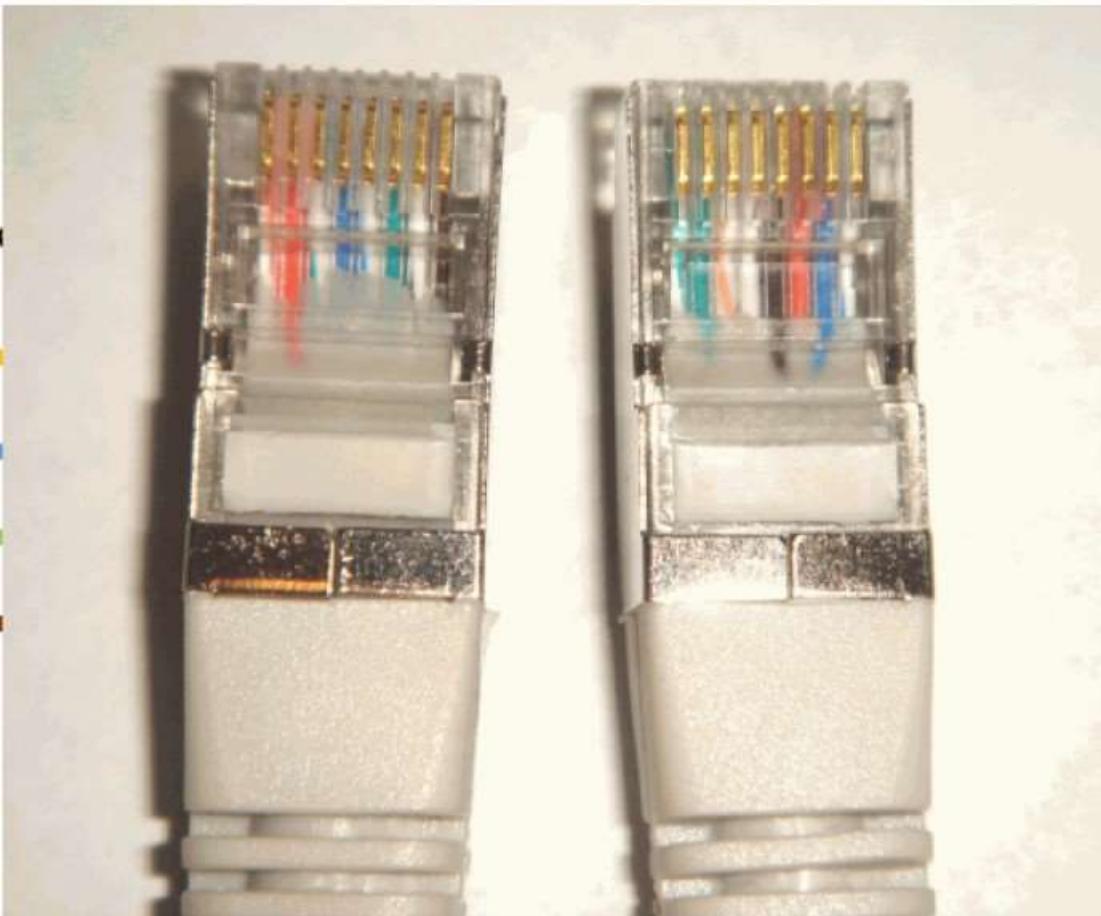


Stecker B



Kabelbelegung Crossover Kabel

Steck



Stecker B



IP

Netzwerk Grundlagen

- Aufbau IP-Adresse (Network-/Host-Address)
- Klassen
 - A-0.x.x.x – 127.x.x.x
 - 128 Netze, 16 Mio Adressen
 - B-128.0.x.x – 191.255.x.x
 - 16 k Netze, 65 k Adressen
 - C-192.0.0.x – 223.255.255.x
 - 2 Mio Netze 254 Adressen
- Subnetzmaske / Suffix (Präfix)
- APIPA 169.254.0.0 /16

Netzwerk Grundlagen

- Aufbau IP-Adresse (Network-/Host-Address)
- Klassen
 - A-~~0.0.0.0 – 127.255.255.255~~ 127.255.255.255
 - B-~~128.0.0.0 – 191.255.255.255~~ 191.255.255.255
 - C-~~192.0.x – 223.255.255.x~~ 223.255.255.255
 - ~~224.0.0.0 – 255.255.255.255~~ 255.255.255.255
- Subnetzmaske / Suffix (Präfix)
- APIPA 169.254.0.0 /16



Veraltet

Dezimal / Binär

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
-------	-------	-------	-------	-------	-------	-------	-------



2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
-------	-------	-------	-------	-------	-------	-------	-------



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

Subnetting

- Unterteilung eines großen Netzes in kleinere
- Abteilungsdrucker senden nicht ins ganze Netz
- 2 Adressen pro Netz nicht adressierbar
 - die erste IP ist immer die NetzID
 - die letzte IP ist immer die Broadcast Adresse
- IP Adresse besteht aus Netzanteil und Hostanteil

Netzanteil	Hostanteil
192.168.10.	0
255 . 255 . 255 .	0
11111111.11111111.11111111.	00000000

Binär	Subnetz- Maske	Präfix (letztes Oktett)
00000000	0	/24
10000000	128	/25
11000000	192	/26
11100000	224	/27
11110000	240	/28
11111000	248	/29
11111100	252	/30
11111110	254	/31
11111111	255	/32

Übung 1

Gegeben:

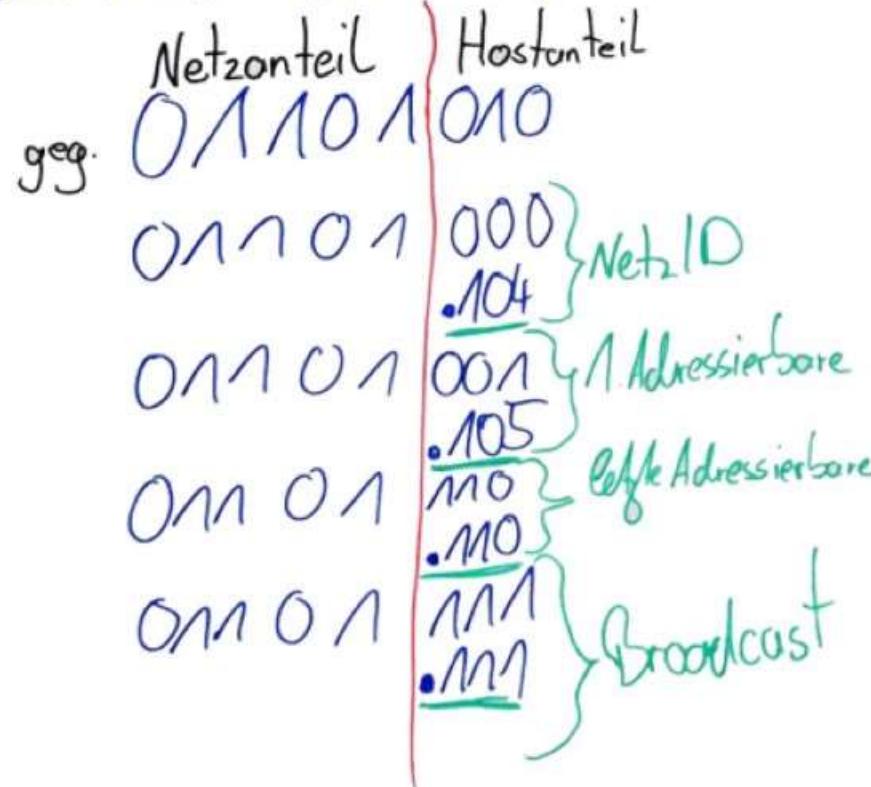
- 192.168.10.106 /29

Gesucht:

- „NetzID“
- Erste Adressierbare Adresse
- Letzte Adressierbare Adresse
- Broadcast IP

Übung 1 Lösung

192.168.10.106/29



$2^0 = 1$	1
$2^1 = 2$	1
$2^2 = 4$	1
$2^3 = 8$	1
$2^4 = 16$	0
$2^5 = 32$	1
$2^6 = 64$	1
$2^7 = 128$	0

Übung 1.2

Gegeben:

- 192.168.36.139 /30

Gesucht:

- „NetzID“
- Erste Adressierbare Adresse
- Letzte Adressierbare Adresse
- Broadcast IP

Übung 2

Gegeben:

- 192.168.6.190 /20

Gesucht:

- „NetzID“
- Erste Adressierbare Adresse
- Letzte Adressierbare Adresse
- Broadcast IP

Übung 2 Lösung

(IP)

192.168.6.190 120

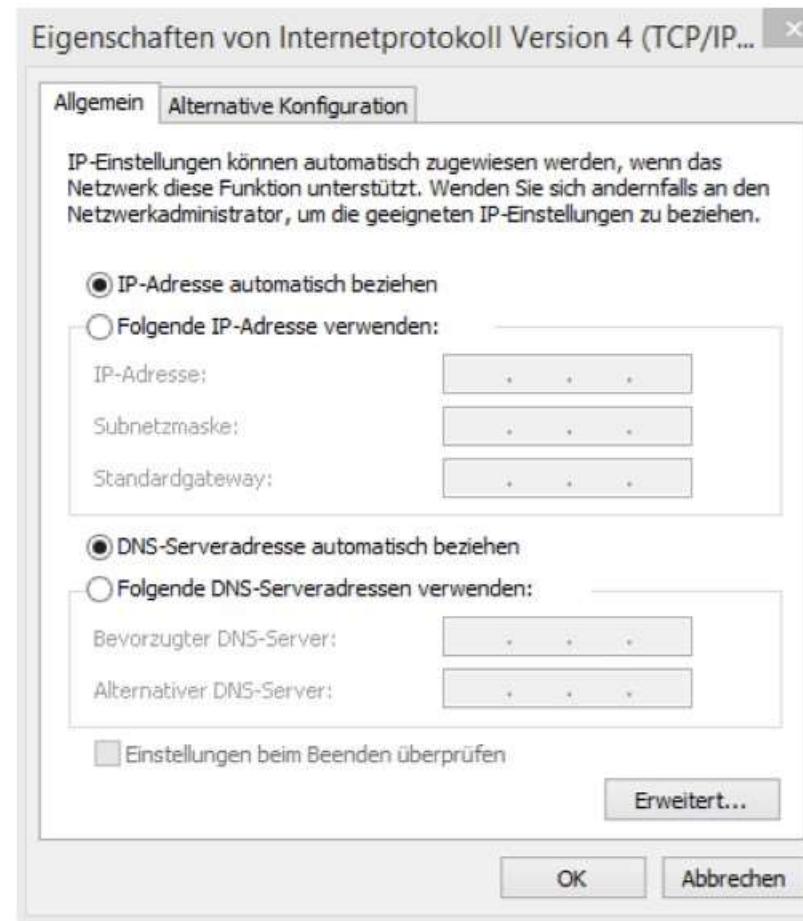
00000	0110	10111110
00000	0000	0.00000000
Netz ID = 192.168.0.0		
00000	0000	.00000001
1. Adressbereiche = 192.168.0.1		
00000	1111	.1111111110
Rücke Adresse = 192.168.15.254		
00000	1111	.1111111111
Broadcast 192.168.15.255		
1111	0000	.0000 0000
Subnetzmaske 255.255.255.240.0		

2^7	128
2^6	64
2^5	32
2^4	16
2^3	8
2^2	4
2^1	2
2^0	1

Übung 3

- Gegeben:
- 6 Stockwerke a 100 Hosts
- Grundbereich 192.168.0.0/16
- Gesucht:
- Wie viele Subnetze möglich
- NetzID vom 1. und 4. Subnetz

Manuelle Konfiguration der IP-Adresse



Automatische Konfiguration von IPv4

- Eine APIPA (Automatic-Private-IP-Adressing) wird dann zugewiesen wenn der Client keinen DHCP Server kontaktieren kann.
- Oder ein IP Adresskonflikt vorliegt

Allgemein lässt sich also sagen das die APIPA bei fehlerhafter IP Konfiguration auftritt.

IPv6

- IPv4: 32 Bit – 4.3 Mrd. Adressen
 - 4.294.967.296
- IPv6: 128Bit – ca. 3.4×10^{38} Adressen
 - 340.282.366.920.938.463.463.374.607.431.768.211.456
 - Dreiundvierzig Sextillionen zweihundertzweiundachtzig Quintilliarden dreihundertsechsundsechzig Quintillionen neunhundertzwanzig Quadrilliarden neunhundertachtunddreißig Quadrillionen vierhundertdreiundsechzig Trilliarden vierhundertdreiundsechzig Trillionen dreihundertvierundsiebzig Billiarden sechshundertsieben Billionen vierhunderteinunddreißig Milliarden siebenhundertachtundsechzig Millionen zweihundertelftausendvierhundertsechsundfünfzig
 - $2,2 \times 10^{24}$ Adressen für jeden m² Landfläche
- 8 Gruppen zu je 16 Bit
 - Bsp.: fe80:12bc:af43:bb15:df23:9836:123f:02a1
- Letzte 64 Bit: Interface Identifier

IPv6

- 128 Bit Adresse in 16 Blöcken

0010000000000001 0000110110111000 0000000000000000
1001011110011101 0000001010101010 0000000011111111
1111111000101000 1001110001011010

- In Hexadezimal dargestellt

2001:0DB8:0000:2F3B:02AA:0OFF:FE28:9C5A

- Vereinfacht dargestellt

2001:DB8:0:2F3B:2AA:FF:FE28:9C5A

IPv6

- führende 0 dürfen weggelassen werden
- ::1/128 loopback, localhost
 - 0000:0000:0000:0000:0000:0000:0000:0001
- ::/128 nicht spezifizierte Adresse
- Adressbereiche:
 - Link Local Address (fe80)
 - nicht routbar
 - Unique Local Unicast
 - Unique local (zentral vom Provider verwaltet) fc00 ..
 - Unique local (lokal verwaltet) fd80
 - Multicast (ff00....)
 - Global Unicast (alle anderen Bereiche)

VLAN

Virtual Local Area Networks

VLAN

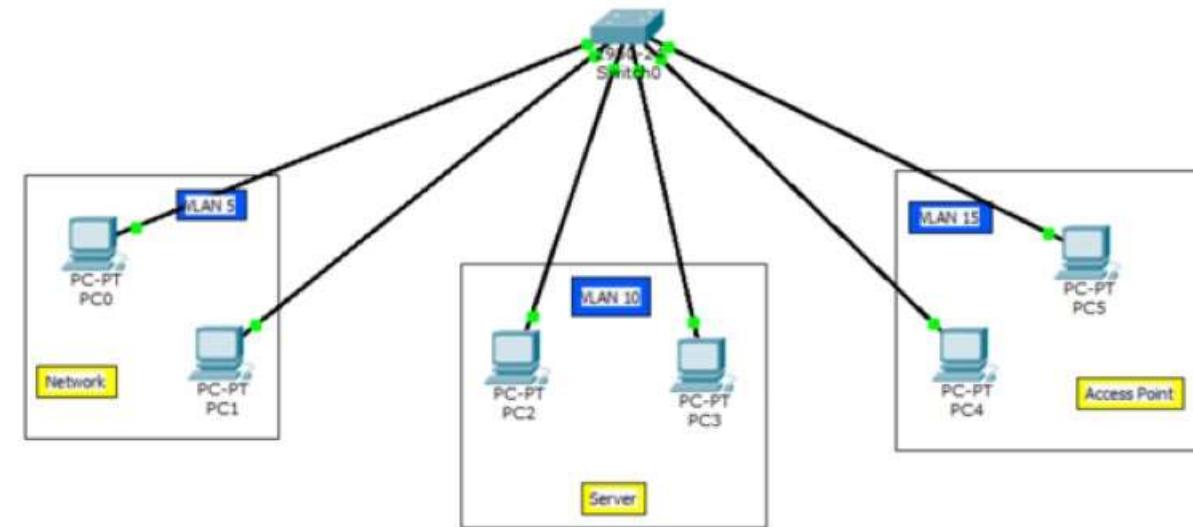
Gliederung

- Was ist ein VLAN?
- Wofür brauchen wir VLAN?
- VLAN Typen
 - Portbasierte VLANs
 - Tagged VLANs

VLAN

Was ist ein VLAN?

- Abkürzung für Virtual Local Area Network
- Unterteilt ein physisches Netzwerk in mehrere logische
- Jedes VLAN hat eine Broadcast-Domain und VLAN-ID



VLAN

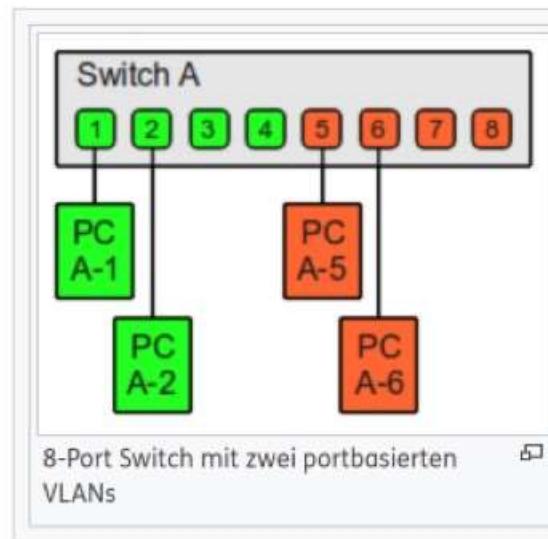
Wofür brauchen wir VLAN?

- Verbesserte Dienstgüte
 - Durch Definition von Vorrangdaten
 - Zeit- und sicherheitskritische Dienste werden verbessert
- Leistung
 - Geringe Kollisionsbereiche
- Management
 - Gruppen sind einfacher, flexibler und kostengünstiger modifiziert werden
- Mehr Sicherheit
 - Durch Paketfilter
 - Verkehr kann erlaubt/verboten werden

VLAN Typen

Portbasierte VLANs

Switch A		
Switch-Port	VLAN ID	angeschlossenes Gerät
1		PC A-1
2	1 (grün)	PC A-2
3		(nicht in Verwendung)
4		(nicht in Verwendung)
5		PC A-5
6	2 (orange)	PC A-6
7		(nicht in Verwendung)
8		(nicht in Verwendung)



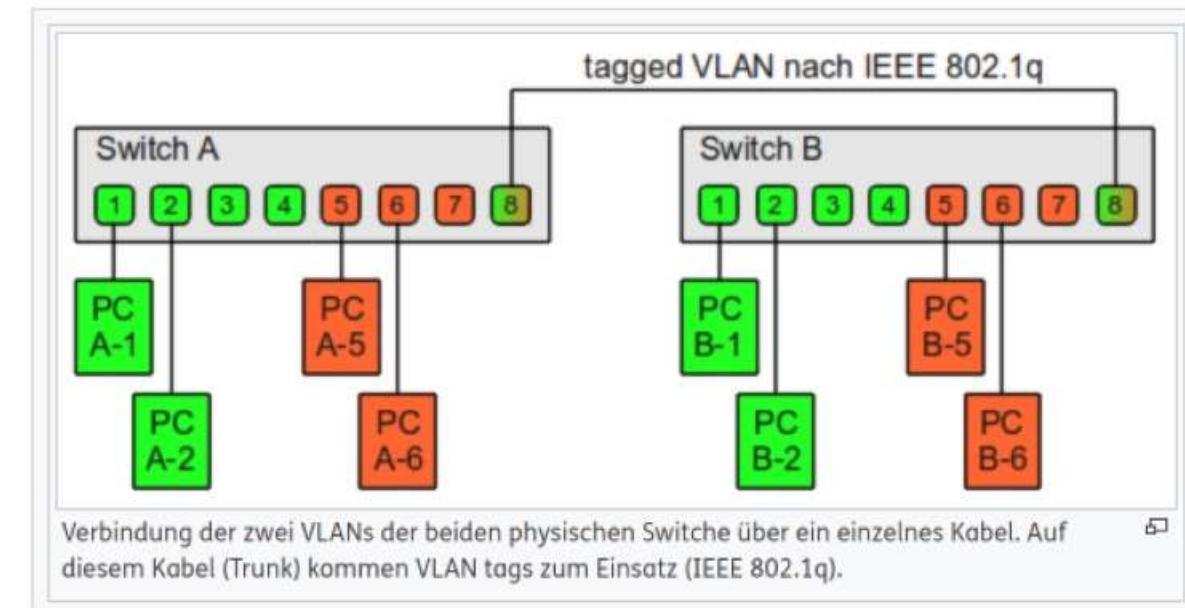
VLANs die kommunizieren:

- PC A-1 mit PC A-2
- PC A-5 mit PC A-6

VLAN Typen

Tagged VLANs

- Mehrere VLANs können einen einzelnen Switch-Port benutzen
- Ethernet Frames werden Tags angehängt
 - VLAN-ID



DNS

Domain Name System

DNS

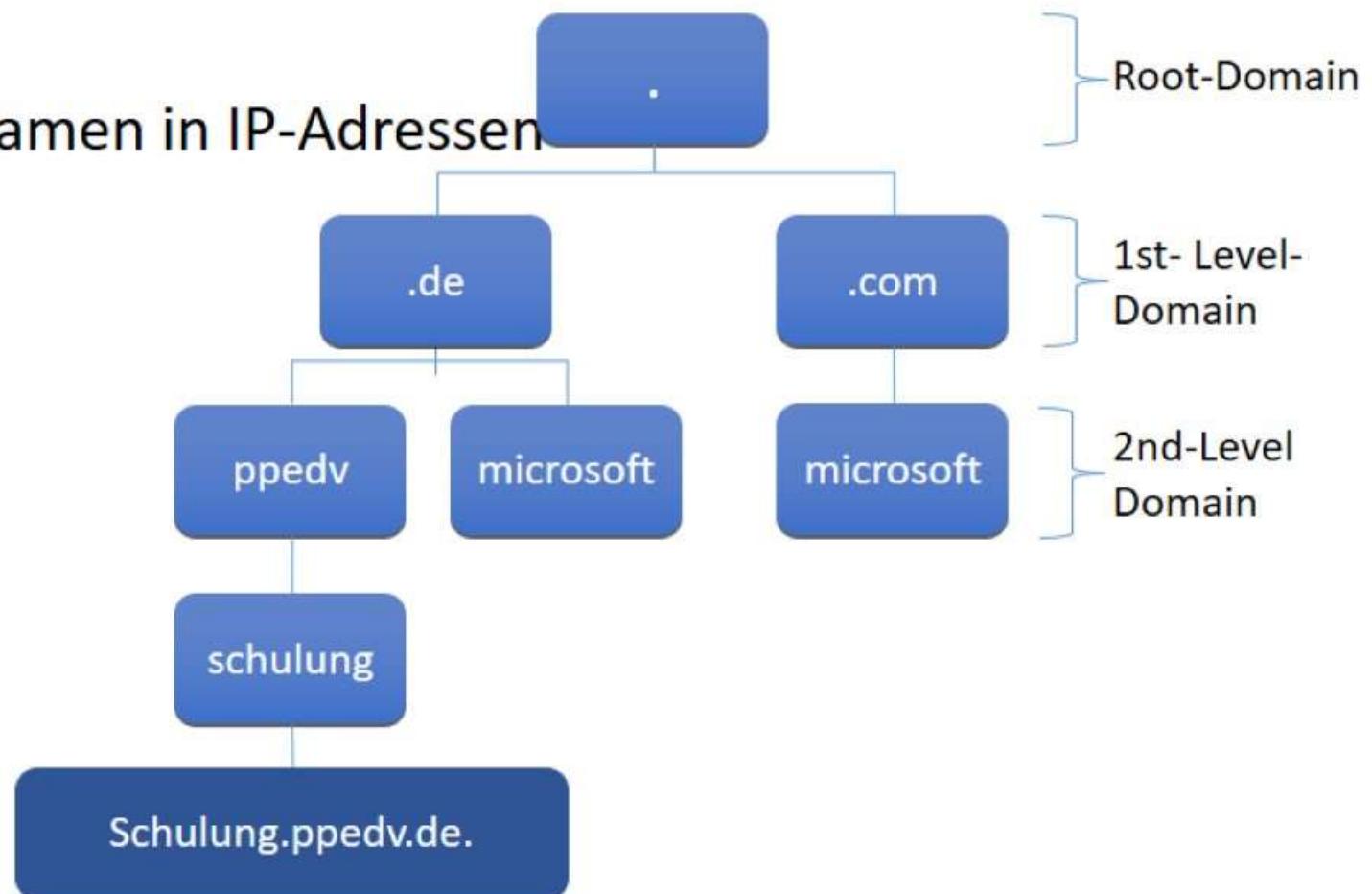
Gliederung

- Funktion
- Aufbau der FQDN
- Lookup Arten
- Abfrage Reihenfolge
- Weiterleitungen

DNS

Zonenaufbau

- Funktion
 - Auflösen der Domänen Namen in IP-Adressen
- FQDN



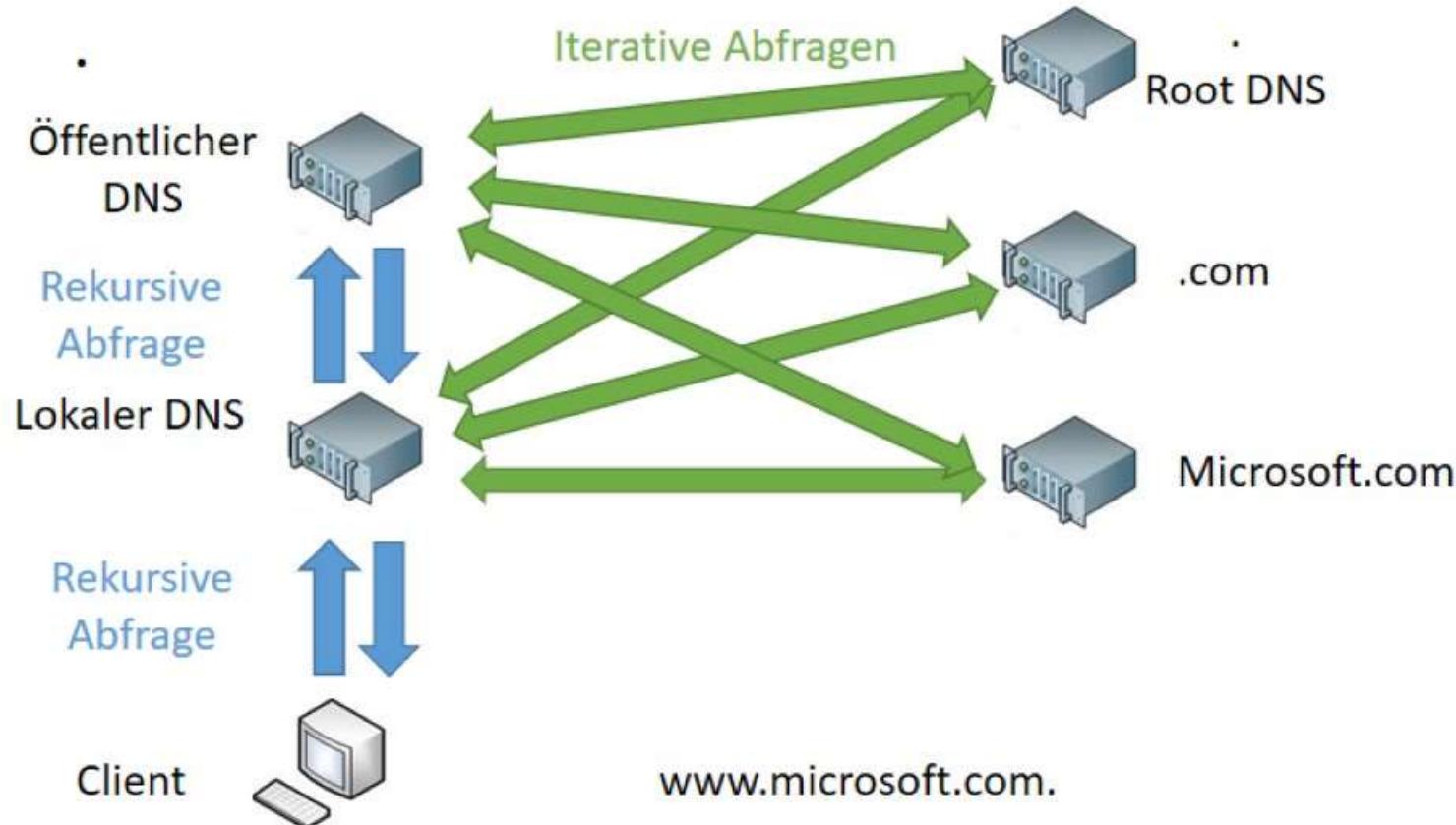
DNS

Lookup / Abfrage

- **Lookup Typen**
 - Forward-Lookup: Name -> IP
 - Reverse-Lookup: IP -> Name
- **Abfrage Reihenfolge**
 - Eigener Hostname
 - Host-Datei
 - Lokaler Cache
 - DNS-Server

DNS

Weiterleitungen / Stammhinweise



DNS

Weiterleitungen

Debugprotokollierung		Ereignisprotokollierung	Überwachen						
Schnittstellen	Weiterleitungen	Erweitert	Stammhinweise						
<p>Bei Weiterleitungen handelt es sich um DNS-Server, die von diesem Server zum Auflösen von DNS-Abfragen nach Einträgen verwendet werden, die von diesem Server nicht aufgelöst werden können.</p> <table border="1"><tr><td>IP-Adresse</td><td>Vollqualifizierter Domänenname ...</td></tr><tr><td>8.8.8</td><td>google-public-dns-a.google.com</td></tr><tr><td>8.8.4.4</td><td>google-public-dns-b.google.com</td></tr></table> <p><input checked="" type="checkbox"/> Stammhinweise verwenden, wenn keine Weiterleitungen verfügbar sind Bearbeiten...</p> <p>Hinweis: Werden bedingte Weiterleitungen für eine bestimmte Domäne definiert, werden sie anstelle von Weiterleitungen auf Serverebene verwendet. Navigieren Sie zum Erstellen oder Anzeigen bedingter Weiterleitungen in der Bereichsstruktur zum Knoten für bedingte Weiterleitungen.</p> <p style="text-align: center;">OK Abbrechen Übernehmen Hilfe</p>				IP-Adresse	Vollqualifizierter Domänenname ...	8.8.8	google-public-dns-a.google.com	8.8.4.4	google-public-dns-b.google.com
IP-Adresse	Vollqualifizierter Domänenname ...								
8.8.8	google-public-dns-a.google.com								
8.8.4.4	google-public-dns-b.google.com								

DNS

Stammhinweise

- Stammhinweise = Root DNS Server
- insgesamt 13 Stück weltweit verteilt
 - größtenteils an geheimen Standorten verteilt
- Standardmäßig eingetragen

DNS

Eintragstypen

Bezeichner	Zweck
A – Address Record	Antwort mit einer IPv4 Adresse wenn Domäne angefragt wurde
AAAA - Eintrag	Antwort mit einer IPv6 Adresse wenn Domäne abgefragt wurde
CNAME – Canonical Name Record	Alias für einen bestehenden A oder AAAA Eintrag wenn einem Host mehrere FQDNs zugewiesen werden sollen.
NSR – Name Server Records	Wird z.B. verwendet, um eine komplette Kind-Domäne an einen alternativen DNS zu delegieren
MX – Mail Exchanger Record	Eintrag welches Ziel für die E-Mail-Verarbeitung innerhalb der Domäne zuständig ist

DNS

Befehle für Troubleshooting

EXAMPLE 1

This example resolves a name using the default options.

Windows PowerShell

```
PS C:\> Resolve-DnsName -Name www.bing.com
```

EXAMPLE 2

This example resolves a name against the DNS server at 10.0.0.1.

Windows PowerShell

```
PS C:\> Resolve-DnsName -Name www.bing.com -Server 10.0.0.1
```

EXAMPLE 3

This example queries for A type records for name www.bing.com.

Windows PowerShell

```
PS C:\> Resolve-DnsName -Name www.bing.com -Type A
```

EXAMPLE 4

This example resolves a name using only DNS. LLMNR and NetBIOS queries are not issued.

Windows PowerShell

```
PS C:\> Resolve-DnsName -Name www.bing.com -DnsOnly
```

```
Nslookup [<-SubCommand ...] [{<ComputerToFind> | -<Server>}]
Nslookup /exit
Nslookup /finger [<UserName>] [{[>] <FileName>|[>>] <FileName>}]
Nslookup /{help | ?}
Nslookup /ls [<Option>] <DNSDomain> [{[>] <FileName>|[>>] <FileName>}]
Nslookup /lserver <DNSDomain>
Nslookup /root
Nslookup /server <DNSDomain>
Nslookup /set <KeyWord>[=<Value>]
Nslookup /set all
Nslookup /set class=<Class>
Nslookup /set [no]d2
Nslookup /set [no]debug
Nslookup /set [no]defname
Nslookup /set domain=<DomainName>
Nslookup /set [no]ignore
Nslookup /set port=<Port>
Nslookup /set querytype=<ResourceRecordType>
Nslookup /set [no]recurse
Nslookup /set retry=<Number>
Nslookup /set root=<RootServer>
Nslookup /set [no]search
Nslookup /set srchlist=<DomainName>[...]
Nslookup /set timeout=<Number>
Nslookup /set type=<ResourceRecordType>
Nslookup /set [no]vc
Nslookup /view <FileName>
```

DHCP

Dynamic Host Configuration Protocol



DHCP

- DHCP = Dynamic Host Configuration Protocol
- Verteilung von IP-Adressen
 - Automatische Zuordnung
 - einmalige Zuordnung
 - Dynamische Zuordnung
 - Zuordnung mit Gültigkeit (Lease)
 - Manuelle Zuordnung
 - Bindung einer IP-Adresse an die MAC Adresse
- Port 67 (Server) / Port 68 (Clients)
- dient der Sicherheit
- Definierung über Scopes / Bereiche

DHCP

- DHCP**DISCOVER**
 - Broadcast des Clients um DHCP Server im Netz zu finden
- DHCP**OFFER**
 - Nachricht des Servers mit „Kontaktdaten“ und Adressvorschlägen
- DHCP**REQUEST**
 - Client fordert eine Adresse aus den Vorschlägen an
- DHCP**ACK**
 - Server bestätigt die IP und liefert die zusätzlichen Daten (DNS, Time, ...)
- DHCP**NAK**
 - Server lehnt DHCPREQUEST ab
- DHCP**DECLINE**
 - Client lehnt Adresse ab
- DHCP**RELEASE**
 - Client gibt Adresse frei
- DHCP**INFORM**
 - Client frägt nur die zusätzlichen Daten an

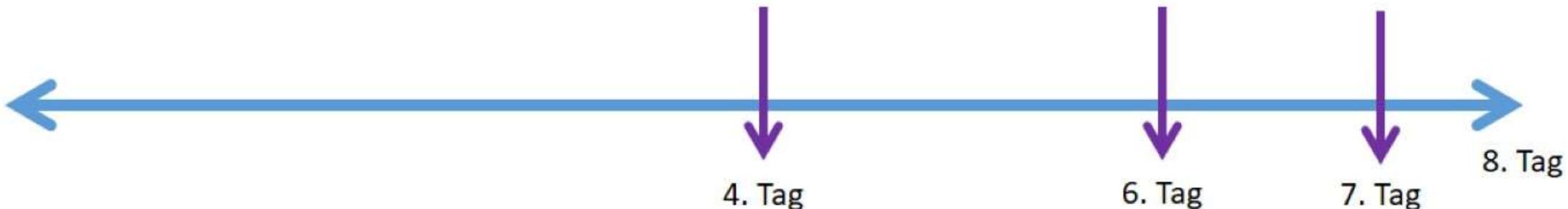
DHCP – Optimaler Ablauf



DHCP – Lease Gültigkeit

Szenario: Client bekommt vom DHCP eine Adresse mit einer Lease von 8 Tagen zugewiesen, wann meldet sich der Client wieder beim DHCP?

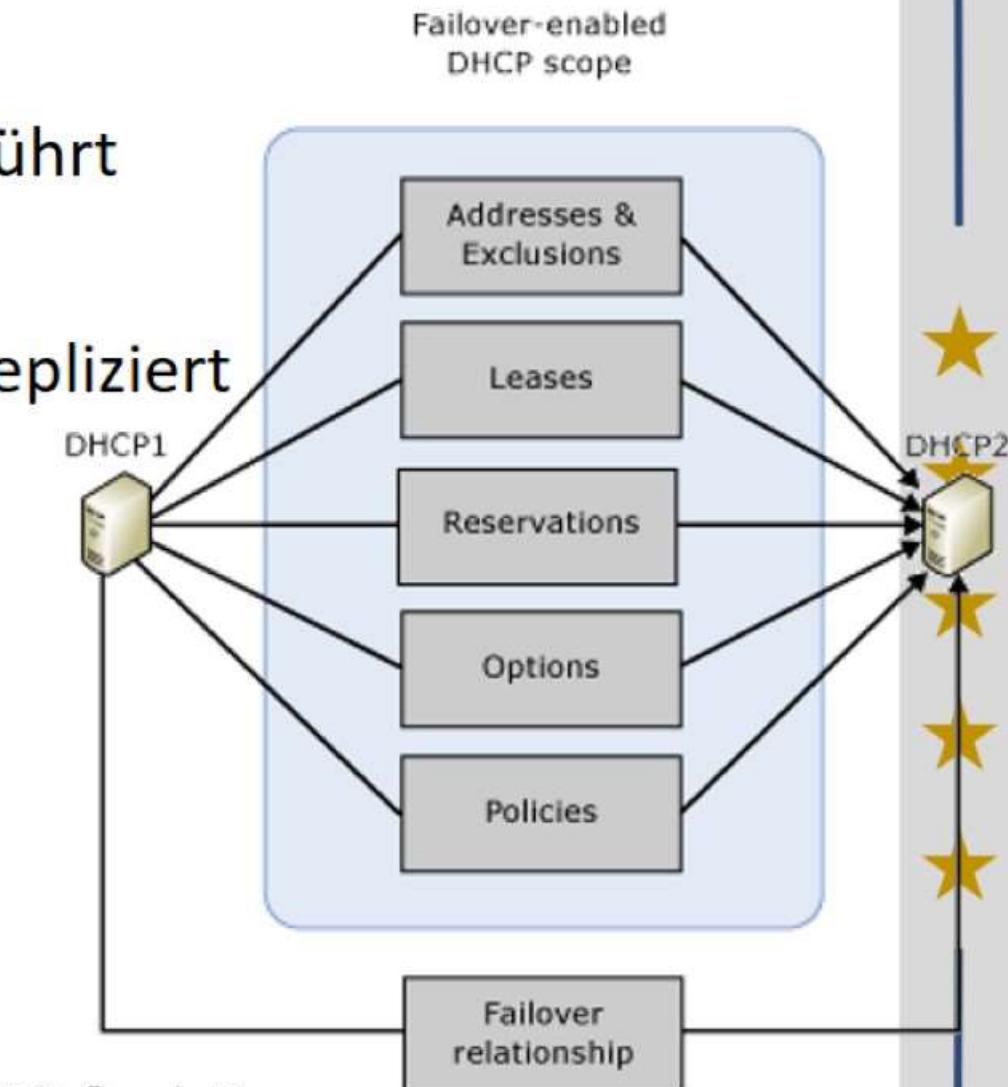
- bei jedem Neustart
- wenn die Hälfte der Leasezeit abgelaufen ist



DHCP

Failover

- wurde mit Windows Server 2012 R2 eingeführt
- Hochverfügbarer DHCP Server
- es werden alle Einstellungen, Leases usw. repliziert
- zwei Modi für den Partner Server
 - Lastenausgleich
 - Bereich wird 50 / 50 aufgeteilt
 - Hot Standby
 - StandbyServer bekommt default 5 % des Bereichs



DHCP

Failover

Failover konfigurieren

Neue Failoverbeziehung erstellen

Erstellen Sie eine neue Failoverbeziehung mit dem Partner "srv2.kurs.intern".

Name der Beziehung:

Maximale Clientvorlaufzeit: Stunde Minuten

Modus:

Lastenausgleich in Prozent

Lokaler Server:

Partnerserver:

Intervall für Zustands-Switchover: Minuten

Nachrichtenauthentifizierung aktivieren

Gemeinsamer geheimer Schlüssel:

- Maximale Clientvorlaufzeit
 - Lease Dauer im FailoverFall (Status: „Partner down“)
- Modus
 - Lastenausgleich
 - Bereich wird 50 / 50 aufgeteilt
 - Hot Standby
 - StandbyServer bekommt default 5 % des Bereichs
- Intervall für den Zustands-Switchover
 - beschreibt Zeit wann vom Status „Communication interrupted“ automatisch zu Status „Partner down“ gewechselt wird
- Nachrichtenauthentifizierung aktivieren
 - wenn aktiviert, wird die Kommunikation zwischen den Partner SHA-256 verschlüsselt (Authentifizierung mit SHA-2)
 - einmalige Eingabe des geheimen Schlüssels, wird danach nicht mehr benötigt da vom Assistenten an beide Seiten gesendet wird

DoD

Application	Data	Data
Host To Host	Message	TCP Header + Data
Internet	Packet	IP Header + TCP Header + Data
Network Access	Frame	Mac Header + IP Header + TCP Header + Data + Prüfsumme

ARP

- Adress Resolution Protocol
- „ARP Request“ an MAC Broadcast
- Um IP Adresse an MAC Adresse zuzuordnen
- ARP Table
 - Lässt sich mit „`arp -a`“ anzeigen
- Gültigkeit wenige Minuten

IP

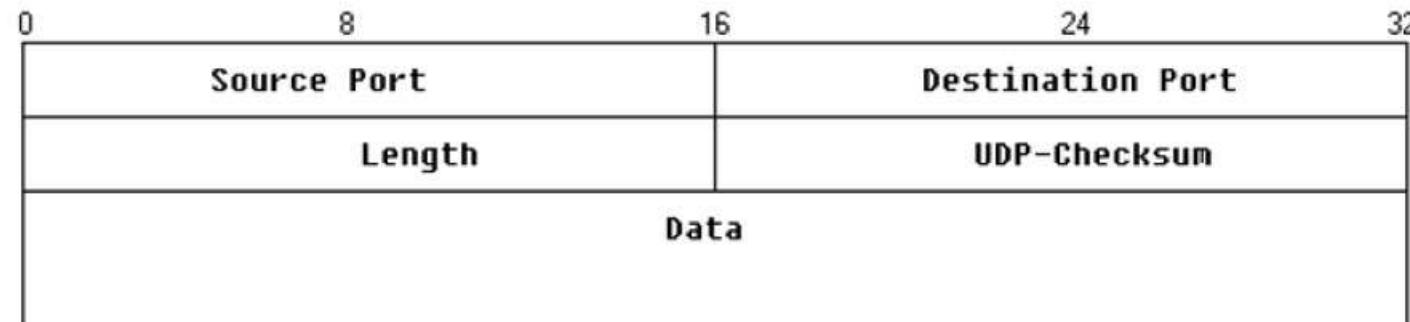
- Verbindungsloses Protokoll
- Version = IP Protokollversion
- IHL (Internet Header Length)
- Type of Service (Steuerinformationen)
- Total Length (Gesamtlänge des Datagramms. Max 64 Kbyte)
- Identification (eindeutige Kennung, Zusammengehörigkeit von Fragmenten)
- Flags (stehen für „dont Fragment“ oder „More fragments“)
- TTL (jeder Gateway decrementeert feld „Hop Counter“)
- Protocol (Upper Layer Protocol zb TCP, UDP, ICMP)
- Header Checksum (16 Bit Länge)
- Options (zb Record Route „Weg des Datagramms protokollieren“)
- Paddings (Füllbits)

0	8	16	24	31
Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
TTL	Protocol		Header Checksum	
Source Address		Destination Address		
Options			Padding	
Data				

UDP

User Datagram Protocol

- Verbindunglos
- Nicht zuverlässig
- Ungesichertes ungeschütztes Übertragungsprotokoll
- Keine Garantie das Paket unverändert ankommt
- Keine Garantie der richtigen Reihenfolge

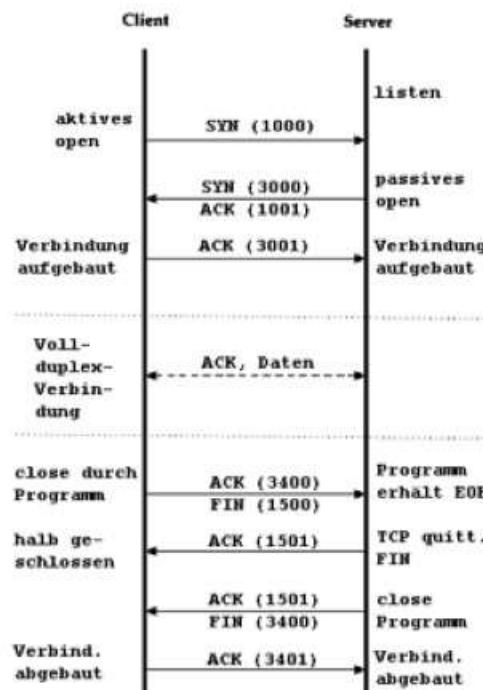


TCP

Transmission Control Protocol

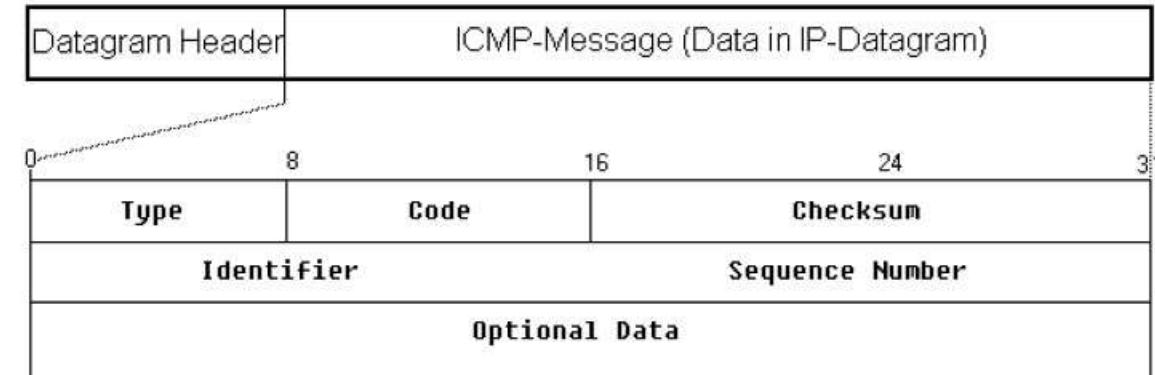
- Verbindungsorientiert
- Jedes Paket kommt einmalig an
- Handshake

Source Port		Destination Port																	
Sequence Number						Acknowledgement Number													
Data Offset	Reserved	Code						Window											
		U	A	P	R	S	F	U	R	C	S	Y	I						
G	K	H	T	N	N														
Checksum						Urgent Pointer													
Options																			
Data																			



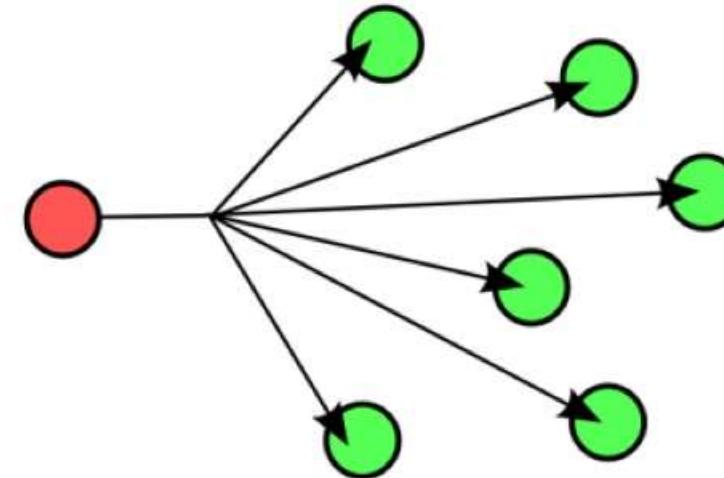
ICMP

- Internet Control Message Protocol
- Type zb. 0 Echo reply , 3 Destination unreachable
- Windows (zb ping oder tracert)



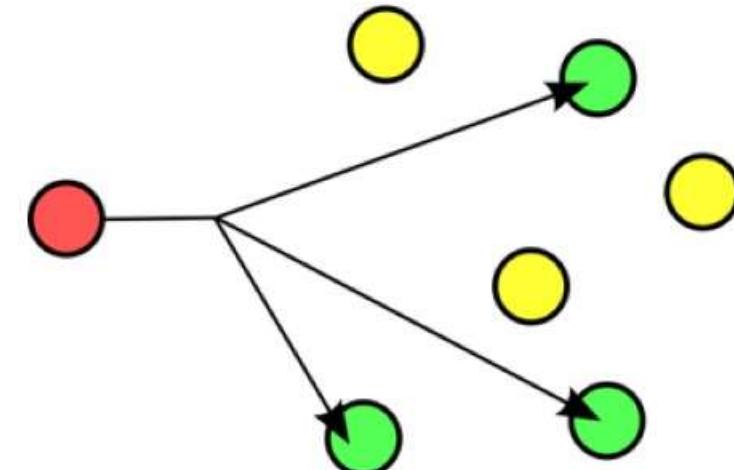
Broadcast

- Limited Broadcast
 - Ziel 255.255.255.255
 - Router leitet nicht weiter
- Directed Broadcast
 - An Broadcast IP des Netz
 - Wird weitergeleitet von Routern wenn Quell und Ziel Netz unterschiedlich



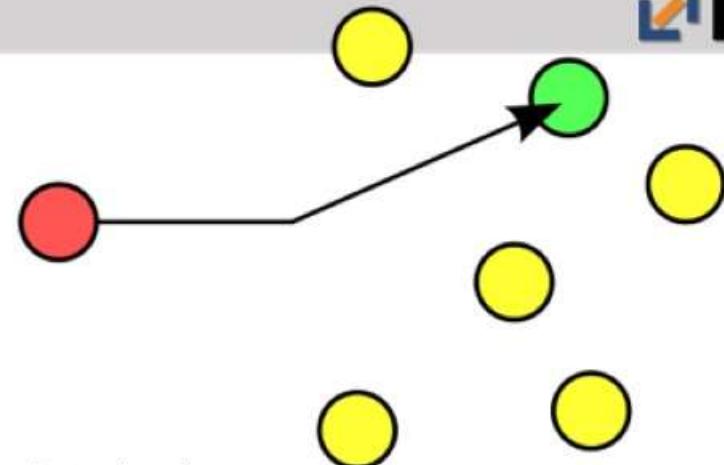
Multicast

- Nachricht von einer Stelle an eine Gruppe
- Adressbereich 224.0.0.0 bis 239.255.255.255
- Datenübertragung muss explizit beim server angemeldet werden



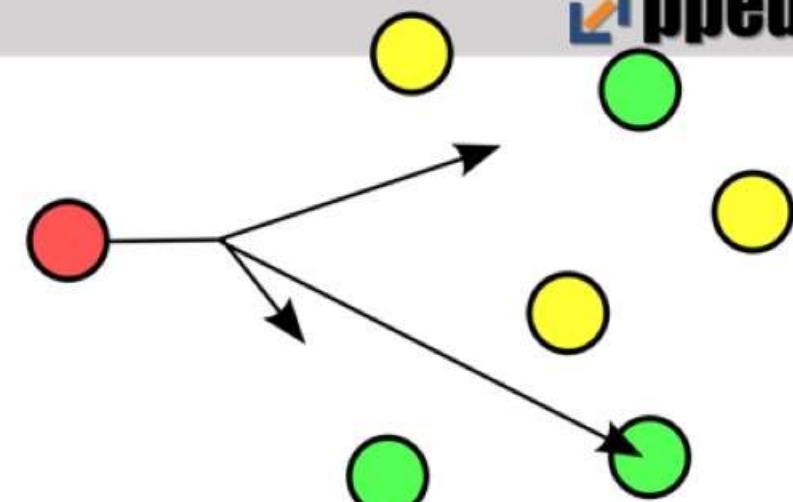
Unicast

- Verbindung zwischen zwei TN
- Unicast Adresse aus Layer3 (Vermittlungsschicht)



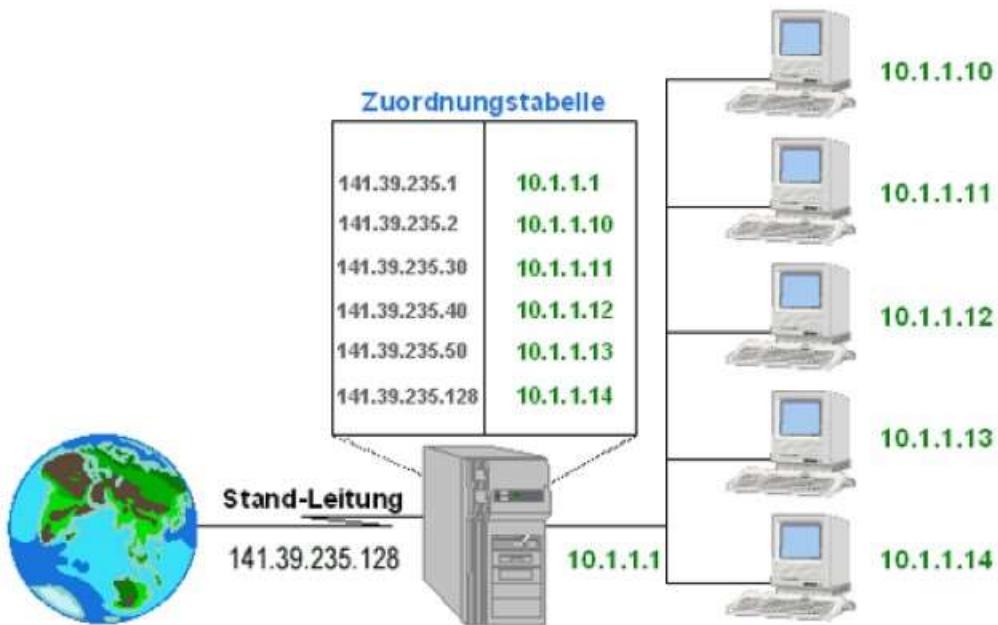
Anycast

- Gleichartige Server erhalten die gleiche IP
- Server Geografisch weit verteilt
- Erhöht die Verfügbarkeit
- Lastverteilung durch Routen
- Es wird immer der nächste Server kontaktiert
 - Zb bei DNS Server im Einsatz



NAT

- Network Adress Translation
- Private Adresse an öffentliche Adresse zuordnen



SNAT

- Source Network Adress Translation
- Mehrere Clients kommunizieren über eine öffentliche Adresse

DNAT

- Destination Network Adress Translation
- Verbindung wird von außen aufgebaut
- Paket wird an definierte interne Zieladresse geleitet

IP Masquerading

- Auch PAT (Port and Adress Translation bezeichnet)
- Einzelne Ports einer öffentlich Adresse werden an verschiedene interne IP Adressen weitergeleitet

VPN

VPN-PPTP

- Point-to-Point-Tunneling-Protkoll
- Alle Betriebssysteme
- Verschlüsselung mit nur 128 Bit
- Nicht besonders sicher

VPN-L2TP/IP

- Layer 2 Tunneling Protocol
- Sicherer als PPTP
- Zweifache Verschlüsselung
- Benötigt mehr Rechenleistung
- Sichere Alternative zu OpenVPN
- 256 bit Verschlüsselung

VPN-OpenVPN

- Sicherste und leistungsfähigstes Protokoll
- Daten werden mit digitalen Zertifikaten authentifiziert
- Hohe Geschwindigkeiten
- SSL / TLS Verschlüsselung
- 256 Bit Verschlüsselung

Routing

- Wegsuche über mehrere Wege bis zum Ziel
- Unterschiede in
 - Routing-Algorithmen
 - Metriken
 - Administrativen Verwaltungsaufwand
- Interior Routing Protocols
 - „für lokale Netzwerke“
 - RIP
 - OSPF

Routing

- Exterior Routing Protocol
- Routing Protokoll für das Routing zwischen autonomen Netzen
- Arbeiten mit Präferenzen oder Policies
- Zb:
 - Boarder Gateway Protocol
 - Link-State-Algorithmus

RIP

- Routing Information Protocol
- Arbeitet mit Distance-Vector-Algorithmus
- Alle Router senden eigene Routing Tabellen als Broadcast
- „Entfernung“ wird aus eigenen Tabellen in relation berechnet
- Maximal 15 Hops
 - 16. Hop ist Infinity und meldet das Netz nicht erreichbar

OSPF

- Open Shortest Path First
- Dynamische Lastverteilung
- Geringer Overhead
- Mehr als 14 Hops möglich (bis zu 65 000)
- OSPF v2 für IPv4
- OSPF v3 für IPv6
- Spanning Tree Verfahren zur Routenfindung
 - Alle vernetzten Punkte nur durch einen Weg miteinander verbunden
 - Wenn BPDU nicht durchkommt wird neuorganisiert