

1 Namensauflösung, DNS - Domain Name System

Die für Menschen notwendigen Namen müssen in IP Adressen umgewandelt werden. Dafür gibt es verschiedene Techniken. zB: eine Liste in einer Datei, DNS, WINS, LDAP, u.a.

1.1 Windows

1. Lokale Datei

? %SYSTEMROOT%\SYSTEM32\DRIVERS\ETC\HOSTS

o Liste IP und Namen

2. DNS/WINS-Server

? Zugewiesen per DHCP oder eingetragen in den Netzwerkeigenschaften

1.2 Unix/Linux

In Unix kann festgelegt werden in welcher Reihenfolge die Naming-Services verwendet werden sollen.

? /etc/nsswitch.conf

HOSTS: FILES DNS -> d.h 1. DATEI 2. DNS

Oder:

HOSTS: NIS FILES LDAP -> d.h.: 1. NIS 2. DATEI 3. LDAP

? /etc/resolv.conf - (ohne „e“)

nameserver <IP1> <IP2>

wobei IP2 nur zur Anwendung kommt wenn IP1 nicht erreichbar ist.

domain <meine.at> Die eigene Domain

search <deine.at> weitere Domains, mit denen alle nicht FQDNs erweitert werden.

1.3 FQDN

Das Ziel von DNS ist die Auflösung eines FQDN (Full Qualified Domain Name, Voll qualifizierter Domänenname) in eine IP-Adresse.

Besteht aus Host + Domänenteile

Beschreibt eindeutig einen Host im Internet

FQDN Bsp: www.sz-ybbs.ac.at . = Rootknoten

at. ... Top Level Domain - TLD

ac.at. ... Second Level Domain - SLD - Subdomain

sz-ybbs.ac.at. ... Third Level Domain - Subdomain
www ... Hostname

1.4 URL - Uniform Resource Locator

beschreibt eindeutig eine Ressource im Internet
z.B: HTML Page, Image, Textfile, Web Service,...

URL

<https://www.sz-ybbs.ac.at:80/schueler/index.php?id=32>

https: Protokoll
[www.sz-ybbs.ac.at](https://www.sz-ybbs.ac.at:80/schueler/index.php?id=32) FQDN
www Host
sz-ybbs Subdomain, Third Level Domain
ac Subdomain, Second Level Domain
at TLD, Top Level Domain
80 Port
schueler Directory
index.php File
id=32 Querystring, Parameter

1.5 Konzepte / Vorteile von DNS

- 1) Verteilte Verwaltung: jede Domäne wird vom Besitzer verwaltet
- 2) Global eindeutige Namen: FQDN weltweit eindeutig
- 3) einfach in der Anwendung: Namen statt IP merken
- 4) skalierbar, erweiterbar: Vorgehensweise ist bei großen und kleinen Systemen identisch
- 5) höchste Verfügbarkeit und Aktualität
- 6) optimiert auf minimalen Datentransfer

1.6 DNS Funktionen

Forward Lookup Anfrage
FQDN -> IP umwandeln
> nslookup www.sz-ybbs.ac.at
85.255.155.147

Reverse Lookup
IP -> FQDN umwandeln
> nslookup 85.255.155.147
www.sz-ybbs.ac.at

Mailserver ermitteln (MX Mailexchanger)

IP des Mailservers einer Domain

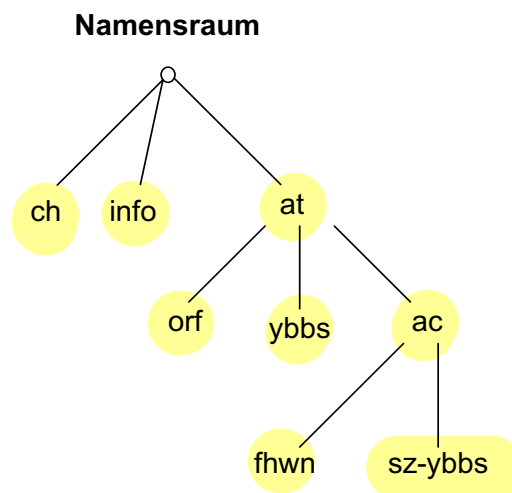
> nslookup

> set type=mx

> sz-ybbs.ac.at

Es wird nur die Domain eingegeben, Ergebnis sind die Hostnamen aller MX

1.7 Namensraum



TLD Top Level Domain

Erster Teil einer FQDN (rechts beginnend) - oberste Ebene im DNS Baum

at de com info biz ...

Subdomain

alle Domains unter einer TLD

Second Level Domain ac facebook

Third Level Domain sz-ybbs

Aufbau von DNS

- ? Baumstruktur
- ? verteilt (geographisch), hierarchisch
- ? gesamter DNS = DNS Namensraum (Namespace)
- ? Daten in DNS werden in Zonen gespeichert

Name FW Zonen

sz-ybbs.local.

sz-ybbs.ac.at.

Name RV Zonen: zur Auflösung von IP in FQDNs

1.168.192.in-addr.arpa

NetzId umgedreht

z.B. 192.168.1.X -> 1.168.192.in-addr.arpa

Ports:

53 UDP

Für DNS – Anfragen

53 TCP

Für den Zonentransfer

1.8 Komponenten

- ? **Namensserver:** Man unterscheidet zwischen primären (einem) und sekundären (beliebig vielen) Nameservern
- ? **Resolver:** Jener Teil des Betriebssystems, der von den einzelnen Applikationen (zB ping, telnet, Browse, ...) über einen Funktionsaufruf angesprochen wird und daraus die DNS-Anfrage an den ihm zugeteilten DNS Server erzeugt. Das Ergebnis wird wieder an die Anwendung zurückgeliefert.
- ? **Tools(zur Fehlersuche, Kontrolle):** „nslookup“, „dig“, „host“, (ping, traceroute) ...

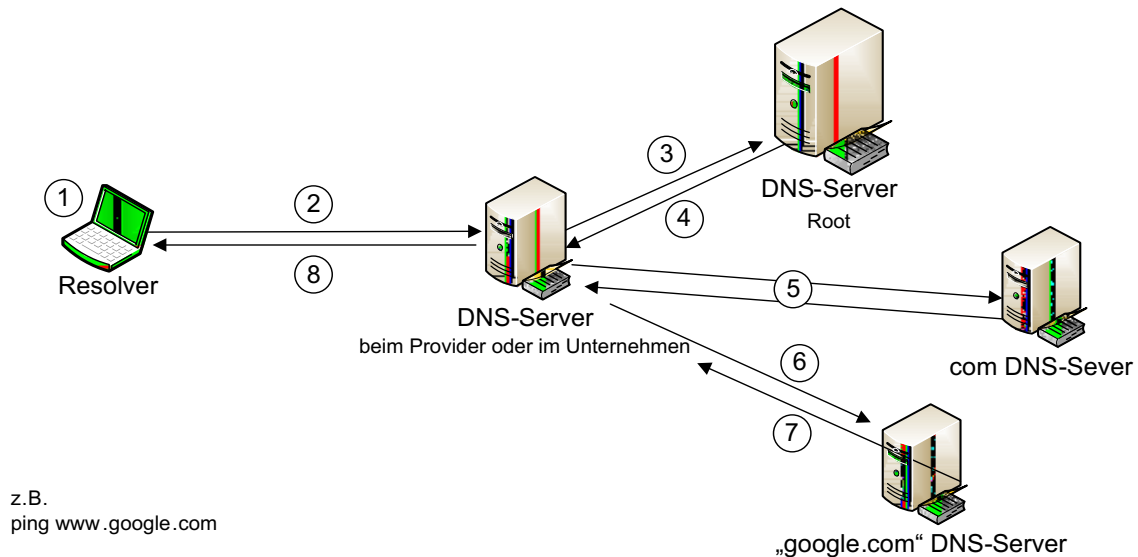
Achtung: DNS-Anfragen + Ergebnisse werden an verschiedenen Stellen gecached und können daher veraltet sein.

Übung:

1. Wie viele und welche nicht länderspezifischen TLDs gibt es?
2. Was sollte eigentlich unter .tt, .cc, .ag, .net und .tv zu finden sein?
3. Unter welchen 5 TLDs sind die billigsten Domains zu bekommen? Preis?
4. Mit welchen Kosten ist für eine .com und .at Domain zu rechnen?
 - a. .at 36€ pro Jahr
5. Wieviel kostet ca. ein Webhostingpaket?

1.9 Funktionsweise

Funktionsweise



1. Applikation übergibt die Anfrage an den Resolver, dieser durchsucht die HOSTS-Datei. Falls dort kein passender Eintrag vorhanden ist erzeugt es eine DNS-Anfrage an den zugeordneten DHCP-oder DNS-Server
2. Anfrage an den lokalen DNS-Server (im Unternehmen oder beim Provider)
3. Beginnend bei der Top-Level Domäne wird nun versucht den zuständigen Namensserver zu finden, jeder DNS-Server hat die Liste der root-DNS-Server (13 Stück) eingetragen. Die root-DNS-Server haben ausschließlich nur die Adressen der Top-Level-Domain DNS-Server eingetragen.
4. Der Root-DNS-Server kann den Namen nicht auflösen, aber er liefert die Adressen des Nameservers für die com-Domäne.
5. Ähnliches: Die Anfrage an den com Server liefert wiederum nur die Adresse des google-Namensserver
6. Erst die Anfrage für den google.com zuständigen DNS-Server liefert eine brauchbare Antwort, welche im Schritt 8 vom lokalen DNS-Server an den Client geliefert wird. Der Resolver kann nun die IP-Adresse dem ping-Befehl liefern

Im Normalbetrieb entfallen viele dieser Anfragen da sie bereits im Cache vorhanden sind.

1.10 DNS Record Typen

A ... Address
Beispiel:

FTP.BMW.DE	IN	A	193.73.81.13
↓	↓	↘	↘
FQDN	Class	Recordtyp	IP

AAAA ... IPv6 Adresse

FTP.BMW.DE IN AAAA ac1d:3fec:3fac:1234:6789:abcd:efab:0347

↓ ↓ ↘ ↓

FQDN Class Recordtyp IP

? **NS** ... Name Server

BMW.DE IN NS SRV17.HE.DE

↓ ↓ ↘ ↘

Domain Class Recordtyp Zuständiger DNS-Server

? **CNAME** ... Canonical=Alias

www.ybbs.at IN CNAME www17.aon.at

? **TXT** ... Text wird verwendet für Kommentare

bmw.de IN TXT Domain gesperrt

? **MX** ... Mail Exchange

bmw.de IN MX 20 SERVER17.GMX.DE

↑ ↑ ↑

Domäne Prior. (niedrigster zuerst) Mailserver

? **SRV** ... Server für bestimmten Dienst

....

? **PTR** ... Reverse Lookup

1.0.168.192.IN-ADDR.ARPA. IN PTR MAIL.SZ-YBBS.AC.AT

Bzw. bei IPv6

b.a.9.8.7.6.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa. IN PTR test.ybbs.at.

Übung: Finde deine offizielle IP heraus und dazu deinen Reverse Namen.

? SOA ... Start of Authority

enthält Verwaltungsdaten einer DNS Zone

bmw.de	IN	SOA	poseidon.bmw.de.	admin.poseidon.	(20071001 ; serial
↑			↑	↑	36000 ; refresh
Domäne			Prim. DNS-SRV	EMAIL des Admin	1800 ; retry
				erster „.“ entspricht @	36000 ; expire
					86400) ; time to live

serial Fortlaufende Nummer die mit jeder Änderung erhöht werden muss.
(Üblich: Datum + 2 Ziffern) Anhand dieser Nummer erkennen die sekundären Server, ob sie ein Update durchführen müssen.

refresh Kontrolliert die Abstände der Überprüfung der Aktualität zwischen primary und secondary (in Sekunden)

retry Wenn eine Verbindung zum primary nicht hergestellt werden konnte probiert er nach der Retry-Zeit die Verbindung noch einmal aufzubauen.

expire Lebensdauer der Daten im secondary wenn keine Verbindung zum primary hergestellt werden kann.

ttl Zeit wie lange ein anderer Nameserver die aus dieser Zone gelernten Daten im Cache behalten soll.

Die Secondary Server brauchen diese Einträge zum Abgleichen mit dem Primary (Timer, ...)

1.11 DNS Root Server

Zum Auflösen der TLDs existieren weltweit verteilt 13 aktive ROOT DNS

Standorte: 10x USA, 1x Schweden, 1x UK, 1x Japan

1.12 Ausfallsicherheit von DNS-Servern

Um Redundanz innerhalb einer DNS-Zone zu erreichen, können beliebig viele autoritative (zuständige) Namensserver konfiguriert werden. Dabei gibt es immer einen Master (Primary), alle weiteren werden als Slave (Secondary) konfiguriert. Alle Änderungen (in der Zonendatei) werden ausschließlich am Master ausgeführt. Die Slaves (Secondary) fragen periodisch im Zeitintervall (laut Zeitintervall refresh im SOA) den Master nach der aktuellen

Seriennummer. Ist diese größer als die eigene, so wird ein Zonentransfer (TCP) durchgeführt.

1.13 Unterschied zwischen Domäne und Zone

Eine Zone besteht aus mindestens einer Domäne (meist ausschließlich). Eine Zone kann jedoch auch eine oder mehrere (muss aber nicht alle) Subdomänen dieser Zone enthalten.

zB: bmx.at Zone enthält auch Einträge von der Subdomäne „intern“.

bmx.at.	IN SOA ...
www.bmx.at.	IN A ...
www.intern.bmx.at.	IN A ...
kueche.intern.bmx.at.	IN A ...

Glue Record: Um einen NS Server einzutragen der für eine Domäne gültig ist in der er sich befindet, muss ein A-Eintrag für den NS Server in der übergeordneten Domäne eingetragen werden.

Bsp.: mzm.com. IN NS dns1.hansi.at. (ohne Probleme aufzulösen)
mzm.com. IN NS dns1.mzm.com. (geht nicht ohne weiteres, da sich der Namensserver in der gleichen Zone befindet)

Abhilfe:

In der (übergeordneten) Domäne .com

mzm.com. IN NS dns1.mzm.com.

dns1.mzm.com. IN A 208.12.234.33 <-Glue Record

1.14 Zonenreplikation


Datenabgleich zw. 2 DNS Servern

Daten werden vom primären DNS Server auf einen / mehrere sekundäre DNS Server übertragen.

Für eine offizielle Domäne (im Internet) werden mindestens 2 DNS Server benötigt.

- vollständiger Zonentransfer: komplette Übertragung der Zone
- inkrementeller Zonentranfer: nur Änderungen werden übertragen

1.15 Werkzeuge

 ping <NAME>

Ping verwendet den Resolver mit den **aktuellen** Einstellungen des Betriebssystems.

- ? **nslookup <Aufzulösender_Name> [anderer_DNS-Srv]**
- ? **nslookup** -> Interaktiver Modus

Wird kein Server angegeben, erfolgt die Auflösung über den Server aus den Betriebssystemeinstellungen (DHCP oder /etc/resolv.conf)

server <anderer DNS-Srv> Alle darauf folgenden Befehle werden an **diesen** Server geschickt.
Vorsicht: Manche Firewalls erlauben keine DNS-Zugriffe nach außen

nslookup liefert standardmäßig nur A-Records, außer:

set type=<Recordtyp>| any Liefert den gewünschten Record Typ, bzw. Einträge aller Typen

z.B.

set type=any
sz-ybbs.ac.at. ? (SOA, Alle: MX's, A's, NS's)

- ? **dig [<Host/Domain>] [-t <typ>] [@<DNS-Server>]**
z.B. dig sz-ybbs.ac.at -t any @dns1.aon.at

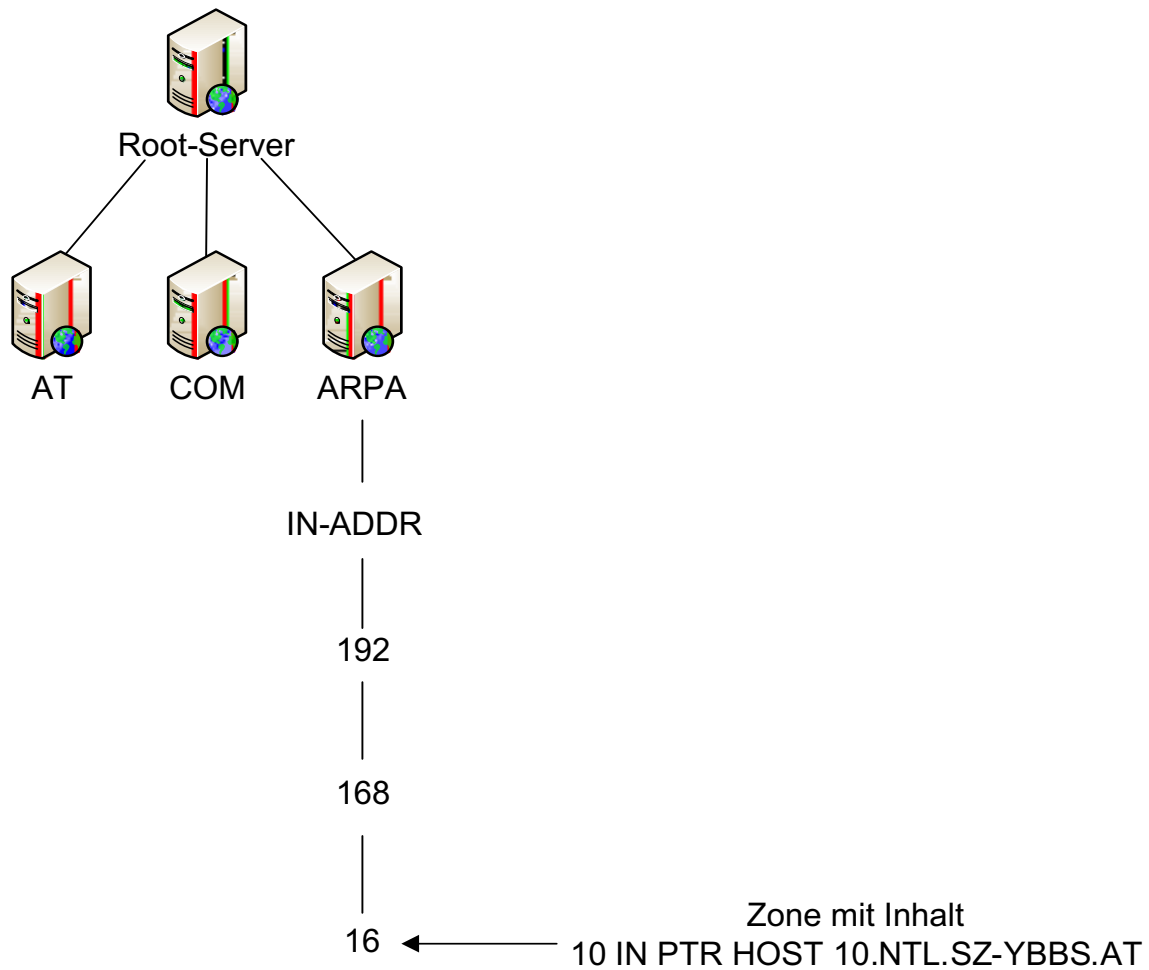
1.16 Reverse-DNS

Dient dazu IP-Adressen in Domain-Namen aufzulösen

Anwendung:

- ? **traceroute**
 - ? um dem Benutzer zusätzliche Informationen über die Route anzubieten
- ? **FTP und SMTP Server**
 - ? wird gelegentlich als Sicherheitsüberprüfung geprüft ob Vorwärts und Reverse – Auflösung übereinstimmen
- ? Um dem Anwender nicht nur die IP sondern bei Verfügbarkeit gleich den (Reverse-) Namen zu zeigen
- ? **netstat -a** (aber OHNE -n)

Reverse – DNS



Beachte: Es besteht keine Notwendigkeit, dass ein Reverse-Eintrag zu einem Forward Eintrag existieren **muss**, noch die Notwendigkeit das diese **zusammenpassen** müssen.

Frage: Wieviele PTR , SOA, A, NS Record gibt es in den verschiedenen Ebenen?

IP-Adresse: 192.168.16.6
NTL.SZ-YBSS.AT

Reverse-Domäne
16.168.192.IN-ADDR.ARPA

Test-Fragen: Kann ich in der Domäne 16.168.192.IN-ADDR.ARPA alles anzeigen?

Antwort: Nein weil ich immer nur einen Domänenname in eine IP-Adresse auflösen kann bzw. eine IP-Adresse in einen Domänennamen. Daher müsste ich um zu sehen was in dieser Sub-Domäne an Pointer ist alle Möglichkeiten durchprobieren um zu sehen was darin ist da ich immer nur einen FQDN auflösen kann.

Bei Reverse-Lookup Zonen ist die kleinste zu verwaltende Einheit ein Klasse C Netz!

d.h. Die Reverse Einträge befinden sich meist am NS des Providers da viele Unternehmen kein ganzes Klasse C Netz von offiziellen IP-Adressen besitzt.

Daher wird die Reverse-Lookupzone meist vom Provider administriert, wenn der Kunde nicht n x 256 offiziellen IPs hat.

1.17 Dynamische Updates

Will ein Administrator mit häufig wechselnden Hosts (zB bei Verwendung von DHCP) nicht ständig sein Zonendaten anpassen, so kann er dynamische Updates aktivieren. Dabei registrieren sich die Clients (oder der DHCP Server) per DNS-Request am (Master-)Server. Das ist zwar recht praktisch, aber sicherheitstechnisch problematisch. Zumindest eine Accessliste sollte beschränken wer Requests senden darf.
Besser: Request mit Signatur (TSIG)

1.18 DDNS Server (*Dyndns, easydns, no-ip,...*)

Wird verwendet um Rechner mit wechselnder IP (Provider vergibt diese bei jedem Verbindungsaufbau neu) auch permanent unter einem Namen erreichbar zumachen.

Funktion:

Eine Clientsoftware (z.B. in Windows, teilweise auch in ADSL-Modems implementiert) schickt periodisch (oder zumind. kurz nach jedem Verbindungsaufbau) die Benutzerkennung an einen Server. Dieser trägt die Absender IP in die Zone des Kunden ein und liefert bei allen darauffolgenden DNS Anfragen zur dieser Zone bereits die neue IP.

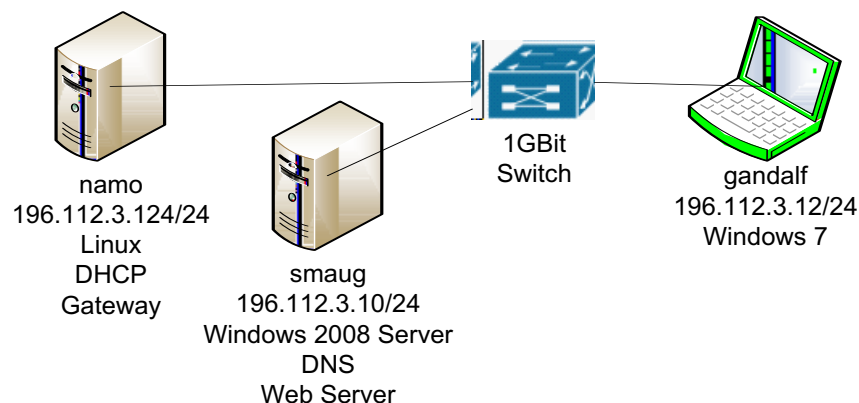
DynDNS (u.dgl.) verwendet nach außen das Standard DNS Protokoll.

DNS

Sie werden von der Firma Oscar Bruch & Sohn (Achterbahnbetreiber) beauftragt, das interne Netzwerk so abzuändern, dass alle Rechner per FQDN anstatt wie bisher über die IP Adresse angesprochen werden können.

Anforderungen

Das Netzwerk besteht aus einem Linux und Windows Server, sowie mehreren Workstations. Es sollen alle Server mit ihrem FQDN angesprochen werden können. Zusätzlich sollen der Mail-Server über mail und der Projekte-Server über project erreicht werden können. Der Mail-Server wird auf namo und der Projekte-Server auf smaug gehostet.



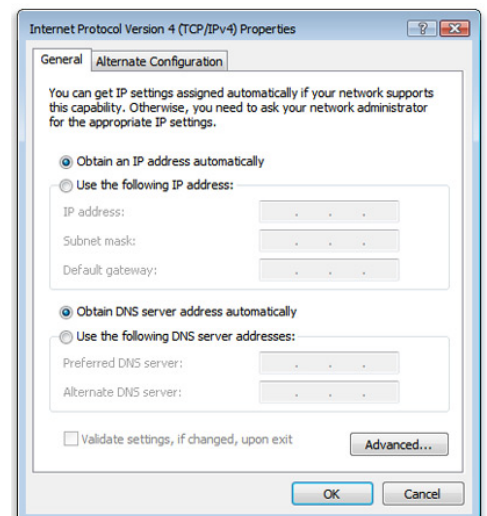
- ? Erklären Sie dem Kunden welche Lösungsmöglichkeiten es gibt.
- ? Schlagen Sie die optimale Lösung vor und begründen Sie diese.
- ? Der Kunde möchte wissen, wie bei DNS eine FQDN in eine IP Adresse umgewandelt wird.

Umsetzung

- ? Legen Sie den Namen der Forward und Reverse Zone fest.
- ? Erstellen Sie alle notwendigen Einträge für den DNS Server (Forward / Reverse)
- ? Legen Sie für eine Workstation die IP Konfiguration fest (ohne DHCP)

Test

- ? Ermitteln Sie die eingestellte IP Konfiguration sowie den DNS über die CMD.
- ? Testen Sie jeweils 2 Forward / Reverse Lookups.
- ? Ermitteln Sie den Mail-Server.
- ? Zeigen Sie die Liste aller DNS Einträge an.



Übung:

a) 1. Möglichkeit: man verwendet lokale Dateien

2. Möglichkeit: man verwendet einen DNS-Server

b) Die zweite Möglichkeit ist besser.

Da bei der ersten Möglichkeit auf jedem Netzwerkdevice die File einzeln geändert werden muss.
Dies muss dann auch bei Updates gemacht werden, (sehr zeitaufwendig, großes Fehlerpotential)

c) Dies wird mit einer Forward Lookup Anfrage gemacht welche an den DNS^{Server} gesendet wird. Der DNS-Server sendet falls er den gesuchten Eintrag besitzt eine Antwort. Falls nicht wird die Anfrage an den nächst höheren DNS-Server gesendet. (wird wiederholt bis der Eintrag gefunden wurde oder es keine höheren DNS-Server mehr gibt)

DHCP - Dynamic Host Configuration Protocol

Motivation

- Zeitersparnis / zentrale Verwaltung
 - bei großen Netzwerken manuelle Konfig. sehr zeitintensiv
- Konfigurationserleichterung, für User/Admins sehr einfach einzusetzen
- Überbuchung: mehr Clients im Netzwerk betreiben, als IP Adressen verfügbar (nicht gleichzeitig -> hintereinander)
- Zuweisung einer **NW-Konfig** an Clients durch DHCP Server
 - IP
 - Subnet
 - Gtw / Router
 - DNS Server
 - Leasetime – Zeitdauer, in der die NW-Konfig. Gültig ist

Bei DHCP werden 3 Varianten der Zuordnung unterschieden:

Manuelle Zuordnung

- am DHCP Server werden IP Adressen fix auf bestimmte MAC Adressen zugewiesen
- Zuweisung auf **unbestimmte Zeit**
z.B. Drucker, (Server eher statische IP (fix eingestellte IP am Server direkt))
NT: relativ hoher Verwaltungsaufwand (für jedes Geräte MAC Adresse bekannt und im Server eintragen)

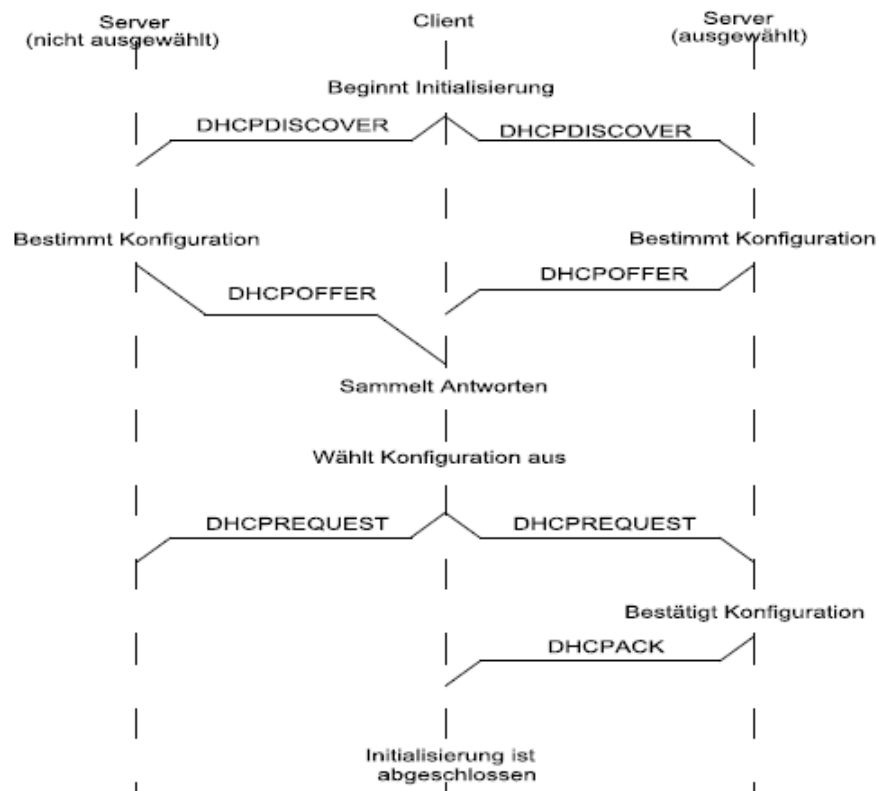
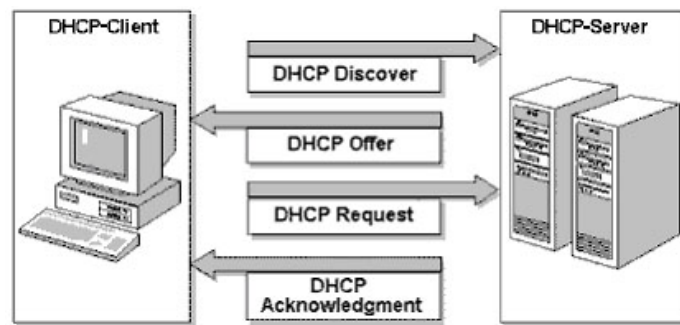
Automatische Zuordnung

- am Server wird ein Bereich von IPs festgelegt, diese werden automatisch an neue Clients vergeben
- Zuweisung wird gespeichert, auf **unbestimmte Zeit**
- **selten verwendet**
- NT: wenn Bereich vollständig vergeben ist, keine neuen Clients mehr möglich

Dynamische Zuordnung

- am Server wird ein Bereich von IPs festgelegt, werden automatisch an Clients vergeben
- am Server wird eine **max. Gültigkeitsdauer festgelegt (Leasetime)**
- spätestens nach Ende Leasetime muss der Client neu anfordern (oder zurück geben)
- VT: geringer Verwaltungswand (Bereich einrichten, Clients auf dyn IP), Überbuchung möglich

Ablauf der Kommunikation



alle 4 DHCP Messages sind BC

Src

- Client: 0.0.0.0
- DHCP Server: IP vom Server

Dest

- 255.255.255.255

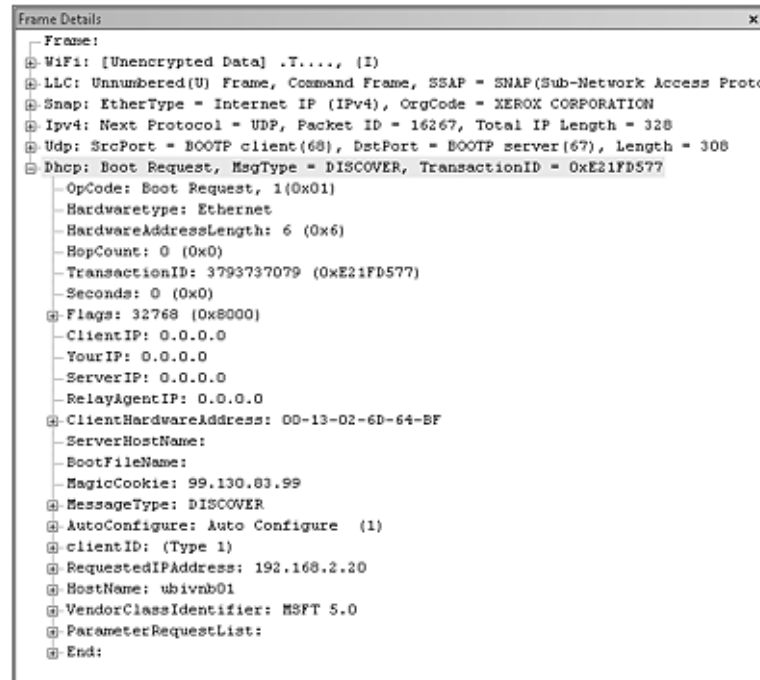
Erst nach dem DHCPACK kann die Netzwerkkonfiguration aktiviert werden und der Client kann **Unicast Messages** senden/empfangen

bei mehreren DHCP Offers

- Client kann auswählen
- nicht gewählter DHCP Server -> erkennt Absage in DHCPRequest Message am Inhalt (nicht sein Angebot)

DHCPDiscover

- Anfrage eines Clients an alle verfügbaren DHCP Server über eine freie IP Adresse
- alle verfügbaren DHCP Server = alle Server in der BC-Domain (Routergrenze)



DHCPOffer

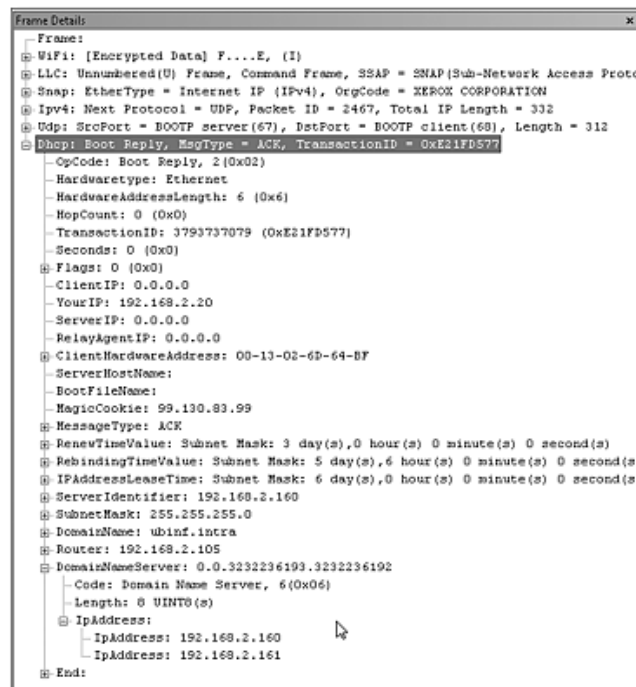
- Antwort eines DHCP Server mit einer IP / NW-Konfiguration
- IP Adresse
- Subnet
- IP DHCP Server
- IP DNS Server
- IP Gtw / Router
- Leasetime

DHCPRequest

- Client fordert eine angebotene IP Adresse an, Inhalt im Request ist auch die angeforderte IP Adresse
- nicht gewählte DHCP erkennt es als Absage

DHCPAck - Acknowledge

- Bestätigung vom DHCP Server über die gewählte IP Adresse



DHCP Optionen

- Einstellungen, die an den Client übermittelt werden

- IP Adresse 050
- Subnet 001
- Gtw / Router 003
- DNS Server 006
- Domain Name 015
- Leasetime 051

DHCP Bereich

- fortlaufender Bereich von IP Adressen, die per DHCP vergeben werden dürfen
- ein Server kann mehrere Bereiche verwalten

DHCP Ausschlussbereich

- Bereich von IP Adresse / einzelne Adresse, die von der Vergabe ausgeschlossen sind
- Bsp: Router, Server, ...

MAC Reservierung

- fixe Zuordnung einer IP Adresse auf eine bestimmte MAC Adresse
- Bsp: Drucker, (Server), (Router)

Lease (= komplette NW Konfiguration)

- vergebene NW-Konfiguration an einen Client
- die Lease enthält die **Leasetime = max. Gültigkeitsdauer der Zuordnung**

Adresspool

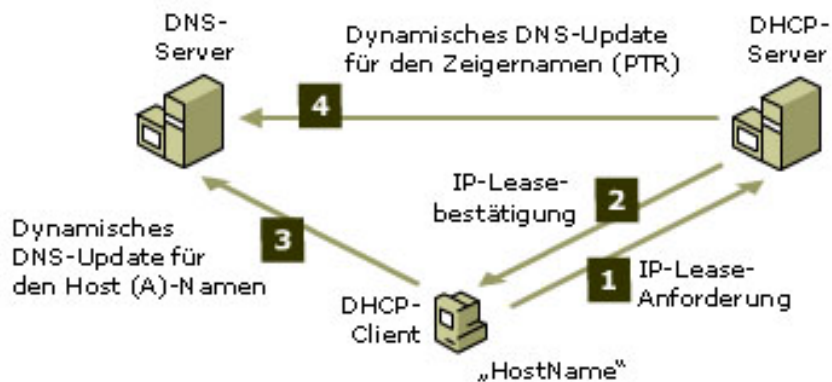
- alle zu einem **bestimmten Zeitpunkt** verfügbaren IP Adressen
- Adresspool = IP Bereich

- vergebene IP Adressen
- Reservierungen
- Ausschlussbereiche

DHCP Relay Agent

- DHCP Messages = BC --> Grenze für BC ist Router
- Anforderung: mehrere Subnetze mit einem DHCP Server versorgen
- > auf Router(n) DHCP Relay Agent aktivieren --> nur **DHCP BC** werden über Router weitergeleitet --> erste Router ergänzt IP Adresse im IP Header vom empfangenden Interface
- > ein DHCP Server soll ein komplettes NW (geteilt in Segmente) verwalten

Dynamische Updates (DNS / DHCP) = Option 81



1. The client initiates a DHCP request message (DHCPREQUEST) to the server and includes **DHCP option 81**. By default, the client requests that the DHCP server register the DNS PTR record, while the client registers its own DNS A record.
2. The server returns a DHCP acknowledgment message (DHCPACK) to the client, granting an IP address lease and including DHCP option 81. If the DHCP server is configured with the default settings (dynamically update DNS A and PTR records only if requested by the DHCP clients), then option 81 instructs the client that the DHCP server will register the DNS PTR record and the client will register the DNS A record.
3. Asynchronously, the client registers its DNS A record, and the DHCP server registers the DNS PTR record of the client.

DHCP Übung

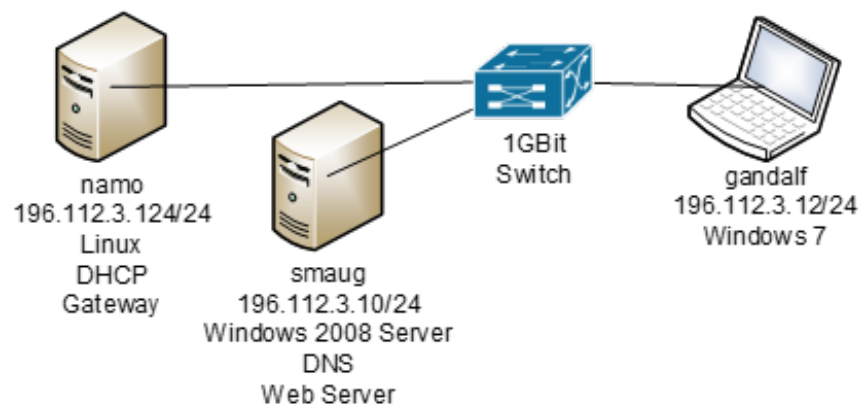
Sie werden von der Firma Oscar Bruch & Sohn (Achterbahnbetreiber) erneut beauftragt, das interne Netzwerk so abzuändern, dass die Netzwerkkonfiguration der Clients automatisch per DHCP zugewiesen wird.

Anforderungen

Das Netzwerk besteht aus einem Linux und Windows Server, sowie mehreren Workstations. Der **DHCP Server** wird auf **namo** gehostet. Alle Server sollen mit fix konfigurierten IP Adressen arbeiten.

Der **Router** ins Internet wird ebenfalls auf **namo** ausgeführt und der **DNS Server auf smaug**. Als **DNS Domainname** soll **bruch.de** verwendet werden.

Es gibt einen **Drucker**, welcher immer unter der gleichen **IP Adresse 196.112.3.100** erreicht werden soll



- ? Welche Möglichkeiten der Zuordnung gibt es bei DHCP?
- ? Entscheiden Sie, welche Zuordnungsart Sie für welche Geräte einsetzen würden?
- ? Erklären Sie dem Kunden, wie Sie es ermöglichen, statische und dynamische IP Adressen in einem Netzwerk kombinieren können?
- ? Der Kunde möchte die bereits durchgeführte DNS Konfiguration (alle Server + Workstations per FQDN erreichbar) auch weiterhin nutzen können. Erklären Sie ihm was zu tun ist?

Umsetzung

- ? Lege den DHCP Bereich inkl. Bereichsoptionen fest.
- ? Lege eine passende Leasetime fest.
- ? Lege die notwendige MAC Reservierung an.
- ? Was muss auf gandalf in der Netzwerkkonfiguration eingestellt werden?
- ? Was ist zu machen, um DNS + DHCP zu kombinieren?

Test

- ? Wie kann auf gandalf eine IP Adresse angefordert / freigegeben werden?
- ? Wie kann auf gandalf die Leasetime kontrolliert werden?
- ? Wo können auf namo die vergebenen IP Adressen kontrolliert werden?
- ? Sie führen zusätzlich einen Test mit Wireshark durch. Welche Messages/Reihenfolge werden Sie erhalten?