

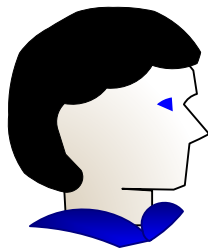
Domain Name System (DNS)

Wozu DNS?

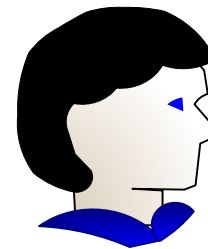
**Menschen merken sich Wörter
leichter als Zahlen!**

80.123.239.24 ???

www.technikum-wien.at



User



User

Chronologie des Internets

1969	Die Network Working Group wird gegründet und erstellt die ersten Protokollbeschreibungen; die ersten vier Knoten des ARPANET (<i>Advanced Research Projects Agency Network</i>) gehen in Betrieb.
1971	Das ARPANET besitzt 15 Knoten. Telnnet und FTP werden entwickelt.
1972	Ray Tomlinson entwickelt das erste E-Mail-Programm.
1973	Das Transmission Control Protocol (TCP) wird publiziert.
1977	Das ARPANET besitzt 111 Knoten.
1982	ISO veröffentlicht OSI Referenzmodell
1983	TCP/IP wird zur universellen Sprache des Internets Das ARPANET hat 400 angeschlossene Rechner.
1984	Das Domain Name System (DNS) wird entwickelt. Das ARPANET hat 1.000 angeschlossene Rechner.
1987	Das ARPANET hat 10.000 Internet Hosts.

Auflösung IP in Hostnamen vor DNS

- „Host Names On-Line“ 1973/74 RFC 606 u. 608
- Auflösung der IP-Adressen durch Einträge in Hosts Datei

```
hosts - Editor
Datei Bearbeiten Format Ansicht ?
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Dies ist eine HOSTS-Beispieldatei, die von Microsoft TCP/IP
# für windows 2000 verwendet wird.
#
# Diese Datei enthält die Zuordnungen der IP-Adressen zu Hostnamen.
# Jeder Eintrag muss in einer eigenen Zeile stehen. Die IP-
# Adresse sollte in der ersten Spalte gefolgt vom zugehörigen
# Hostnamen stehen.
# Die IP-Adresse und der Hostname müssen durch mindestens ein
# Leerzeichen getrennt sein.
#
# Zusätzliche Kommentare (so wie in dieser Datei) können in
# einzelnen Zeilen oder hinter dem Computernamen eingefügt werden,
# aber müssen mit dem Zeichen '#' eingegeben werden.
#
# Zum Beispiel:
#
#      102.54.94.97      rhino.acme.com      # Quellserver
#      38.25.63.10      x.acme.com          # x-Clienthost
#
127.0.0.1      localhost
195.245.225.43  cis.technikum-wien.at
128.130.2.9    www.tu-wien.ac.at
```

Nachteile von Host Datei

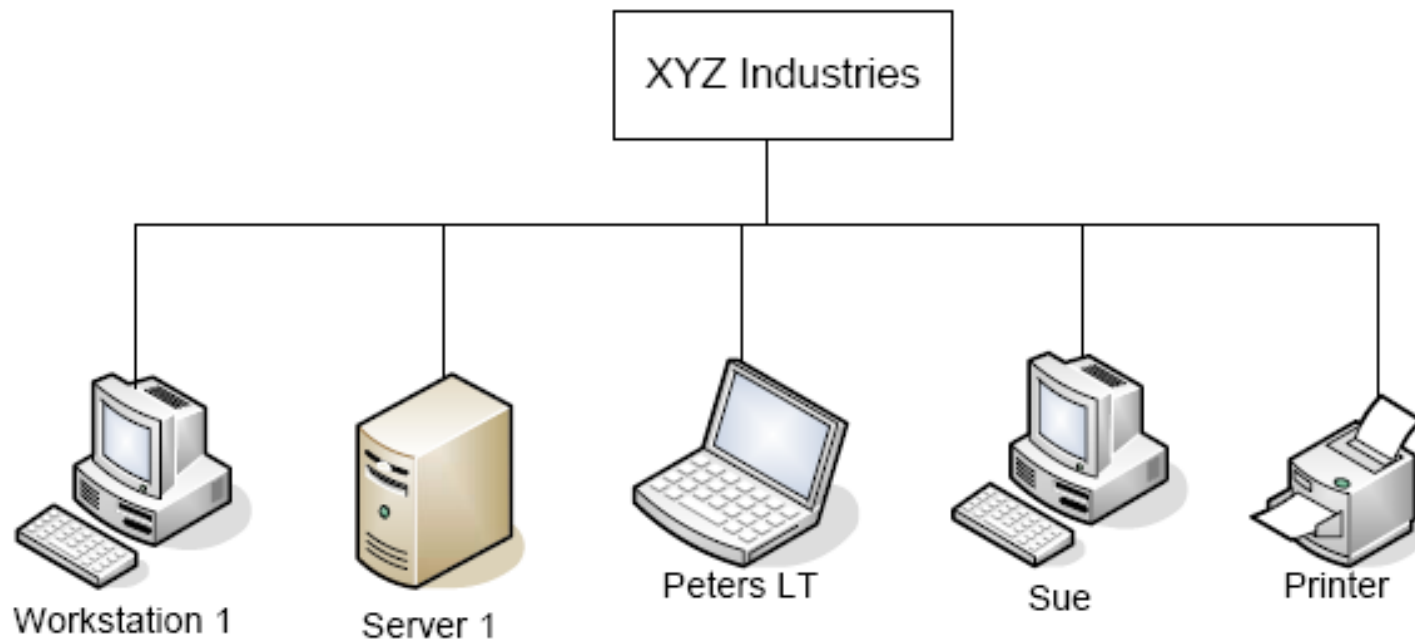
- Hoher Administrativer Aufwand durch häufige Veränderungen
- Langsames Reagieren auf Veränderungen im Netz
- Stetig wachsender Platzverbrauch durch größer werdende Hostdateien
- Hoher Bandbreitenverbrauch durch das Überspielen der Hostdateien an die Hosts
- Menschliches Versagen durch Tippfehler oder Vergessen von Hostupdates
- Probleme durch flachen Namensraum

Namensräume

- Der Grundgedanke eines Namenssystems ist, eine Möglichkeit zur Verfügung zu stellen um Vorrichtungen mit symbolische Namen zu kennzeichnen.
- Die Architektur des Namensraumes stellt fest, ob Namen als einfacher unstrukturierter Satz Symbole oder als eine komplizierte interne Struktur verwendet werden.

Flache Namensarchitektur

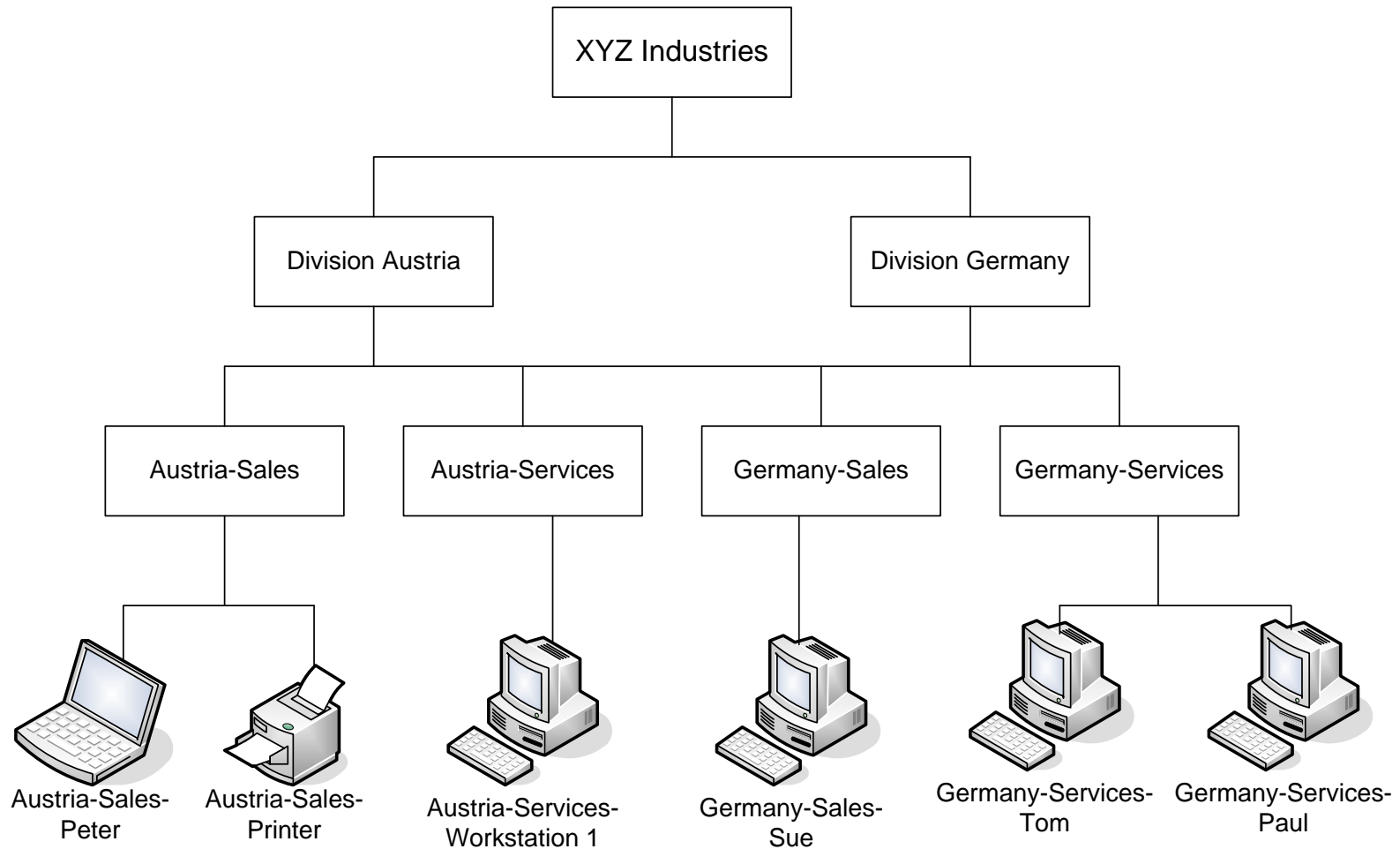
- Reihenfolge von Symbolen zugewiesen ohne irgendeine interne Struktur.
- Es gibt kein Verhältnis zwischen jedem möglichem Namen und irgendeinem anderen Namen.



Hierarchische Namensarchitektur

- In hierarchischer Namensarchitektur sind die Namen eine Reihenfolge von Symbolen, diese werden anhand einer spezifischen Struktur zugewiesen.
- Jeder Name besteht aus diskreten Elementen, die untereinander verbunden sind (meist durch eine Eltern/Kind Semantik)

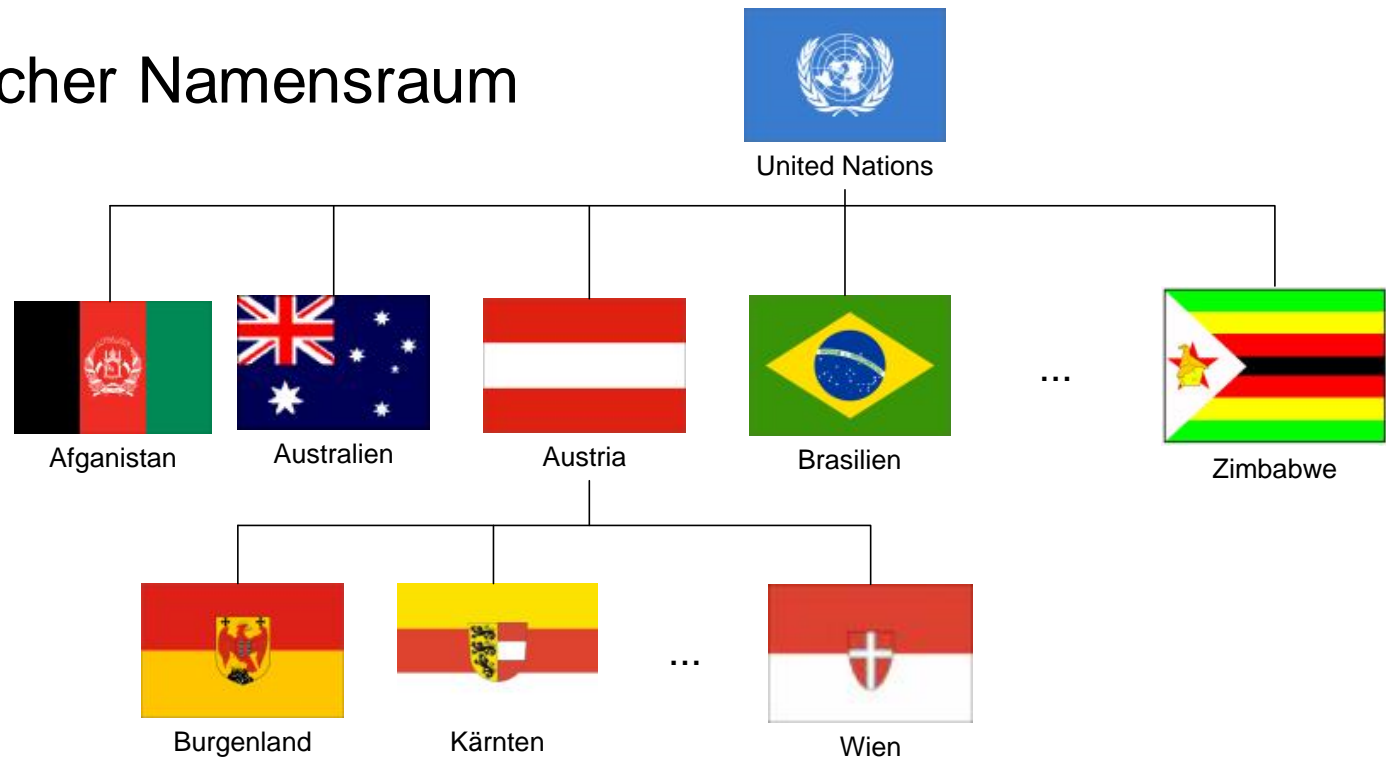
Beispiel hierarchischer Namensraum



Domains

- Ein Bereich des Einflusses, der Steuerung oder des politischen Einflusses

- Hierarchischer Namensraum



Fully Qualified Domain Name (FQDN)

- Dient der eindeutigen Bestimmung eines Knotens im hierarchischen Namensraum.
- Die Notation erfolgt durch die Aneinanderreihung der Namen aller Knoten getrennt durch einen Punkt. Von links nach rechts vom untersten Knoten bis zur Wurzel.
 - Wien.Austria.United Nations.
 - www.technikum-wien.at.
 - ftp.technikum-wien.at.

Top Level Domains (TLD)

- Höchste Ebene der Namensauflösung
- TLDs können dabei drei Hauptgruppen aufgeteilt werden:
 - allgemeine TLDs (*generic TLD*)
 - länderspezifische TLDs (*country-code*)
 - gebietsspezifische TLDs

Ursprüngliche allgemeine TLD

- .arpa – TLD des ursprünglichen Arpanets (inzw. veraltet)
- .com – Kommerzielle Organisationen
- .edu – Bildungseinrichtungen (4-jährig)
- .gov – Regierungsorgane der USA
- .int – Internationale Organisationen
- .mil – US Militär
- .net – große Network-Support-Center
- .org – Nichtkommerzielle Organisationen

Beispiele für neue allgemeine TLD

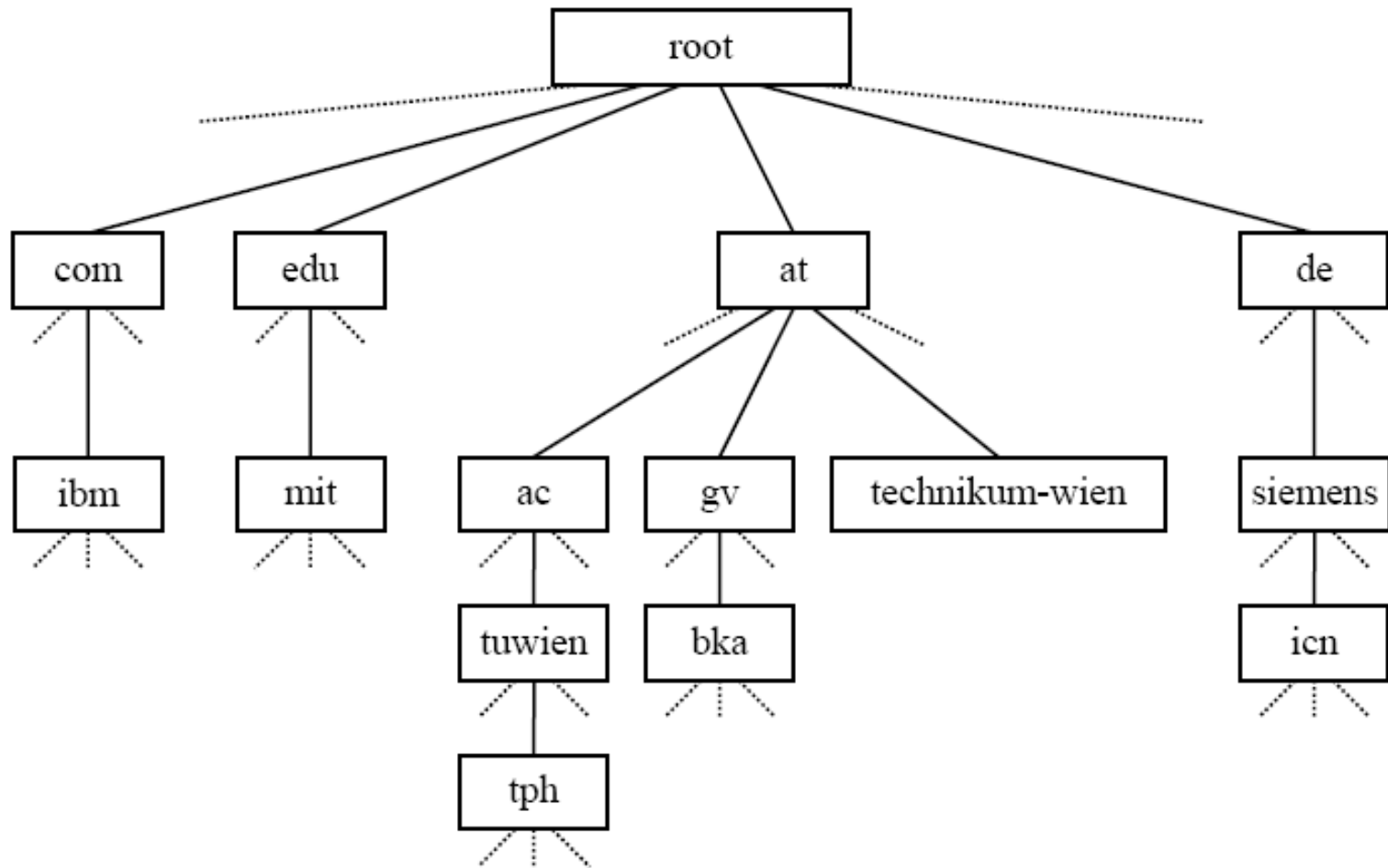
- .aero –Luftfahrt tätige Organisationen
- .biz –Handelsfirmen
- .coop –Genossenschaften
- .info – Informationsanbieter
- .jobs - Firmen mit Stellenangeboten
- .mobi - Webseiten speziell für mobile Endgeräte
- .museum – Museen
- .name –natürliche Personen oder Familien
- .pro –Anwälte, Steuerberater, Ärzte in den USA
- .travel – für die Reise-Industrie

Länderspezifische TLD

- Bestehen aus 2 Buchstaben des ISO 3166 Ländercodes
- Viele Länder unterteilen ihre Länderdomain noch durch länderspezifische Second Level Domain.
 - Österreich:
 - co.at
 - ac.at
 - USA:
 - ny.us

ae	United Arab Emirates
at	Austria
ch	Suisse
de	Germany
fr	France
it	Italy
uk	United Kingdom
us	United States
zw	Zimbabwe

Hierarchische Baumstruktur von Internet domain servers



Domain Name System Server

DNS Server Funktionen (1)

- **Interagieren mit anderen Servern:** DNS-Auflösungsprozess erfordert häufig, dass mehrere Server beteiligt sind.
- **Zonenmanagement und -übertragungen:** Der Server muss DNS-Informationen innerhalb der Zone für die er zuständig ist bearbeiten können. Außerdem muss er seine kompletten Informationen an untergeordnete Server weitergeben können.

DNS Server Funktionen (2)

- **Leistungsverbessernde Funktion:** Aufgrund der hohen Anzahl an DNS Anfragen verwendet der Server Techniken, um die Bearbeitungszeit zu verringern.
 - Cachen der Namensinformationen
 - Loadbalancing

- **Administration:** Viele administrative Details werden von den Servern abgespeichert. z.B.
 - Kontaktinformationen
 - MX Record

Name Server Typen

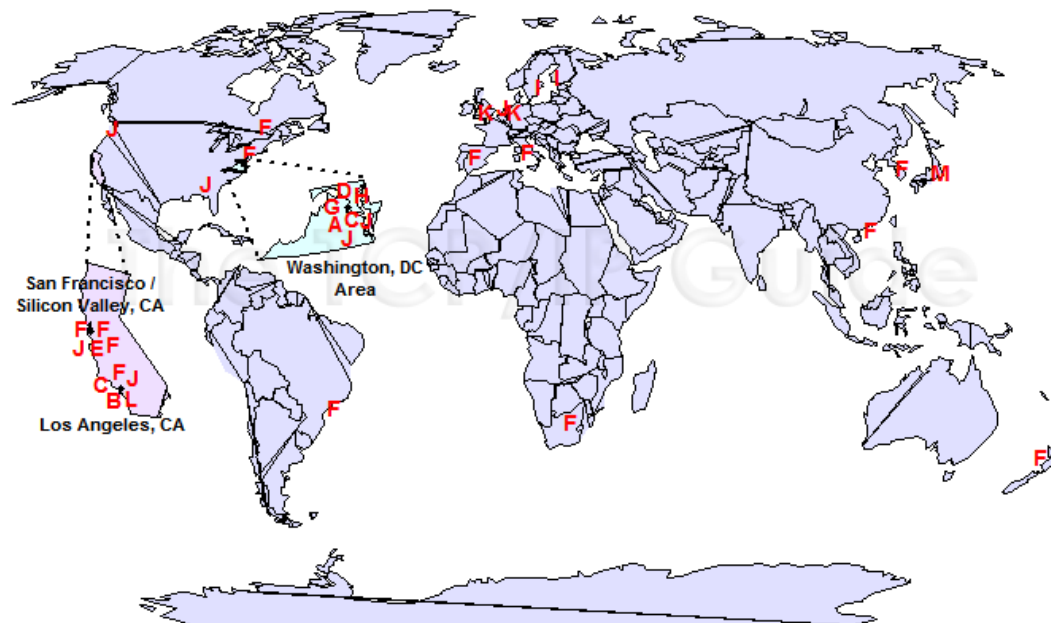
- **Primary bzw. Master name server**
 - Hat Autorität über seine Zone. Bezieht seine Zoneninformation von der eigenen Harddisk.
- **Secondary bzw. Slave name server**
 - DNS-Informationen qualitativ gleichwertig zum Primary und ist ebenfalls autorativ für die Zone. Er holt seine Zoneninformationen vom Primary durch Zonentransfer.
- **Caching-only name server**
 - Hat selbst keine Autorität, bezieht die Informationen vom Primary oder Secondary.

Gründe für Secondary name server

- **Redundanz:** Ausfallssicherheit des Dienstes
- **Wartbarkeit:** Wartung eines Servers ist kein Problem wenn andere weiter den Dienst anbieten.
- **Lastenausgleich:** Bei vielen Anfragen kann so die Last auf mehrere Server verteilt werden.
- **Effizienz:** Verteilung von mehreren Name Servern kann zur Effizienzsteigerung führen. Z.B. entferntes Büro angeschlossen über langsame WAN Verbindung.

Root Name Server

- Es gibt 13 Root Name Server die von 12 unterschiedlichen Organisationen betrieben werden
 - a.root-servers.net bis m.root-servers.net
- Es handelt sich aber nicht um 13 Server sondern um Cluster, insgesamt sind es hunderte von Einzelservers



Typische Arten der DNS Auflösung

- **Namensauflösung:** Liefert IP Adresse zu einem Domainnamen
- **Umgekehrte Namensauflösung:** Liefert den Namen zu einer IP Adresse
- **Auflösung der Elektronischen Mail:** Liefert die IP Adresse des Mailservers einer Domain

Domain Name System Resolver

Aufgaben des Resolver

- DNS Client heißt **RESOLVER**
- Unterstützt Applikationen mit DNS Informationen
- Erstellt DNS Anfragen an den Server
- Verarbeitet das Ergebnis und beliefert die anfragende Applikation

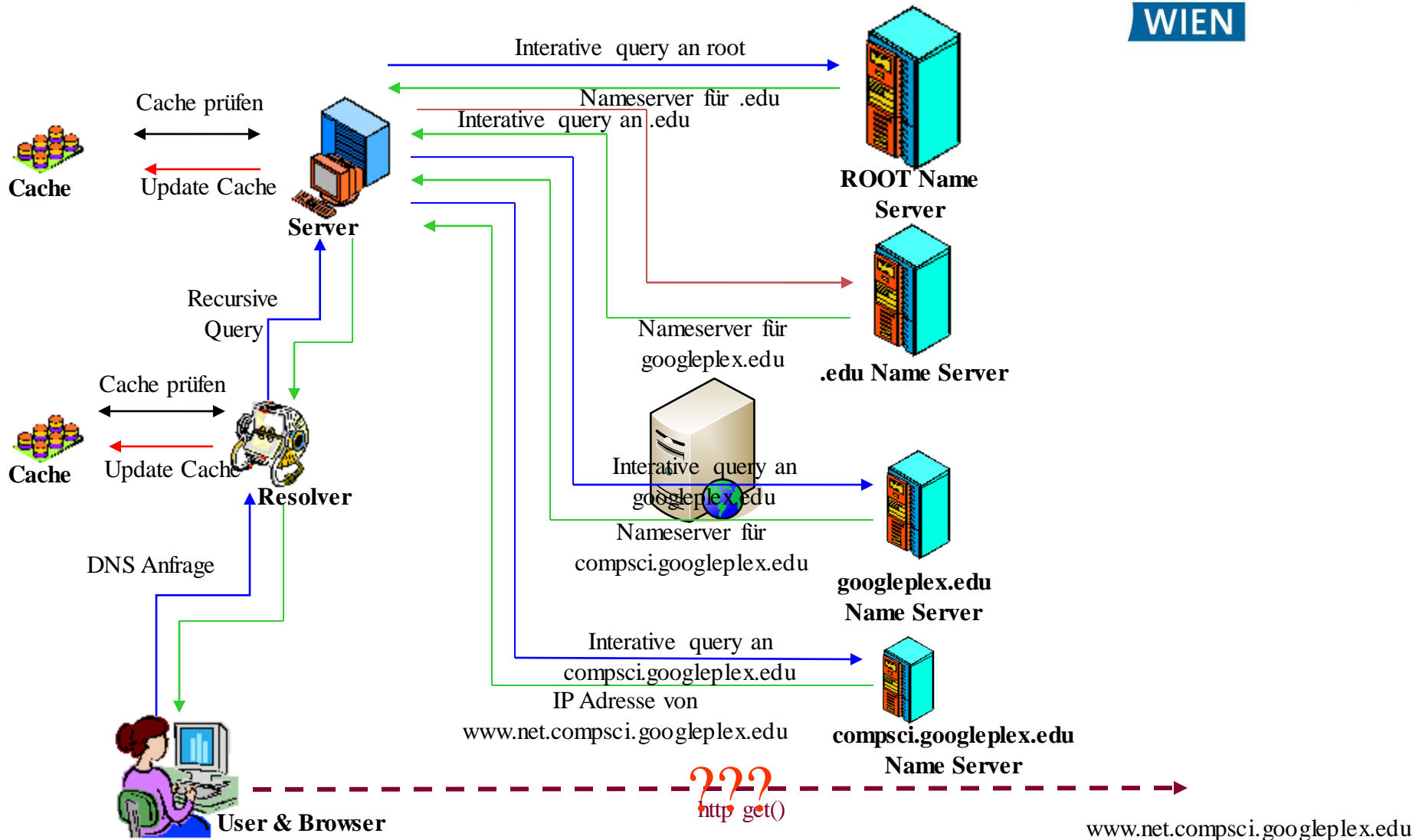
Abfragearten

- **Rekursive Abfrage:** Der Resolver stellt eine Abfrage an den Server und dieser beschafft alle benötigten Informationen. Wird von Hosts verwendet.
- **Iterative Abfrage:** Der Resolver stellt eine Anfrage an den Server, der liefert wenn er das Ergebnis nicht weiß, die IP Adresse des „zuständigeren“ Servers. Der Resolver fragt nun diesen usw. bis er die Antwort kennt. Wird von DNS Servern verwendet.

Arten von Resolver

- **Full resolver:** Kann rekursive und iterative Abfragen verwenden. Server
- **Stub resolver:** Kann nur rekursive Abfragen verwenden. Host

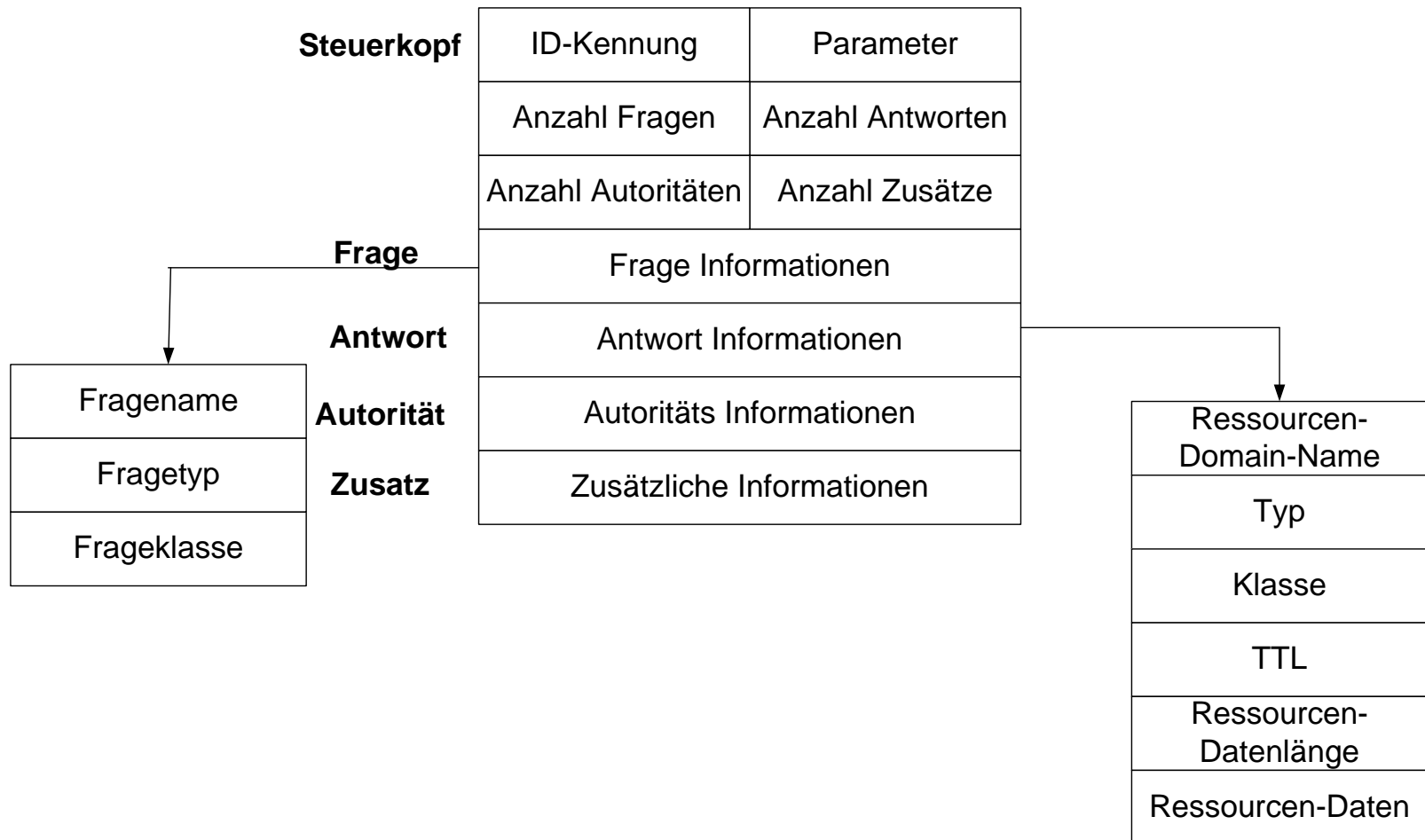
DNS Prozess



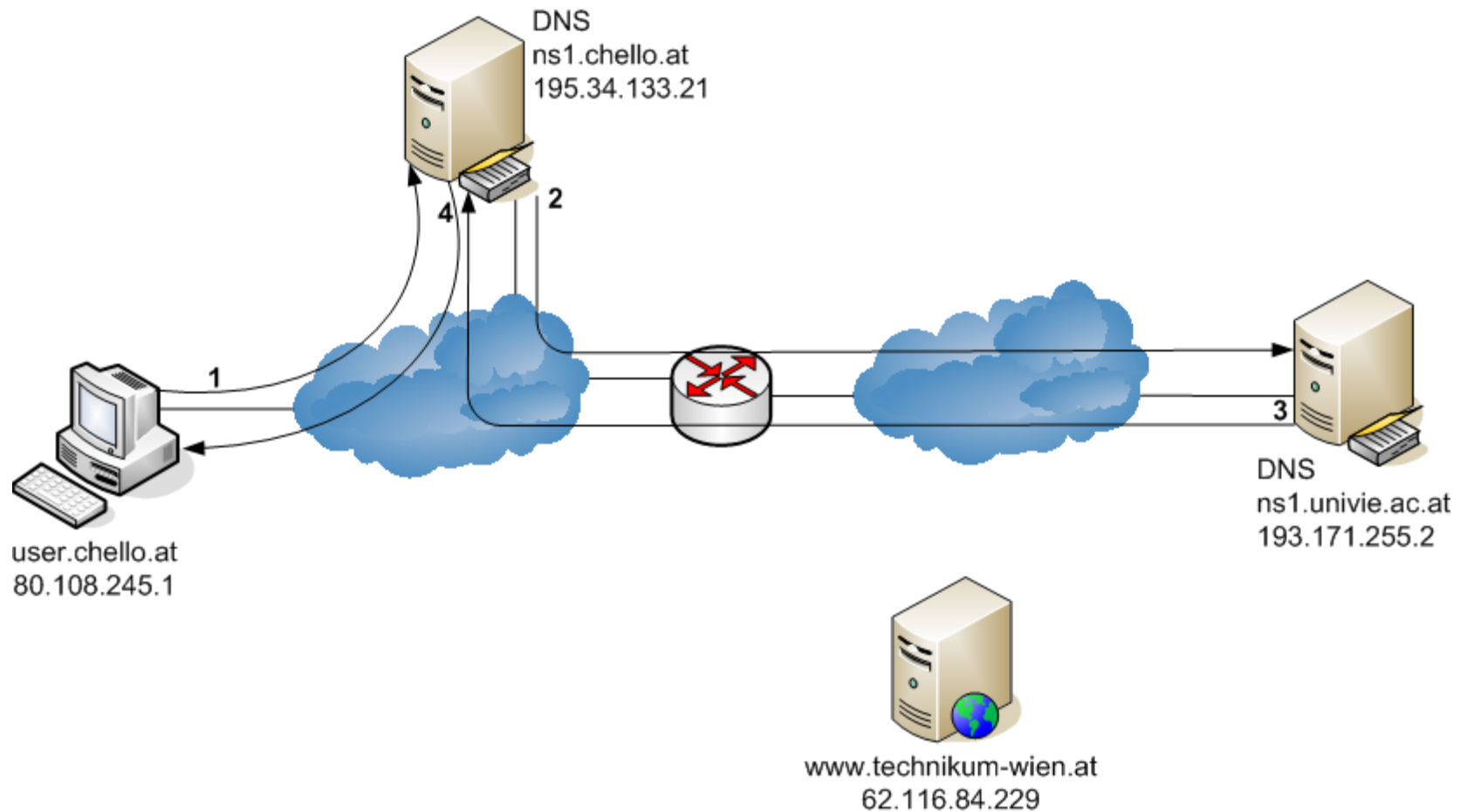
DNS Protokoll

- Besitzt 5 Abschnitte
 - Protokollkopf
 - Anfrage
 - Antwort
 - Informationen über Autorität
 - Zusätzliche Informationen
- Anforderungen und Antworten verwenden dasselbe Format
- Formatsabhängig sind nicht alle Felder befüllt

DNS Protokoll



Beispiel DNS Anfrage



Beispiel DNS Anfrage (1)

DNS Anfragepaket von user.chello.at and ns1.chello.at

MAC Kopf		
IP Kopf		
IP-Adressen	Empfänger = 195.34.133.21	Absender = 80.108.245.1
DNS Kopf	ID-Kennung	Parameter = QR+RD
	Anzahl Fragen = 1	Anzahl Antworten = 0
	Anzahl Autoritäten = 0	Anzahl Zusätze = 0
Frage	Name = www.technikum-wien.at	Typ = A Klasse = IN

Parameter: QR = Anfrage; RD = Rekursion gefordert

Typ: A = Host Adresse

Klasse: IN = Internet

Beispiel DNS Anfrage (2)

DNS Anfragepaket von ns1.chello.at an ns1.univie.ac.at

MAC Kopf		
IP Kopf		
IP-Adressen	Empfänger = 193.171.255.2	Absender = 195.34.133.21
DNS Kopf	ID-Kennung	Parameter = QR
	Anzahl Fragen = 1	Anzahl Antworten = 0
	Anzahl Autoritäten = 0	Anzahl Zusätze = 0
Frage	Name = www.technikum-wien.at	Typ = A Klasse = IN

Parameter: QR = Anfrage

Typ: A = Host Adresse

Klasse: IN = Internet

Beispiel DNS Anfrage (3)

DNS Antwortpaket von ns1.univie.ac.at an ns1.chello.at

MAC Kopf		
IP Kopf		
IP-Adressen	Empfänger = 195.34.133.21	Absender = 193.171.255.2
DNS Kopf	ID-Kennung	Parameter = ResponseBit, RA
	Anzahl Fragen = 1	Anzahl Antworten = 1
	Anzahl Autoritäten = 0	Anzahl Zusätze = 0
Frage	Name = www.technikum-wien.at	Typ = A Klasse = IN
Antwort	Name = (Zeiger auf Frage Abschnitt) Typ = A Klasse = IN TTL = (20.864 Sekunden) Länge = 4 Antwort = 62.116.84.229	

Parameter: RA = Rekursion verfügbar

Typ: A = Host Adresse

Klasse: IN = Internet

TTL: legt fest wie lange die Antwort zwischengespeichert wird (hier etwa 5h 48min)

Beispiel DNS Anfrage (4)

DNS Antwortpaket von ns1.chello.at an user.chello.at

MAC Kopf		
IP Kopf		
IP-Adressen	Empfänger = 80.108.245.1	Absender = 195.34.133.21
DNS Kopf	ID-Kennung	Parameter = ResponseBit RD
	Anzahl Fragen = 1	Anzahl Antworten = 1
	Anzahl Autoritäten = 0	Anzahl Zusätze = 0
Frage	Name = www.technikum-wien.at	Typ = A Klasse = IN
Antwort	Name = (Zeiger auf Frage Abschnitt) Typ = A Klasse = IN TTL = (20.864 Sekunden) Länge = 4 Antwort = 62.116.84.229	

Parameter: RD = Rekursion gefordert

Typ: A = Host Adresse

Klasse: IN = Internet

TTL: legt fest wie lange die Antwort zwischengespeichert wird (hier etwa 5h 48min)

DNS Abfragetypen

- Diese werden von der IANA ausgegeben
- Typische Abfragearten
 - A - host Adresse
 - MX – Mailserver Adresse
 - NS – Zuständiger Nameserver
- Es gibt aber noch sehr viele weitere andere Abfragetypen
 - <http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml>

DNS Abfragen

- DNS liefert viele Informationen über öffentliche und manchmal auch private Server
 - IP Adresse
 - Server Namen
 - Server Funktion
- Verschiedenste DNS Clients
 - Host, nslookup, dig

```
root@kali:~# nslookup technikum-wien.at
Server:      192.168.146.2
Address:     192.168.146.2#53

Non-authoritative answer:
Name:   technikum-wien.at
Address: 94.136.22.156
```

MX Queries

- Identifizierung des Mail Servers

```
root@kali:~# nslookup -type=MX technikum-wien.at
Server:      192.168.177.2
Address:     192.168.177.2#53

Non-authoritative answer:
technikum-wien.at      mail exchanger = 10 polyxena.technikum-wien.at.
technikum-wien.at      mail exchanger = 10 mail.technikum-wien.at.

Authoritative answers can be found from:
technikum-wien.at      nameserver = samba4dc1.technikum-wien.at.
mail.technikum-wien.at internet address = 10.127.0.22
polyxena.technikum-wien.at internet address = 10.127.0.21
samba4dc1.technikum-wien.at internet address = 10.63.0.10
```

- Die Zahl vor dem Domain Name zeigt an welcher Mailserver beim Erhalt einer Email präferiert wird
 - Je kleiner die Zahl desto höher die Präferenz
 - Polyxena ist also der Primäre Mail Server

NS Queries

- Identifizierung des Name Server

```
root@kali:~# nslookup -type=NS technikum-wien.at
Server:          192.168.177.2
Address:         192.168.177.2#53

Non-authoritative answer:
technikum-wien.at      nameserver = samba4dc1.technikum-wien.at.

Authoritative answers can be found from:
samba4dc1.technikum-wien.at      internet address = 10.63.0.10
```

DIG

- DIG ist ein noch viel mächtigeres Tool als nslookup
- Allgemeine Ausgabe
 - `dig technikum-wien.at +short`
- Mailserver
 - `dig technikum-wien.at MX`
- Nameserver
 - `dig technikum-wien.at NS`
- Zonentransfer
 - `dig axfr @samba4dc1.technikum-wien.at technikum-wien.at`

Bootstrap und Autoconfiguration (BOOTP, DHCP)

Wichtige Parameter eines TCP/IP Netz

- IP-Adresse
 - Zum Senden und Empfangen von Datagramme
- Subnetmask
 - Unterteilt IP-Adresse in Netzwerk und Hostteil
- Gateway
 - Zum Senden von Datagramme in andere Netze
- DNS
 - Zum Auflösen von Namen in IP-Adressen

Auflistung der Parameter

```
C:\WINDOWS\system32\cmd.exe

C:\>ipconfig /all

Windows-IP-Konfiguration

    Hostname. . . . . : fluffy
    Primäres DNS-Suffix . . . . . :
    Knotentyp . . . . . : Unbekannt
    IP-Routing aktiviert. . . . . : Nein
    WINS-Proxy aktiviert. . . . . : Nein
    DNS-Suffixsuchliste . . . . . : localdomain

Ethernetadapter LAN-Verbindung 2:

    Verbindungsspezifisches DNS-Suffix: localdomain
    Beschreibung. . . . . : NVIDIA nForce Networking Controller
    Physikalische Adresse . . . . . : 00-11-D8-79-FF-D1
    DHCP aktiviert. . . . . : Ja
    Autokonfiguration aktiviert . . . : Ja
    IP-Adresse. . . . . : 10.1.0.10
    Subnetzmaske. . . . . : 255.255.0.0
    Standardgateway . . . . . : 10.1.0.1
    DHCP-Server . . . . . : 10.1.0.1
    DNS-Server. . . . . : 10.1.0.1
    Lease erhalten. . . . . : Sonntag, 26. März 2006 18:06:20
    Lease läuft ab. . . . . : Sonntag, 26. März 2006 19:06:20

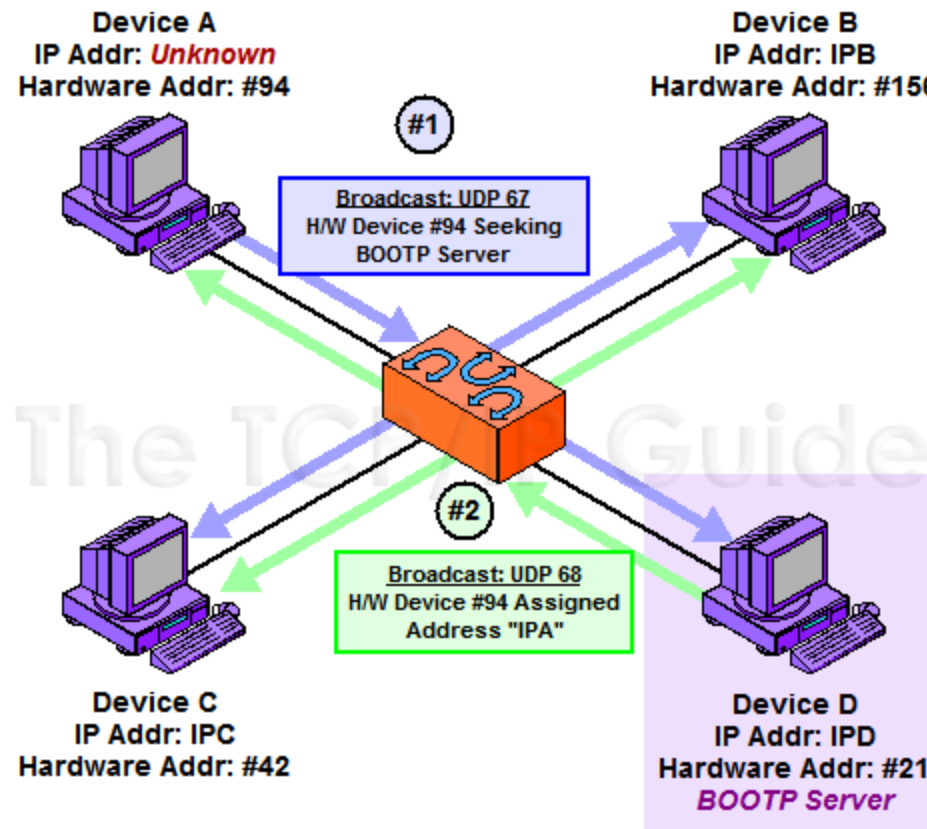
C:\>
```

BOOTstrap Protocol BOOTP

BOOTP

- Entwickelt um Nachteile des RARP zu überwinden
- Client/Server Prinzip
- Verwendet UDP und IP
 - Server Port 67, Client Port 68
- Überträgt IP Adresse und zusätzliche Informationen
- Kann mit Hilfe von Realyagents gerootet werden

Grundsätzlicher Ablauf von BOOTP



BOOTP resend

- Bekannt Probleme durch UDP IP
 - Nachrichten können verloren gehen
 - Nachrichten kommen verzögert mehrfach an
 - IP keine Prüfsumme daher kann UDP Datagramm mit beschädigten Bits ankommen
- BOOTP verwendet konventionelle Zeitüberschreitungs- und Wiederholungstechnik
 - Client startet bei Übertragung Timer
 - Erfolgt innerhalb der Zeit keine Antwort erfolgt resend
 - Zufällige Verzögerung wird benutzt
 - Bei resend wird Verzögerung verdoppelt

Vor und Nachteile

- + BOOTP überträgt mehr Information als RARP
- + Kann in Verbindung mit TFTP Images für Diskless-Computer verwendet werden
- Konzipiert für statische Umgebungen mit seltenen Änderungen
- Keine dynamische IP Adressen zuweisung

Dynamic Host Configuration Protocol DHCP

DHCP

- Ersetzt BOOTP nicht sondern nutzt seine Stärken und erweitert es
- Dynamische IP Adressen Vergabe
- Verbesserte Client/Server Kommunikation
- RFC 2131

DHCP Zuordnungsarten

- Manuelle Zuordnung
 - Anhand der MAC Adresse bekommt der Host immer dieselbe, vom Administrator zugewiesene IP
- Automatische Zuordnung
 - DHCP Server vergibt dem Client automatisch eine permanente IP Adresse dh. Der Client wird später vom Server immer wieder diese IP zugewiesen bekommen
- Dynamische Zuordnung
 - DHCP Server vergibt eine IP Adresse auf Zeit (Lease)

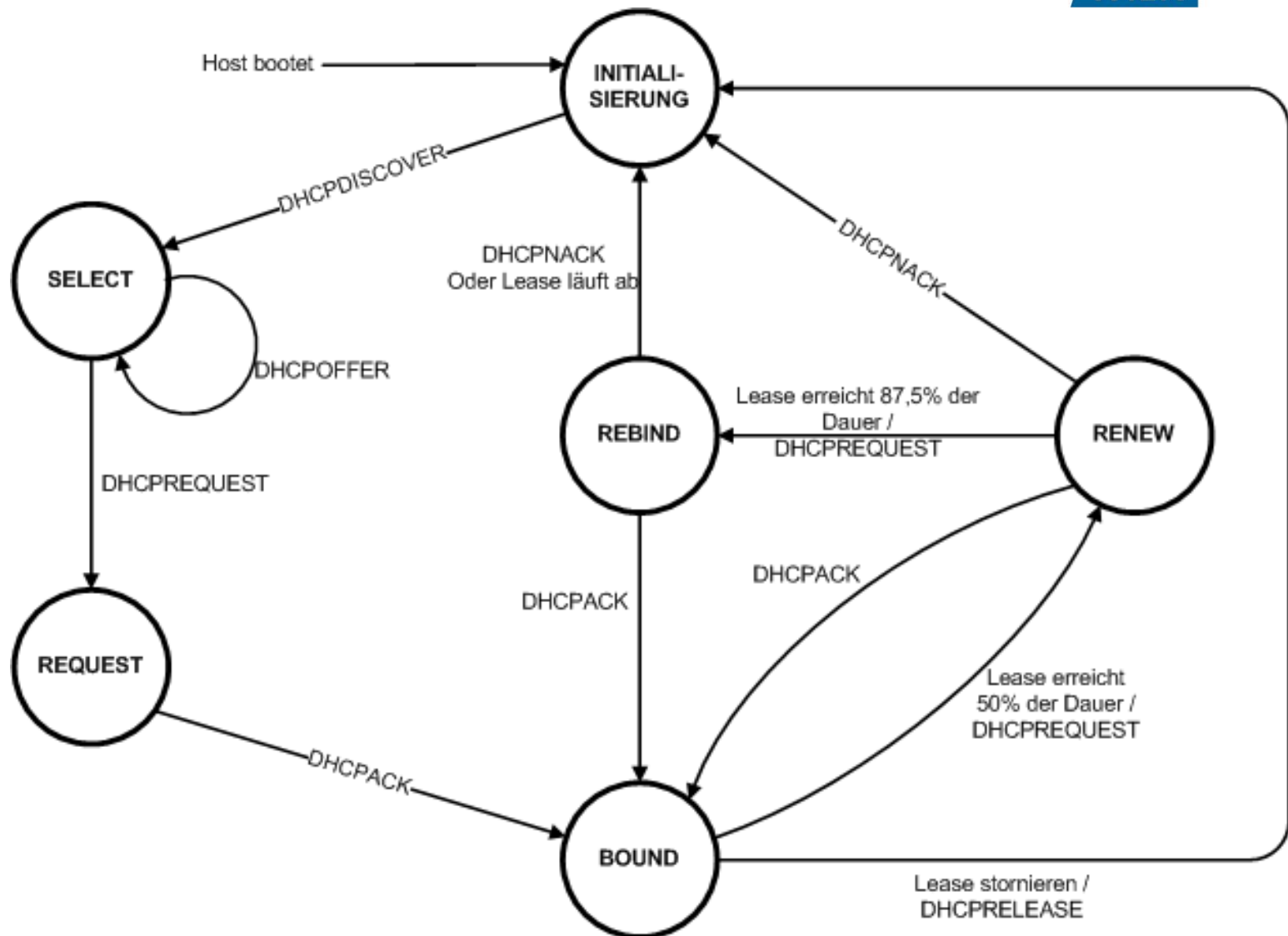
DHCP Nachrichtentyp (1)

- DHCPDISCOVER
 - Broadcast Nachricht an alle DHCP Server dem Client einen IP Vorschlag zu schicken
- DHCPOFFER
 - Servervorschlag einer IP Adresse
- DHCPREQUEST
 - Anfrage von Client eine explizite IP Adresse verwenden zu dürfen
- DHCPDECLINE
 - Nachricht von Client an Server, die vorgeschlagene IP Adresse ist bereits in Verwendung

DHCP Nachrichtentyp (2)

- DHCPACK
 - Bestätigungsnachricht vom Server, dass die IP nun dem Client zugewiesen ist
- DHCPNACK
 - Absage vom Server, Client darf IP Adresse nicht mehr verwenden
- DHCPRELEASE
 - Nachricht vom Client, IP Adresse wird nicht mehr benötigt, Lease wird beendet
- DHCPINFORM
 - Anfrage des Client auf Übermittlung weiterer Parameter

DHCP Finite State Machine (Ausschnitt über wichtigsten Zustände)



DHCP Prozessablauf laut RFC 2131

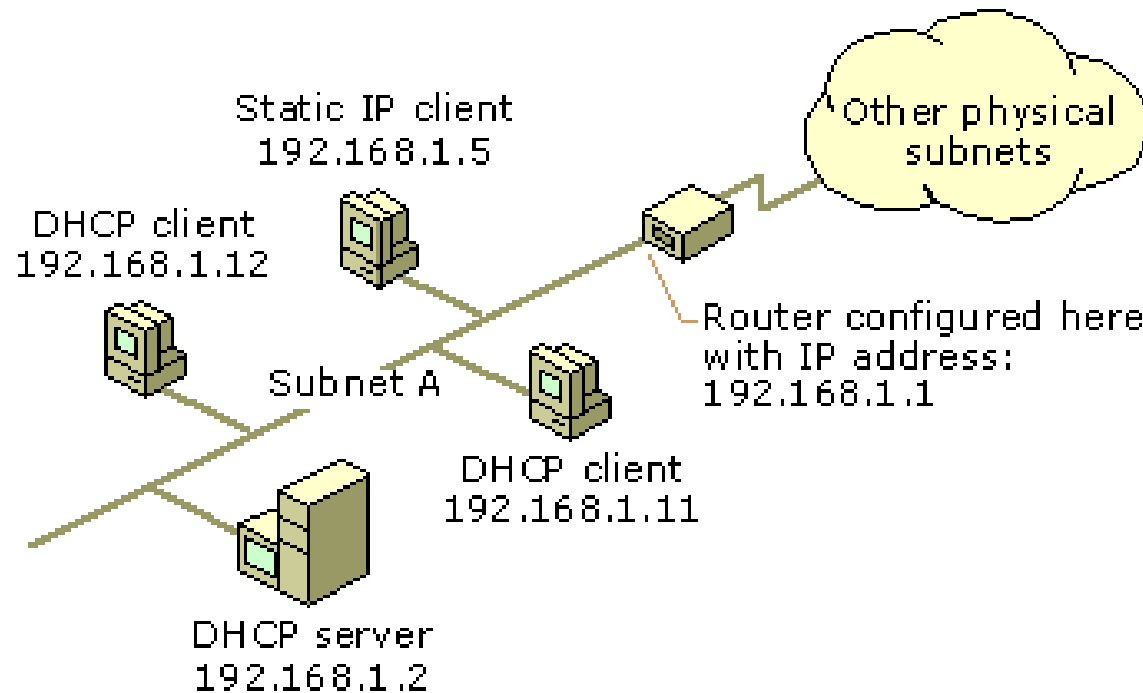
1. Der Client broadcasts ein DHCPDISCOVER
 - Vorschläge hinsichtlich gewünschter IP Adresse oder Leasezeit dürfen (may) angegeben sein
2. Jeder DHCP-Server darf (may) antworten mit einem DHCPOFFER, vorher sollte (should) der Server prüfen ob die IP Adresse bereits vergeben ist (z.B. ICMP Echo request)
3. Der Client erhält ein oder mehrere DHCPOFFER (er kann auch zunächst auf weitere warten) dann entscheidet er sich für eines und sendet ein DHCPREQUEST broadcast zurück inklusive Server Identifier Option

DHCP Prozessablauf laut RFC 2131

4. Die Server erhalten den DHCPREQUEST, jene mit anderem Server Identifier werden das als Absage des Client, der ausgewählte DHCP Server sendet ein DHCPACK inklusive Konfigurationsparamater
5. Der Client erhält das DHCPACK und sollte (should) nochmals überprüfen ob die IP überhaupt frei ist (z.B. ARP Request). Stellt er fest, dass die IP Adresse vergeben ist muss (must) er ein DHCPDECLINE an den Server senden und zumindest 10 Sekunden warten bis er den gesamten Prozess erneut startet

RFC should, could, may usw. <https://www.ietf.org/rfc/rfc2119.txt>

DHCP simple case



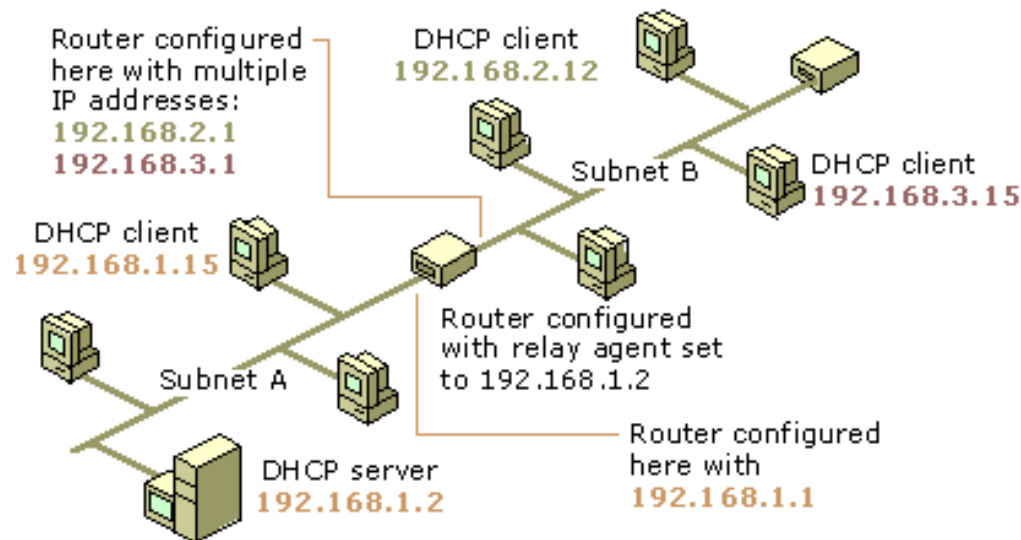
Single scope here configured as follows:

Scope 1: 192.168.1.1 - 192.168.1.254

Subnet mask: 255.255.255.0

Excluded addresses: 192.168.1.1 - 192.168.1.10

DHCP in einem gerouteten Netz



Scope for local Subnet A:

Scope 1: 192.168.1.1 - 192.168.1.254

Subnet mask: 255.255.255.0

Excluded addresses: 192.168.1.1 - 192.168.1.10

Superscope added here with member scopes for Subnet B:

Scope 2: 192.168.2.1 - 192.168.2.254

Scope 3: 192.168.3.1 - 192.168.3.254

Subnet mask: 255.255.255.0

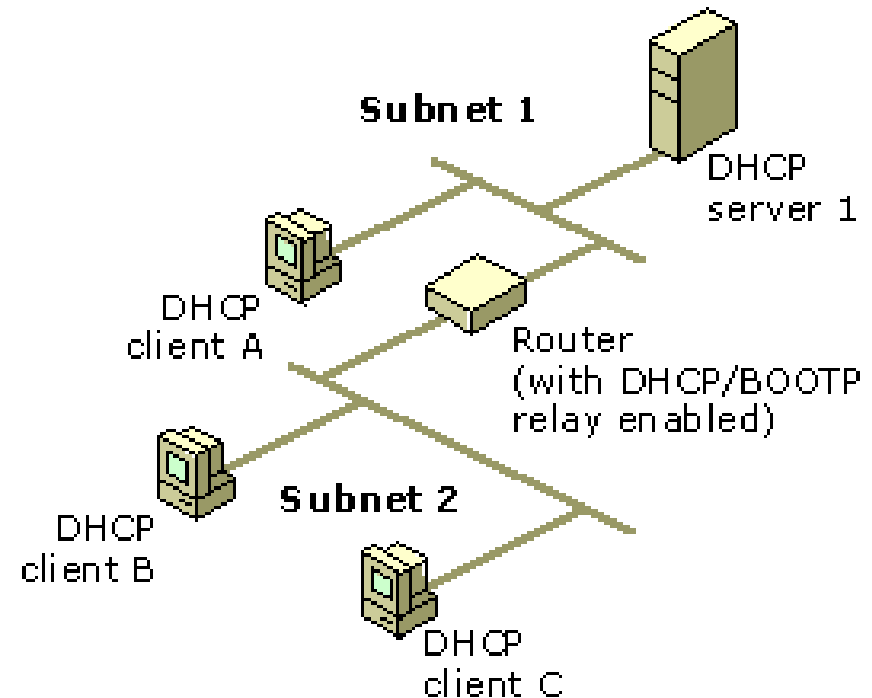
Excluded addresses:

(Scope 2) 192.168.2.1 - 192.168.2.10

(Scope 3) 192.168.3.1 - 192.168.3.10

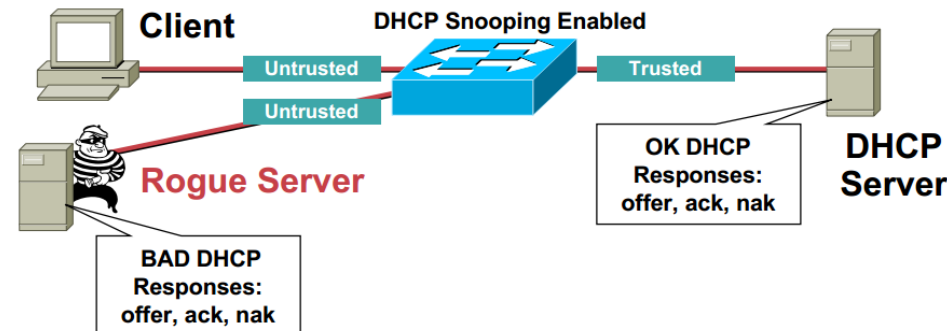
Relay Agent

1. Client C sendet DHCP Discover
2. Relayagent befüllt das Relayagentfield mit seiner IP Adresse
3. Relayagent sendet DHCP Discover an DHCP Server
4. DHCP Server erkennt an der Relayagent IP aus welchen IP Adressbereich er die IP Adresse vergeben kann



DHCP Angriffsmöglichkeiten

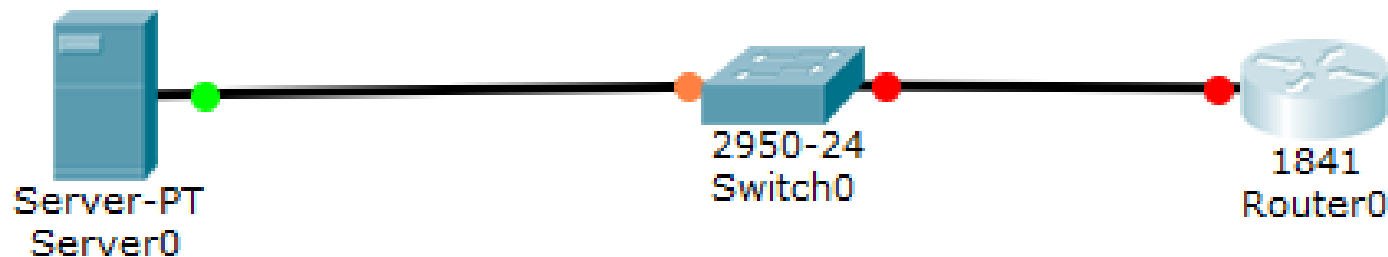
- DHCP Starvation Attack
 - Denial of Service Attack bei dem der IP Adresspool des Servers aufgebraucht wird
 - Gegenmaßnahme
 - Port Security am Switch
 - IDS/IPS
- Rogue DHCP Server Attack
 - Versuch eines DHCP Spoofing um selbst z.B. als Gateway zu fungieren
 - Gegenmaßnahme
 - DHCP Snooping
 - ACL am Switch
 - DHCPLOC



DHCPv6 Übung

DHCPv6 Übungsangabe

- Wir verwenden den Cisco Packet Tracer um einen DHCPv6 Server zu simulieren
- Domainname: mydomain.at
- Global IP Addressbereich: 2001:1234:5678::/64
- Wir platzieren Server, Router und Switch



IP Adressen Pool

- Zunächst konfigurieren wir den Router damit er IPv6 unicast Adressen routet

```
Router(config)#ipv6 unicast-routing
```

- Nun erstellen wir einen DHCP Adresspool

```
Router(config)#ipv6 dhcp pool mydomain
```

- Im Anschluss konfigurieren wir die Prefix Verteilung (inklusive maximale und erwünschte Lifetime), den Domainname und den DNS Server

```
Router(config-dhcp)#prefix-delegation pool mydomain lifetime 5400 3600
Router(config-dhcp)#domain-name mydomain.at
Router(config-dhcp)#dns-server 2001:1234:5678::5
```

Router Interface konfigurieren

- Nun legen definieren wir den Interface Teil der IPv6 Adresse

```
Router(config)#ipv6 local pool mydomain 2001:1234:5678::/40 64
```

- Wir konfigurieren am Router Interface eine IPv6 Adresse und linken den DHCPv6 Pool an dieses Interface

```
Router(config)#int fa 0/0
Router(config-if)#ipv6 address 2001:1234:5678::1/64
Router(config-if)#ipv6 dhcp server mydomain
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed s
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastE
up

Router(config-if)#exit
Router(config)#
```


DHCPv6 Test

- Wir erstellen einen Client, verbinden diesen mit dem Netz und sehen ob er eine IPv6 Adresse erhält

Gateway/DNS Ipv6

☒ DHCP
☐ Auto Config
☐ Static

IPv6 Gateway

IPv6 DNS Server

IPv6 Configuration

☒ DHCP
☐ Auto Config
☐ Static

IPv6 Address /

Link Local Address:

Quellen

- Kozierok, Charles M. “Welcome to The TCP/IP Guide!”, www.tcpipguide.com. Accessed 6 May 2020.