DHCP und NTP

Jörn Stuphorn
stuphorn@rvs.uni-bielefeld.de

Stand der Veranstaltung

13. April 2005	Unix-Umgebung
20. April 2005	Unix-Umgebung
27. April 2005	Unix-Umgebung
4. Mai 2005	ARP, ICMP, ping
11. Mai 2005	IP-Adressen & Subnetzmasken
18. Mai 2005	Einführung in Bridging, Routing, ...
25. Mai 2005	IOS, Spanning-Tree
1. Juni 2005	IOS Befehle, Brigding, Routing
8. Juni 2005	Statisches Routing
15. Juni 2005	UDP-, MTU- und IP-Fragmentierung
22. Juni 2005	TCP-Verbindungen und -Datenfluss
29. Juni 2005	***DHCP und NTP***
6. Juli 2005	*NAT und Firewalls*
13. Juli 2005	*Verschlüsselung, Vertraulichkeit, Authentisierung*
20. Juli 2005	*Sichere Anwendungen*

DHCP Aufgaben

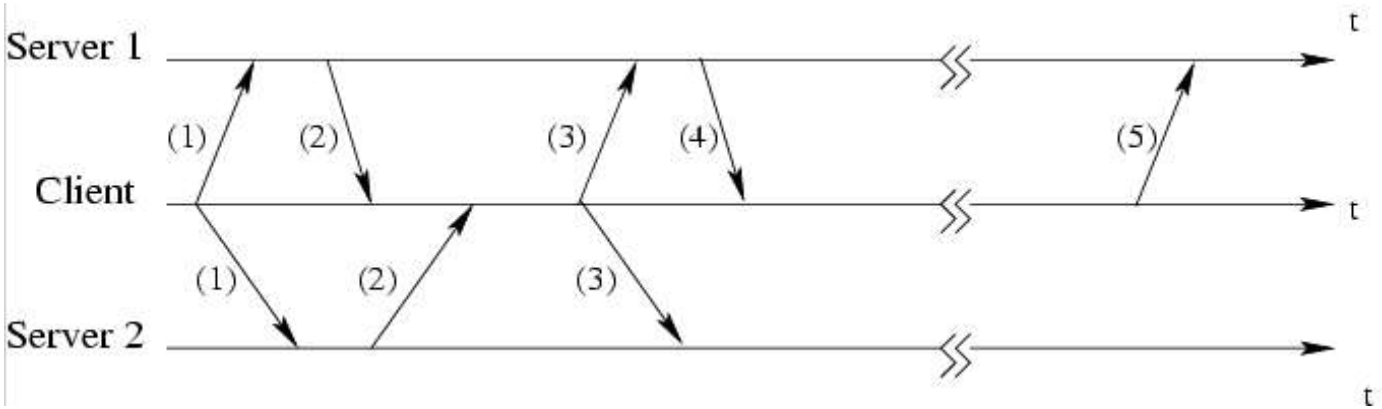
- Dynamic Host Configuration Protocol
- Ziel
  - Host dynamisch konfigurieren
  - von zentralem DHCP Server gesteuert
- DHCP Server bestimmt
  - IP Adresse
  - Subnetz Maske
  - Default Gateway Adresse
  - weitere Konfigurationsparameter
- DHCP Client fragt Server nach Parametern
- Server liefert Parameter in Antwort

DHCP Operationsvarianten

- Operationsvarianten:
  - Dauerhafte Speicherung von Netzparametern für Client
    - Client kann bei jedem Bootvorgang mit gleichen Parametern versehen werden
    - Server hält Key-Value Eintrag für jeden Client,
    - Eintrag wird zur Zuordnung von Client Anfragen verwendet
    - Bsp.: Subnetz-Adresse und MAC Adresse
  - Dynamische Zuweisung von Parametern
    - Server kann Parameter aus Pool vergeben
    - Bei Anfrage wird ungenutztes Parameterset zurück geliefert
    - Parameterset gilt nur für bestimmte Periode
    - Client muss Set regelmäßig aktualisieren oder es verfällt und kann vom Server neu vergeben werden.

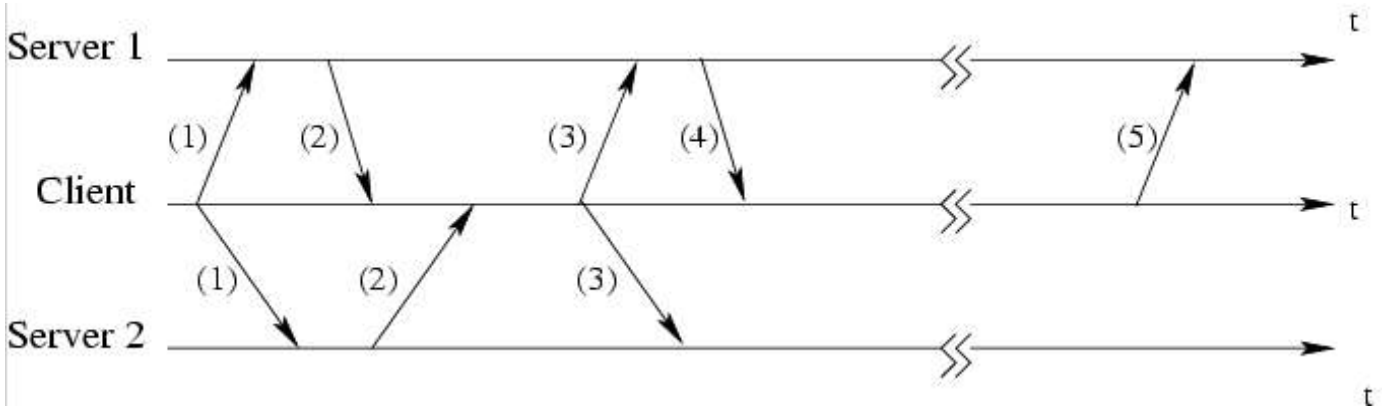
DHCP Operation

- Verwendung von mehreren (hier: 2) DHCP Servern
  - Client sendet DHCPDISCOVERY Message
    - Nachricht kann über Relays an entfernte Netzsegmente weitergeleitet werden
  - Jeder Server liefert DHCPOFFER Nachricht mit freier Netzadresse
  - Client empfängt mehrere DHCPOFFER Nachrichten
  - Client wählt einen Server anhand der angebotenen Parametern aus
  - Client sendet DHCPREQUEST mit Server ID um gewählten Server zu identifizieren

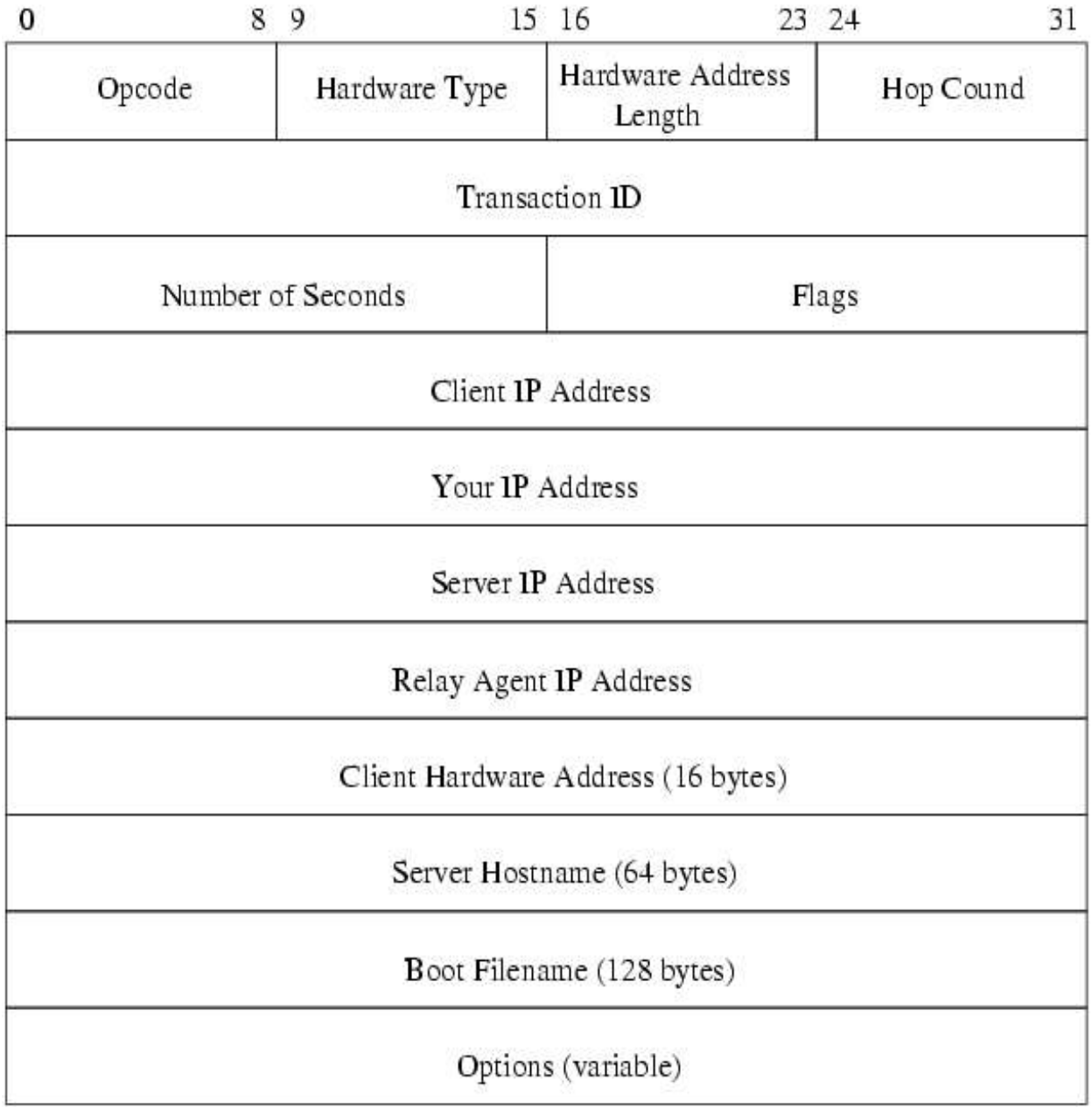


DHCP Operation

- Verwendung von mehreren (hier: 2) DHCP Servern
  - Server empfängt DHCPREQUEST Nachricht
  - Angesprochener Server reagiert mit DHCPACK Nachricht
    - DHCPACK Nachricht enthält vollständiges Parameterset
  - Client richtet sein TCP/IP Modul gemäß empfangener Parameter ein
  - Parameterset liefert Lease (Zeitspanne der Gültigkeit)
  - Läuft Lease ab (5) erneuert Client das Parameterset
  - Sonst verfällt Lease und Parameterset kann an anderen Host vergeben werden
  - Client kann DHCPRELEASE senden um Set freizugeben



DHCP Format


0
8
9
15
16
23
24
31
Opcode
Hardware Type
Hardware Address Length
Hop Cound
Transaction ID
Number of Seconds
Flags
Client IP Address
Your IP Address
Server IP Address
Relay Agent IP Address
Client Hardware Address (16 bytes)
Server Hostname (64 bytes)
Boot Filename (128 bytes)
Options (variable)

DHCP Felder

- Opcode
  - 1: Boot Request von Client
  - 2: Boot Antwort von Server
- Hardware Address Type
  - Gemäß „Assigned Numbers“ RFC: 1 für Ethernet MAC Adresse
- Hardware Address Length
  - Länge der Hardware Adresse
- Hop Count
  - optional, benötigt bei Verwendung von Relay Agents
  - Relay-Agent: Host oder Router, der DHCP Anfragen weiterleitet
- Transaction ID
  - zufällig vergeben
  - Zuordnung von Anfragen und Antworten zwischen Client&Server
- Number of Seconds
  - Vergangenen Zeit seit Client 1. Anfrage gesendet hat

DHCP Felder

- Flags
  - Broadcast Flag
    Client kann kein unicast Datagramm empfangen bevor Interface konfiguriert wurde
  - restliche 15 bit für „Future Use“ reserviert
- Client IP Address
  - Wenn Client in Bound, Renew oder Rebinding Zustand ist kann er auf ARP Anfragen antworten.
- Your IP Address
  - Von Server angebotene IP Adresse
- Server IP Address
  - IP Adresse des nächsten Servers, der verwendet werden soll (Bootstrap)
- Relay agent IP Address
  - IP Adresse des Relays (Bootstrap)

DHPC Felder

- Client Hardware Address
  - Die Hardware Adresse des Client
  - bei Ethernet:
    - Ersten 6 Byte werden gefüllt, restlichen Bytes auf 0 gesetzt
- Server Hostname
  - Name des DHCP Servers
- Boot Filename
  - Angabe des Vollqualifizierten Pfadnamens eines Files, der für Bootstrap verwendet werden soll.
- Options
  - optionale („vendor specific“) Felder

DHCP Konfiguration


```
1   # Sample /etc/dhcpd.conf
2   default-lease-time 600;
3   max-lease-time 7200;
4   option subnet-mask 255.255.255.0;
5   option broadcast-address 128.238.66.255;
6   option routers 128.238.66.1;
7   #option domain-name-servers 128.238.2.38, 128.238.3.21;
8   #option domain-name "poly.edu";
9
10  subnet 128.238.66.0 netmask 255.255.255.0 {
11      range 128.238.66.111 128.238.66.112;
12  }
13
14  host apah {
15      hardware ethernet 08:00:20:79:e9:9f;
16      fixed-address 128.238.66.110;
17  }
```

DHCP Übung

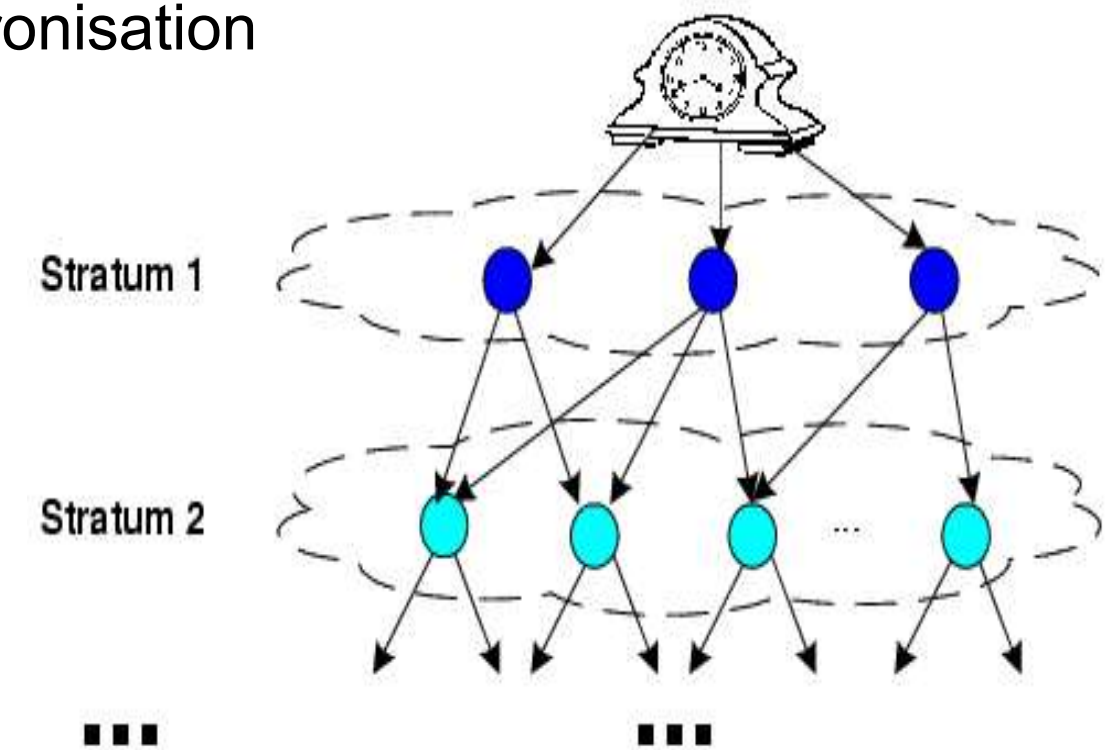
- Richte Server (yoda) gemäß Tabelle ein
- Starte DHCP Server im Vordergrund und im Debug Modus
  - /usr/sbin/dhcpd -d -f
- Protokolliere Traffic mit Ethereal
  - yoda & windu
- Stelle für windu Konfiguration des Interfaces über dhcp ein
- Starte Netzwerk auf windu neu
  - /etc/init.d/network restart
- Überprüfe Netzwerkkonfiguration von windu
  - ifconfig -a
  - netstat -rn
- Beschreibe anhand der Ausgabe, wie DHCP funktioniert
- sichere Ethereal Logfiles

NTP

- Exakte Zeitangabe ist wichtig für
  - Netzwerk Design
  - Netzwerk Management
  - Sicherheit
  - Diagnose
- NTP (Network Time Protocol)
  - Anwendungslayer (Layer 7) Protokoll, das
  - UDP oder TCP Port 123 verwendet
  - für akkurates Timing innerhalb des Netzes
  - Synchronisation von
    - Routern,
    - Hosts und
    - weiteren Netzwerkgeräten

Timing Service

- Organisiert in 16 Stratums
- NTP Primary Server (stratum-1) wird durch hochpräziser Uhr synchronisiert
- Über das Internet sind
  - über 300 stratum-1 Server und
  - über 175.000 Hosts mit NTP
- Jeder Server wählt einen oder mehr Server höheren stratums zur Synchronisation



Operations Modi

- Client und Server können in Multicast oder Broadcast Modus operieren
  - Timing Information wird von Server via multi- oder broadcast übertragen
  - Client kann „proaktiv“ Server nach Timing Information fragen
- NTP Client synchronisiert sich mit Server auf zwei Arten:
  - Anforderung von Timing Informationen von einem entfernten NTP Server zur Synchronisation
  - Synchronisation mit einem entfernten NTP Server kontinuierlich und automatisch

NTP Übung - 1

- Reboote Geräte um Originalzustand wieder herzustellen
- Kontrollier mit ***date*** die Uhreinstellung auf windu und yoda
- Probier die folgenden date Kommandos aus:
  - ***date --date='2 days ago'***
  - ***date --date='3 months 2 days'***
  - ***date --set='+3 minutes'***
  - ***date -r*** *file_name*
    file_name: irgendeine Datei im aktuellen Verzeichnis
- Welches Ergebnis liefern die Aufrufe?

NTP Übung - 2

- Protokolliere mit Ethereal den Traffic auf yoda und windu

- windu: rufe ***netdate -p*** yoda auf
- windu: rufe ***netdate -p -u*** yoda auf

- Welches Ergebnis liefern die Aufrufe?
  - Welche Portnummern wurden verwendet?
  - Wie viele Byte wurden vom Remote Timeserver gesendet (TCP und UDP)?
  - Welche TCP Headeroptionen wurden gesetzt?

NTP Übung - 3

- Überprüfe die */etc/ntp.conf* auf yoda und windu
- Passe ntp.conf gegebenenfalls an

- yoda:
  - Starte NTP Server mit */etc/init.d/ntpd start*
  - Kontrolliere Status mit */etc/init.d/ntpd status*

- Protokolliere mit Ethereal den Traffic auf yoda und windu

- windu:
  - Synchronisiere host mit yoda:
    ntpdate -d -v *yoda*

- Welche Ports benutzt der NTP Server?
- Wie sehen die Ausgaben von ntpdate und Ethereal aus?
- windu: rufe ***netdate -p*** yoda auf

NTP Übung - 4

- Lasse NTP Server auf yoda laufen
- Protokolliere mit Ethereal den Traffic auf yoda und windu
- windu: rufe ***/etc/init.d/ntpd start*** auf
- Warte einige Minuten
- Breche Protokollierung ab
- windu: rufe ***ntptrace*** auf um client/server Beziehung von NTP anzuzeigen
- Zeige das protokollierte NTP Paket an
- Mit welcher Rate wurden NTP Nachrichten gesendet?
- Zu welchem Stratum gehören windu und yoda?

DHCP Übung 2

- Richte Server (yoda) ein
- Richte Server (windu) ein

- Starte DHCP Server im Vordergrund und im Debug Modus
  - /usr/sbin/dhcpd -d -f
- Protokolliere Traffic mit Ethereal
  - yoda & windu

- Stelle für deinen Client Konfiguration des Interfaces über dhcp ein
- Starte Netzwerk auf deinem Client neu
  - /etc/init.d/network restart
- Überprüfe Netzwerkkonfiguration von deinem Client
  - ifconfig -a
  - netstat -rn

- Beschreibe anhand der Ausgabe, was passiert ist
- sichere Ethereal Logfiles