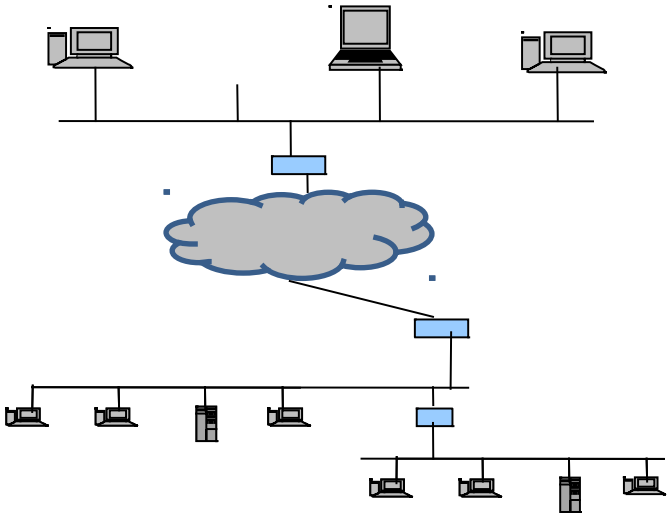


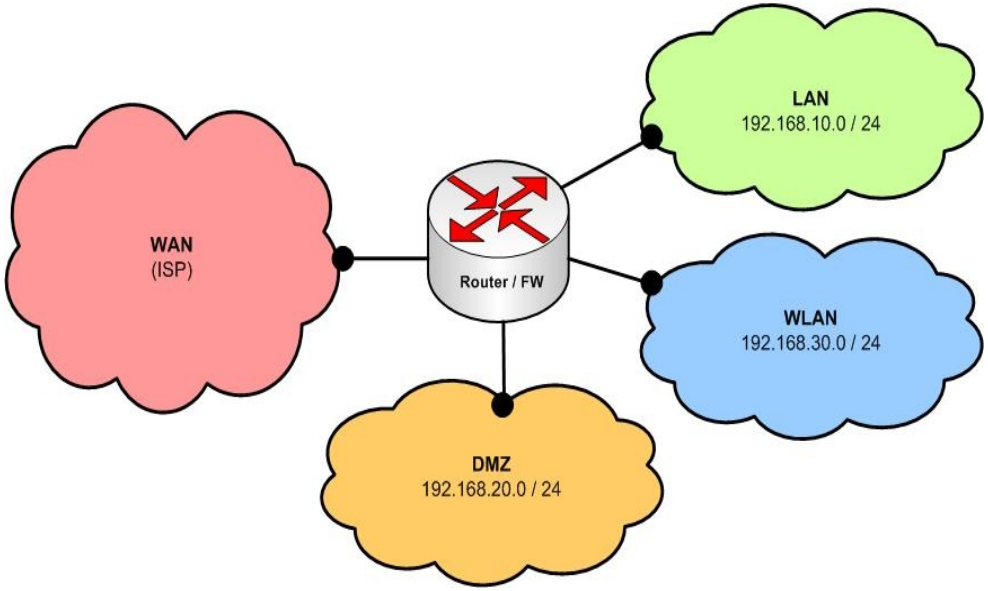
DHCP

DNS

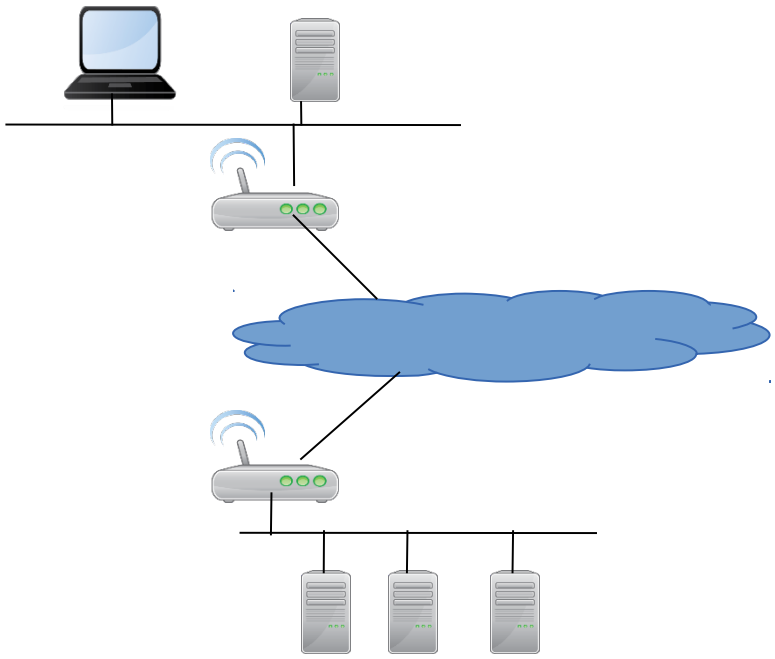
APACHE

MAIL

PROXY



http://www.tsbe.ch



DNS

1. Lokales Cache / hosts
2. Resolver (suffix) -> DNS
3. Anfrage an DNS

4. DNS – Cache
5. named.conf.local -> zuständig
6. db.tsbe.ch – Auflösung IP
7. forwarders – DNS

Apache

6. db.tsbe.ch Auflösung Web-Server
7. Anfrage an IP-Web-Server
8. DocumentRoot – Verzeichnis
9. index.htm

Kursziel

- Sie verstehen den Anwendungszweck und können die Softwarepakete installieren
- Sie können einen Dienst auf einfache Fehler prüfen und einfache Konfigurationsanpassungen vornehmen

Dynamic Host Configuration Protokoll (DHCP)

DHCP sollte eine Arbeitserleichterung für die Sysadmin darstellen.

Die Netzwerkbetreiber sind froh, wenn sie nicht einzelne Geräte in ein Netzwerk konfigurieren müssen.

Zuerst wurde durch eine Anfrage, welche ARP-Adresse bekommt welche IP ein erster Ansatz der heutigen Lösung umgesetzt. Die Angaben zum Routing waren damit aber noch nicht übertragen.

Also wurde ein Dienst ermittelt, welcher sich beim Start wie folgt verhält:

- IP-Adresse ermitteln
- Per Broadcast im Netz nach Parameter fragen
- IP-Konfiguration aufgrund der Parameter anpassen
- Bootfile- und Serverangaben für den Bootvorgang

DHCP ist abwärtskompatibel, damit ist sichergestellt, dass auch ältere Protokolle bedient werden können und wird durch die Internet **Engineering Taskforce** (IETF) standardisiert.

DHCP ist völlig unabhängig von der eingesetzten Plattform. Das heisst, es kann sowohl Windows-, Unix- oder Mac-Systeme mit den Netzwerkeinstellungen versorgen.

Um ein Mindestmass an Verfügbarkeitsanforderungen zu erfüllen, sollte natürlich mehr als nur ein DHCP-Server vorhanden sein, da sonst dessen Ausfall die Funktion sämtlicher Server und Clients beeinträchtigt.

Der Client hat eine physische Verbindung zum lokalen Netzwerk, selber aber noch keine IP-Adresse.

Daher schickt er eine DHCP-Anfrage in einem Paket an die Broadcastadresse im Netzwerk.

Mit der Anfrage über die Broadcastadresse ist sichergestellt, dass alle im Netz verbundenen Rechner diese Anfrage erhalten und der zuständige Server diese beantworten kann.

Das Paket mit der Anfrage wird über UDP an Port 67 gesendet, also an diejenige Adresse welche auch der Server verwendet.

Die erste Nachricht ist vom Typ **DHCPDISCOVER**. Der Client fragt so ohne Angabe einer eigenen Adresse. Die Menge der Informationen welche der Client erwartet ist flexibel, üblich ist:

- Eigene IP-Adresse
- Sunetmaske
- Defaultroute
- DNS-Server

Dem Client können nun **mehrere Server antworten**. Häufig sorgen DCHP-Server, die nicht deaktiviert wurden für Verwirrung da sie Clients mit alten Informationen beliefern.

Die Antworten nennt man **DHCPOFFER**. Der Client kann abwarten, ob mehrere Antworten eintreffen und aufgrund der eingetroffenen Parameter entscheiden, welcher „Offer“ er annimmt.

Um diese Adresse zugewiesen zu bekommen schickt der Client eine Nachricht vom Typ **DHCPREQUEST**. Das Paket wird nicht via Broadcast versendet, sonder an den Server, welche die Adresse angeboten hat.

Server quittiert die Adresszuweisung mit der Nachricht vom Typ **DHCPACK** in welcher die tatsächlich übermittelten Parameter sicherheitshalber noch einmal mitgeschickt werden.

Bei Erhalt der ACK-Nachricht sollte der Client überprüfen, ob die Adresse im Paket stimmt und mittels ARP-Request testen, ob die IP nicht schon existiert.

Wenn dies der Fall ist,teilt der Client dem Server den **Misserfolg** mit einem **DHCPDECLINE** mit.

Verweigert der Server die Zuteilung (als Antwort auf das Request-Paket), schickt er ein **DHCPNAK** (Not Acknowledged) statt eines ACK.

Bleiben die Anfragen des Clients unbeantwortet, probiert er es mit einem DHCPDISCOVER mehrere Male von Neuem.

Eine zugewiesene IP kann beim Herunterfahren des Clients mit einer **DHCPRELEASE-Nachricht** an den Server freigegeben werden und sie steht damit im Pool wieder zur Verfügung.

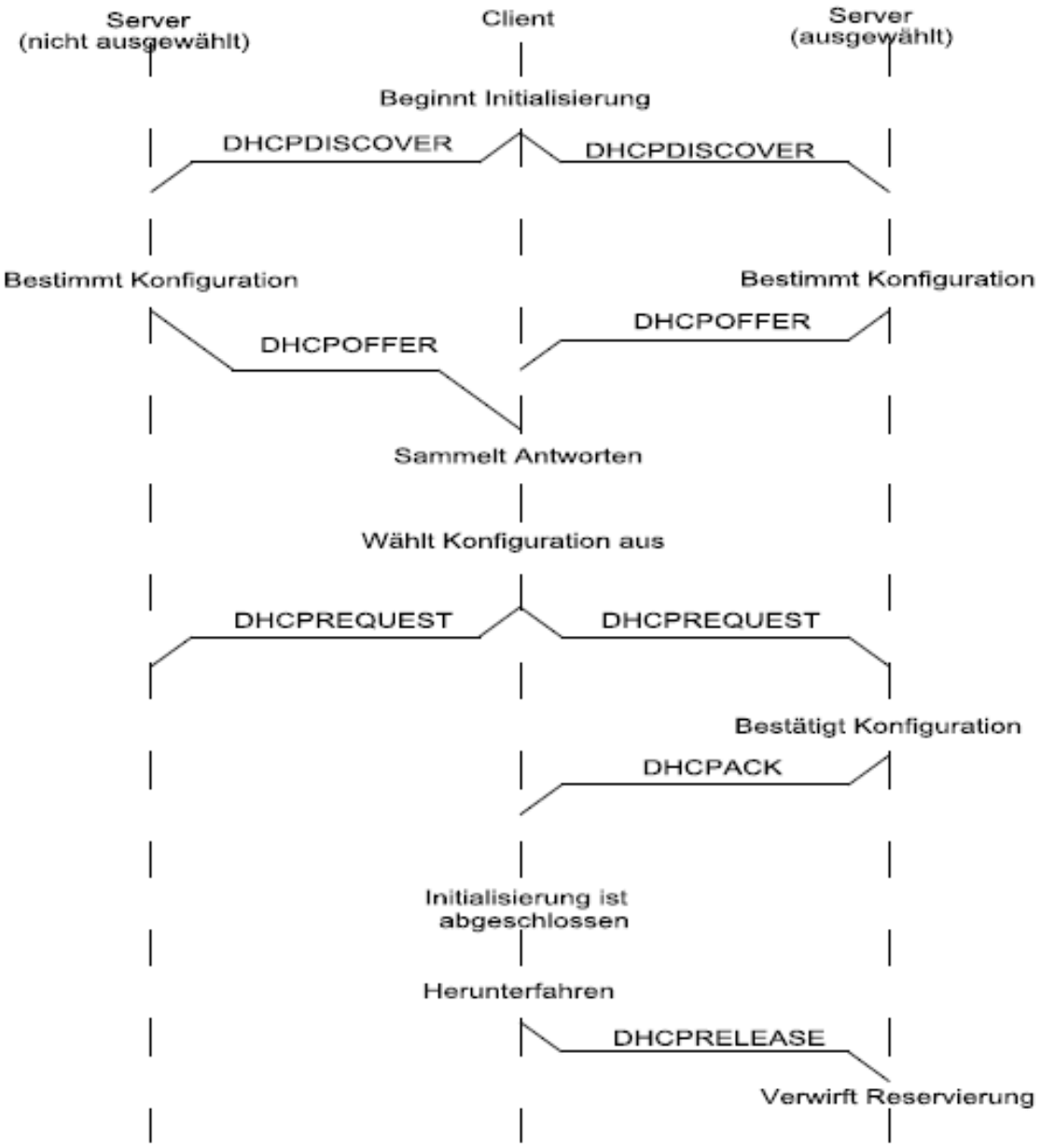
Jede zugewiesene Adresse wird mit einer Gültigkeitsdauer (Lease Time) versehen, die von der Konfiguration des DHCP-Servers abhängt. Ist diese verstrichen, finden die Verhandlungen erneut statt.

Wenn man nicht in jedes Subnetz einen eigenen DHCP-Server installieren möchte, bietet sich ein **DHCP Relay Agent** auf einem dazwischenliegenden Router an.

Damit kann ein DHCP-Server Clients in verschiedenen Netzwerken auch verschiedene Konfigurationen zuweisen.

Damit aber der Server nun weiss, aus welchem Netz die Anfrage kommt, muss diese bereits im DISCOVER , das eigentlich noch gar keine IP enthält, kenntlich gemacht werden. Dazu füllt der Relay Agent das giaddr-Feld im DHCP-Paket mit der IP des Interfaces.

DHCP
Verbindungs-aufbau



IPv6 - Verbindungsaufbau

Bei IPv6 benötigt die IP-Konfiguration eigentlich keinen DHCP-Dienst.
Dafür gibt es die Stateless Address Autoconfiguration (**SLAAC**). Mit SLAAC kann sich ein IPv6-Host vollautomatisch konfigurieren und die notwendigen IP-Konfiguration besorgen.
In der Praxis sind nicht alle Betriebssysteme dazu in der Lage

Weil bei DHCPv6 die IP-Konfiguration zentral vergeben und gespeichert wird, spricht man von "Stateful" Address Configuration.

In der Praxis sieht die IP-Autokonfiguration häufig so aus: Per Router-Advertisement werden die IP-Grundparameter verteilt und mit DHCPv6 alles weitere. Die Autokonfiguration bleibt dabei "stateless"

Der verwendete Hostname kann entweder vom Client gesendet oder vom DNS-Server vergeben werden.

DNS-Anbindung

Haben die Clients über den DHCP-Server eine Adresse bezogen, sind sie zunächst einmal über diese Adresse ansprechbar.

Um Clients aber auch mit dem einem im ganzen Netzwerk bekannten Namen anzusprechen, lässt sich der DHCP-Server mit einem Nameserver koppeln.

Nach der Zuweisung einer Adresse an einem Client werden die Adresse und ein Hostname auf dem DNS-Server eingetragen.

Der verwendete Hostname kann entweder vom Client gesendet oder vom DNS-Server vergeben werden.

Hochverfügbarkeit und Load Balancing
Theoretisch kann einfach ein zweiter Server mit identischer Konfiguration aufgesetzt werden.

Die Fehlersuche wird dadurch komplizierter. Sinnvoller ist die Ausfallsicherheit in Form einer synchronisierten und redundanten Konfiguration bei der die Server abgleichen wer welche Adressen vergibt.

Eine solche Konfiguration kann auch zum Load Balancing verwendet werden.

Netzwerkboot
Neben der IP-Konfiguration muss dem Client noch ein Dateiname übermittelt werden, der das zu bootende Betriebssystem oder einen ersten Teil davon enthält.

Das PXE (Preboot Execution Environment) von Intel ermöglicht, dass disklose Booten über das Netzwerk.

Die PXE-Spezifikation ermöglicht, dass über den DHCP-Server Daten für ein Auswahlmenu übermittelt werden. Somit kann der Benutzer auswählen, welches Betriebssystem er booten möchte.

DDNS

Funktionsweise
Das Geheimnis hinter DDNS ist die Kommunikation zwischen DHCP- und DNS-Server. Sobald sich ein Rechner im LAN meldet (mit einem DHCPDISCOVER), bekommt er nicht nur vom DHCP-Server eine IP-Adresse zugewiesen, sondern teilt ihm auch seinen Hostnamen mit.

Der DHCP-Server sagt diesen Hostname weiter an den DNS-Server, zusammen mit der IP-Adresse, die er ihm gegeben hat. Der DNS-Server erstellt daraus die Einträge zur Namens- und Reverse-Auflösung selbst.

Sicherheit
Aus Sicherheitsgründen muss ein Schlüssel erstellen werden, den der DHCP- und der DNS-Server nutzen, um die gegenseitige Kommunikation zu erlauben, was mit einem einfachen "shared secret key" funktioniert, also quasi einem Passwort, das beide Dienste kennen.

Einfache Konfiguration

```
#/etc/dhcpd.conf
#
authoritative;
#
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "mydomain.example";

subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.10 192.168.1.100;
range 192.168.1.150 192.168.1.200;
        host bla1 {
                hardware ethernet DD:GH:DF:E5:F7:D7;
                fixed-address 192.168.1.2;
        }
}
```