Webzugriff

Was passiert dabei im Detail?

Dirk Geschke

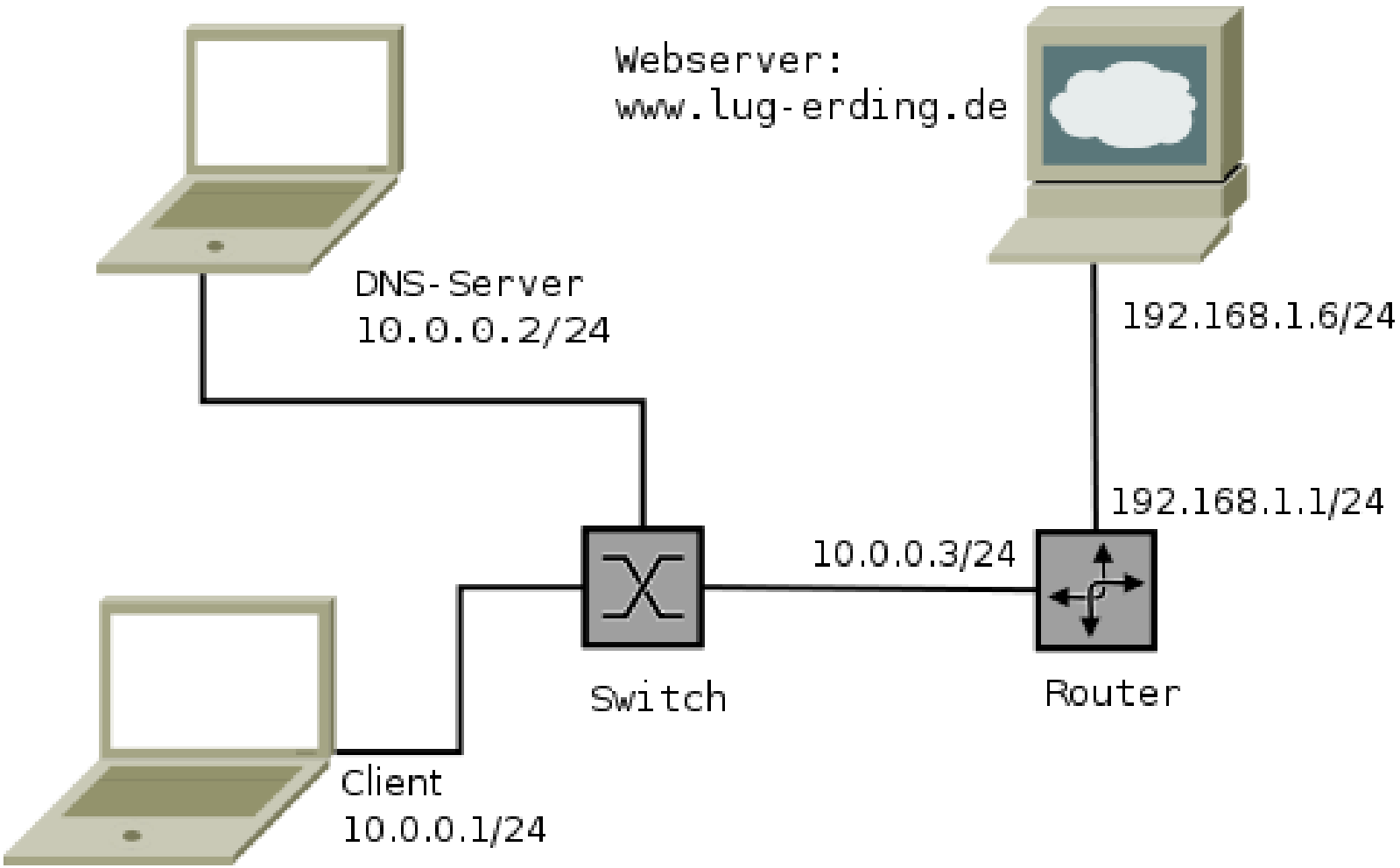
Linux User Group Erding

26. Januar 2011

Gliederung

Die Gliederung entfällt, wir wollen sie ja erarbeiten...

Testaufbau


Webserver:
www.lug-erding.de
DNS-Server
10.0.0.2/24
192.168.1.6/24
192.168.1.1/24
10.0.0.3/24
Switch
Router
Client
10.0.0.1/24

Zerlegen der URL

Als Beispiel-URL verwenden wir:

http://www.lug-erding.de/index.html

- Protokoll: HTTP, also TCP-Verbindung über Port 80 (*tcp* aus `/etc/protocols`, *www* aus `/etc/services`)
- Name des Servers: `www.lug-erding.de`
- Absoluter Pfad auf dem Server: `/index.html`
- Was kommt als nächstes?

Proxy finden

Es gibt mehre Möglichkeiten:

1. Keinen Proxy verwenden
2. Manuelle Proxy-Konfiguration
3. Automatische Proxy-Konfiguration via URL
4. Proxy-Einstellungen des Systems
5. Proxy-Einstellungen über das Netzwerk automatisch erkennen

Namensauflösung

- relevant ist `/etc/nsswitch.conf`
- Mögliche Werte für Namensauflösug "hosts":
  - `files` $\longrightarrow$ `/etc/hosts`
  - `dns` $\longrightarrow$ `/etc/resolv.conf`
  - `nis` oder `nisplus`
  - `ldap`
  - `mdns` (*avahid*)
- gewöhnlich: hosts: files dns
- Wichtig: Reihenfolge und *localhost* in `/etc/hosts`

Finden des DNS-Servers

Das finden, sofern ein DNS-Server verwendet wird, erfolgt in mehreren Schritten:

- Analyse der Routingtabelle
- ARP-Request für den Server oder den Router
- UDP-Paket an die IP-Adresse des Servers: Port 53, *domain* aus `/etc/services`)
- MAC-Adresse des Servers bzw. Routers.
- DNS-Server sendet ein Antwort-UDP-Paket.
- Rekursive Namensauflösung muss der DNS-Server machen!

HTTP-Request senden

- Analyse Routingtabelle
- ARP-Request für Webserver oder Router
- TCP-Verbindung zu Port 80 des Servers mit MAC-Adresse des Servers oder Routers (SYN, SYN+ACK, ACK)
- HTTP-Request senden
- HTTP-Response vom Server
- Schließen der Verbindung (FIN+ACK, ACK, FIN, ACK) (außer bei persistenten Verbindungen)

Weiteres Vorgehen

- Browser analysiert erhaltenen Header
- Content-Type gibt Auskunft über Art der Daten
- Nachladen von weiteren Elementen bei HTML, auch von anderen Servern
- Rendern der Seite und Anzeige oder
- Bei nicht-HTML-Daten:
  - Plugins
  - Browser-Einstellungen: Edit $\longrightarrow$ Preferences $\longrightarrow$ Applications
  - aus Datei `/etc/mailcap` oder `~/.mailcap`

Mögliche Probleme

- DNS, wird der Server gefunden, funktioniert dieser? `dig` oder `nslookup`
- Proxy-Problem: Soll einer verwendet werden, funktioniert dieser? `telnet proxy port`
- Routing-Problem: Stimmt das Routing? `netstat -rn`, `ping`, `traceroute -n`
- ARP-Problem? `arp -n`
- Antwortet der Server? `telnet Server 80`, manueller HEAD-Request
- Mitsniffen des Traffics: `tcpdump -n host` *servername*

That’s all!?!