LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

KMBD KOMPETENZNETZWERK Medienbildung und Digitalisierung

IT-Infrastruktur in der Schule

Dr.sc.nat. Michael J.M. Wagner, KMBD*

Revision 266

Inhaltsverzeichnis

*wagner@maxjosefstift.de

1 Einführung

Die IT-Infrastruktur einer Schule hat heute viele Merkmale der Struktur eines mittleren Unternehmens. Wir finden mehrere interne, von einander getrennte Netze, die mit Netzübergängen (*router, gateway*) verbunden sind. Eines der Netze hat üblicherweise auch eine Verbindung zum Internet. Desweiteren stehen im Netz Rechner für den E-Mail-Verkehr und die Bereitstellung von Internetseiten zur Verfügung (Mailserver, Webserver). Ein Server ist ein Rechner innerhalb eines Netzes, der Dienste für andere Rechner zur Verfügung stellt.

2 Internet

Für die „Erfindung" des Internets werden zwei Ereignisse gehandelt:

- 1968: Aufbau des *ARPANET* durch das US-Amerikanische Verteidigungsministerium
- 1991: Einführung des HTTP-Protokolls durch Roy Fielding, Tim Berners-Lee und andere am CERN[1].

Das *ARPANET* war ein Computer-Netzwerk, ursprünglich im Auftrag der US-Luftwaffe ab 1968 entwickelt. Es ist der Vorläufer des heutigen Internets. Kennzeichen waren die teilvermaschte Netztopologie und die paketvermittelten Netze[2]

Das *hypertext transfer protocol* (HTTP) ist ein Internet-Protokoll zum Abruf von Texten, die ihrerseits Verweise auf andere Texte haben können (*Hypertexte*).

Das Internet ist das „Netz der Netze", also ein Zusammenschluss verschiedener Netze. Man unterscheidet dabei private und öffentliche Netze. Die Netzelemente der öffentlichen Netze haben Weltweit eindeutige Adressen. Als Adressen dienen im Internet Vierertupel von Zahlen zwischen 0 und 254 (IPv4-Adresse). Da sich diese Zahlen schlecht merken lassen, gibt es parallel ein System, das Domainnamen in solche Zahlentupel umsetzt. Dieser Dienst nennt sich *Domain Name Service* (DNS).

Die Netzelemente privater Netze können vom Internet aus nicht adressiert werden, da sie keine eindeutige Adresse haben. Netzelemente desselben Netzes teilen sich die ersten Ziffern ihrer Adresse. Damit das *routing* (die Suche des Datenwegs zum gewünschneten Netzelement) weiß, ob sich dieses Element im eigenen Netz oder in einem anderen Netz befindet, muss bekannt sein, wieviele führende Ziffern das Netz bestimmen. Die Anzahl der führenden Ziffern wird durch die Netzmaske (*netmask*) bestimmt. Daten, die für ein anderes Netz bestimmt sind, werden dem Router zur Weiterleitung übergeben. Diese Informationen kann man sich in den „Verbindungsinformationen" anschaun (s. Abb. 1). Dabei bedeuten:

- IP-Adresse: Adresse des Netzelements
- Subnetz-Maske: Die ersten drei Ziffern des Tupels bestimmen das Netz.
- Vorgaberoute: Die Adresse des Routers.
- Primärer DNS: DNS-Server, der für die Auflösung von Domainnamen angefragt wird.

[1] Wikipedia: HTTP (7.7.2017)
[2] Wikipedia: ARPANET (7.7.2017)

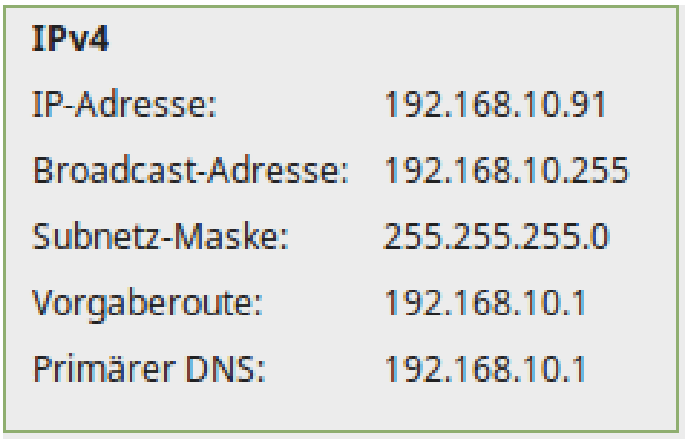

Abbildung 1: Verbindungsinformationen

Wie in der Abbildung ersichtlich, handelt es sich um IP**v4**-Adressen. Seit Jahrzehnten gibt es einen weiteren Standard: IPv6. IPv6-Adressen sind deutlich länger (128 bit, 16 Byte). Daher ist es möglich, jedem Gerät weltweit eine eindeuige Adresse zu geben. IPv6-Adressen haben etwa folgendes Aussehen: `2001:4ca0:4f04:f096::8d54:95e0`. IPv6 wird in diesem Kurs nicht weiter besprochen.

Abbildung 2 zeigt ein schematisches Netzwerkbild. Es handelt sich hierbei um Netze mit einer sternförmigen Topologie. Netzwerke, die über Ethernet verbunden sind, haben typischerweise diese Topologie. Router bilden die Netzübergänge. Diese gehören zu beiden (mehreren) Netzen.

Zur Unterscheidung öffentlicher und privater Netze haben sich auch die Begriffe *worldwide area net* (WAN) und *local area net* (LAN) eingebürgert. Ist ein Rechner im LAN nicht mit einem Netzwerkkabel, sondern über eine Funkstrecke mit dem Netz verbunden, so spricht man von einem *wireless local area net* (WLAN). Das mit dem LAN verbundene Ende der Funkstrecke nennt sich *access point* (AP). Ist ein AP mit einem Router in ein Gerät integriert, sprich man von einem WLAN-Router.

Im Folgenden werden Netzwerkdieste beschrieben, die typischerweise nicht nach innen für das LAN wirken, sondern nach außen in das Internet. Sie werden daher meist nicht aus dem privaten Netz heraus angeboten, sondern von bereits in einem öffentlichen Netz befindlichen Server.

2.1 Webserver

Webserver gibt es in verschiedenen Ausprägungen:

- HTTP-Server
  - beantwortet HTTP-Anfragen mit statischen Dateien aus dem Dateisystem
  - Beispiel: Apache
- Servlet-Engine
  - beantwortet HTTP-Anfragen durch Delegation an Programmcode
  - Apache + PHP-Plugin

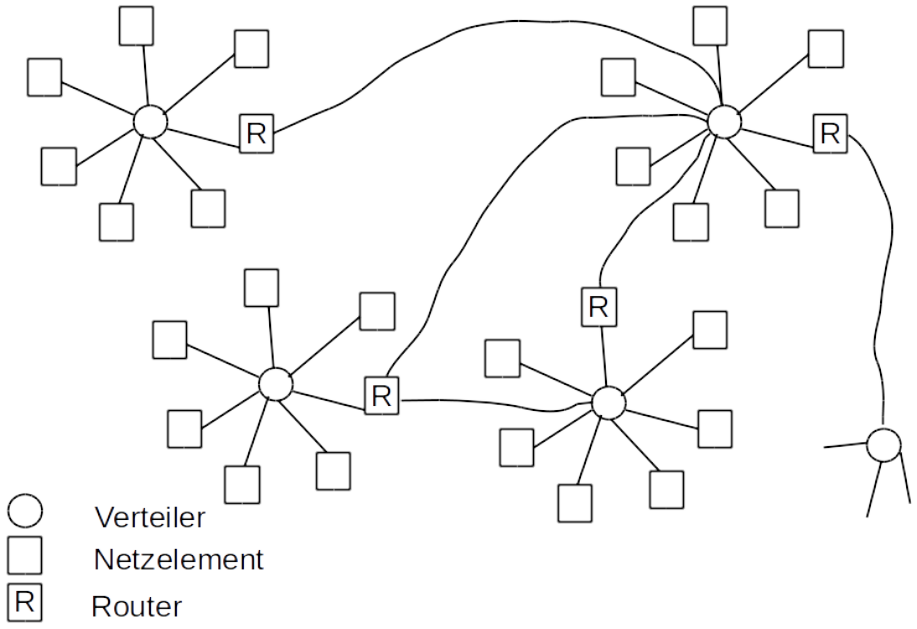

Abbildung 2: Sternförmige, über Router verbundene Computernetze

  - Tomcat (Java Servlet Engine)
- Application Server
  - Servlet-Engine + EAI-Middleware
  - Geronimo (ASF)
  - JBoss (JBoss)
  - WebSphere (IBM)

Während man in den 90er Jahren häufig statische HTML-Seiten antraf, für die ein schlichter HTTP-Server genügte, haben sich heute *content management systems* (CMS) etabliert. Diese ermöglichen die Pflege der Seiteninhalte über eigene Internetseiten, die zur Adminstration dienen. Die CMS benötigen entweder *servlet engines* oder *application server*.

Statische Seiten eignen sich für den Unterricht, um die Funktionsweise von HTTP zu demonstrieren. Sollen im Unterricht nicht nur einzelne alleinstehende Seiten, sondern ein echter *hypertext* entstehen, so müssen die Seiten auf einen Webserver gebracht werden.

2.2 Mailserver

Ein Server, der für den Empfang und das Versenden von E-Mails arbeitet, muss stets vom Internet aus erreichbar sein. Grundsätzlich empfiehlt es sich aus Datenschutzgründen nicht-private Mails nicht bei den großen Mail-Anbietern (GMX, t-online, ...) zu betreiben.

Für die Verwendung von E-Mails ist ein Mail-Programm nötig. Dieses kann entweder lokal auf dem Rechner des Anwenders laufen (Outlook, Thunderbird, ...) oder als Web-Applikation auf dem

Mailserver selbst. In letzterem Fall wird das Mailprogramm über den Browser (HTTP) bedient. Letzeres Verfahren hat den Nachteil, dass keine Ende-zu-Ende-Verschlüsselung verwendet werden kann.

Beim Austausch von E-Mails sind zwei Protokolle von Bedeutung:

- *Simple Mail Transfer Protocol* (SMTP): Dieses Protokoll wird zum Versenden von E-Mails verwendet, gegebenenfalls in zwei Schritten:
  - Wird ein lokaler Mail-Client verwendet, so schickt dieser die Mail an den eigenen Mailserver.

    Grund: Der fremde Mailserver akzeptiert meist keine Mails, die keinen „ordentlichen" Absender haben (Spam).
  - Der eigene Mailserver schickt die Mail an den fremden Mailserver, der die Mail in das Postfach des Nutzers legt.
- *Internet Message Access Protocol* (IMAP): Über dieses Protokoll holen lokale Mailprogramme die Mails vom Server und können sie auf dem lokalen Rechner speichern.

3 Netzwerkdienste

In diesem Kapitel werden nach und nach die verschiedenen Netzwerkdienste vorgestellt, die zum Funktionieren des Internets beitragen. Zur Illustration der jeweiligen Dienste werden diese dann anhand einer kleinen Übung mit der Lernsoftware Filius[3] behandelt.

Für die Übungen mit Filius ist ein SSchulnetz"vorbereitet:

Aufgabe:

- Starten Sie *filius* und laden Sie das vorbereitete Schulnetz (`Schulnetz.fls`[4])
- Starten Sie die Simulation.
- Verbinden Sie sich mit dem Rechner `172.16.10.0` (einfach draufklicken) und starten Sie darin die Konsole.
- Öffnen Sie das Protokollfenster des Rechners (rechter Mausklick „Datenaustausch anzeigen").

[3] `http://lernsoftware-filius.de` (20.01.2021)
[4] Verfügbar unter `http://wagnertech.de/public/KMBD/`

3.1 Routing

Das *routing* ist eines der zentralen Netzwerkdienste. Jedes Netz ist durch den führenden Teil der IP-Adresse identifiziert. Jeder Rechner entscheidet anhand der Adresse, ob für ein IP-Paket das Ziel im eigenen Netz zu suchen ist, oder an einen Router übergeben wird. Jeder Rechner/Router hat eine Standardroute (*default route*), an die er alle Pakete weitergibt, deren Netze er nicht kennt. Auf diese Weise besteht die Hoffnung, dass jedes Paket irgendwann sein Ziel erreicht. *IP routing* ist nicht deterministisch!

Wir müssen also zwei Dinge unterscheiden: Den Knoten, an den ein Datenpaket erst mal gegeben wird, u.U. mit der Bitte der Weiterleitung und den Rechner, den das Paket final erreichen soll. Daher werden sog. OSI-Modell[5] verschiedene Protokollschichten unterschieden. Die Schicht, die die Kommunikation von Paketen mittels IP-Adressen beschreibt, ist Schicht 3 (Vermittlung). Die direkte Punkt-zu-Punkt-Kommunikation ist in Ebene 2 (Netzzugang) beschrieben.

In OSI-Ebene 2 werden die Rechner nicht mit ihren IP-Adressen, sondern mit den MAC-Adressen adressiert. Oftmals hat ein Rechner mehrere Netzwerkschnittstellen zur Verfügung, die zu verschiedenen Netzen gehören (z.B. Netzwerkkabel und WLAN). Die Zustellung von Datenpaketen läuft daher nach folgendem Muster ab:

- Prüfe die Ziel-IP-Adresse: Liegt sie in einem meiner Netze?
  - Wenn Ja, frage in diesem Netz nach der MAC-Adresse dieses Geräts.
    - Wenn niemand antwortet, beende mit einer Fehlermeldung
  - Sende das Paket an den Rechner mit der ermittelten MAC-Adresse
- Ermittle die Defaultroute.
- Prüfe, zu welchem meiner Netze die Defaultroute gehört.
- Frage in dem Netz nach der MAC-Adresse der Defaultroute.
  - Wenn niemand antwortet, beende mit einer Fehlermeldung
- Sende das Paket an die MAC-Adresse der Defaultroute.
- Die Defaultroute wird das Paket übernehmen. Im Paket steht die IP-Adresse des eigentlichen Ziels. Jetzt beginnt im Router das Spiel von neuem.

Das Ebene-2-Protokoll zur Ermittlung der MAC-Adresse nennt sich *address resolution protocol* (ARP).

Zur Überprüfung der eigenen IP- und MAC-Adressen stehen folgende Befehle zur Verfügung:

```
ipconfig /all      (Windows)
ip a               (Linux)
ipconfig           (filius)
```

Um ein Paket an einen anderen Rechner zu schicken, gibt es den Befehl `ping <ziel>`. Für die Verfolgung der Route stehen folgende Befehle zur Verfügung:

[5] `https://de.wikipedia.org/wiki/OSI-Modell` (21.01.2021)

```
tracert <ziel>        (Windows)
traceroute <ziel>     (Linux)
traceroute <ziel>     (filius)
```

Aufgabe:

- Überprüfen Sie die eigene IP- und MAC-Adresse.
- Pingen Sie einen Rechner im eigenen Netz, sowie einen Rechner in einem anderen Netz an. Im eigenen Netz können Sie stets Ihre Defaultroute anpingen.
- Betrachten Sie die Route zu diesen Rechnern.
- Führen Sie die genannten Operationen auch auf dem Client `172.16.10.1`.
- Betrachten Sie den Datenaustausch.

3.2 Domain Name Service (DNS)[6]

Das TCP/IP-Protokoll verwendet IP-Adressen um Rechner im Netz zu adressieren. Da diese für den menschlichen Nutzer wenig aussagekräftig sind, zudem sich immer wieder mal ändern, stehen alternativ dazu Rechnernamen zur Verfügung. Die Umsetzung dieser Rechnernamen in IP-Adressen leistet der Domain Name Service (DNS).

DNS ist eine verteilte Datenbank. Es besteht aus zwei wichtigen Elementen: Zum einen den Namenservern, die die DNS-Server-Software ausführen und auf Anfrage Namensinformationen herausgeben, zum anderen aus dem hierarchischen System der Domain-Namen selbst.

Ein vollständiger Domain-Name (*fully qualified domain-name* (FQDN) ist dabei von rechts nach links zu interpretieren. Ganz rechts steht die *top level domain* (TLD). Diese werden der *Internet Assigned Numbers Authority* (IANA), einer Unterorganisation der *Internet Corporation for Assigned Names and Numbers* (ICANN) verwaltet. Die wichtigsten TLD sind die US-amerikanischen `.com`, `.net`, etc. und die Länderkennungen `.de`, `.ch`, ...

Neben der TLD steht die *second level domain* (SDL). Diese können sich Organisationen und Privatpersonen bei den TLD registrieren lassen. Für die .de-Domain ist die DENIC zuständig. SDL und TDL bilden die *Zone*. Innerhalb einer Zone können weitere Hosts definiert sein (`www.example.de, ftp.example.de`, ...). Die Verwaltung der Zone erfolgt üblicherweise durch den Inhaber der SLD.

Jeder Rechner, der mit dem Internet kommuniziert, kennt mindestens einen Nameserver. Dieser wird entweder direkt konfiguriert, oder dem Rechner über DHCP (s. Abschn. 3.3) mitgeteilt. Der Host, der eine Namensauskunft wünscht, befragt nun die ihm bekannten Nameserver der Reihe nach.

Umgekehrt kann das DNS-System IP-Adressen in FQDN umsetzen. Zur Überprüfung beider Richtungen stehen auf einem Linux-System folgende Befehle zur Verfügung:

```
nslookup <dns-name>     (Windows)
host <dns-name>         (Linux, filius)
```

[6] Suse 10: S. 600ff.

Mit diesen Kommandos kann auch der FQDN für eine gegebene IP-Adresse abgefragt werden.

Aufgabe:

- Ermitteln Sie die IP-Adresse von `wagnertech.de`.
- Fragen Sie, welcher Name zur erhaltenen IP gehört.
- Machen Sie die diesselben Abfragen in filius und betrachten Sie den Datenaustausch.

3.3 Domain Host Configuration Protocol (DHCP)[7]

Das DHCP-Protokoll versorgt Rechnner innerhalb eines Netzes mit Konfigurationsdaten. Die wichtigsten sind dabei

- die IP-Adresse,
- die IP-Adresse des Default-Gateways,
- die IP-Adresse des Name-Servers.

Aktiviert ein Client eine Schnittstelle (Netzwerkkarte, WLAN-Verbindung), die über das DHCP-Protokoll konfiguriert werden soll, läuft folgender Datenaustausch ab:

- Der Client schickt ein *DHCP Discover* als Broadcast, um im Netz befindliche DHCP-Server ausfindig zu machen.
- Der Server antwortet mit einem *DHCP Offer*. Dem Client werden Konfigurationsdaten angeboten.
- Der Client akzeptiert das Angebot mit einem *DHCP Request*.
- Der Server bestätigt die Konfigurationsdaten mit einem *DHCP ACK*.

Damit ist im Gutfall die Kommunikation beendet. Will ein Client die IP-Adresse wieder frei geben, erfolgt das mit einem *DHCP Release*.

Soll auf einem Client überprüft werden, ob dieser über DHCP mit den richtigen Daten versorgt worden ist stehen dafür folgende Befehle zur Verfügung:

```
ipconfig /all      (Windows)
ip a               (Linux)
ipconfig           (filius)
```

Aufgabe:

- Führen Sie die genannten Befehle auf Ihrem Rechner aus.
- Führen Sie in *filius* `ipconfig` auf der Konsole des Client `172.16.10.0` aus.
- Betrachten Sie hier auch den Nachrichtenfluss, insbesondere den Verkehr nach dem Start des Rechners.

[7] TCP/IP

3.4 Network Address Translation (NAT)

Beim Routing wird davon ausgegangen, dass eine IP-Adresse weltweit eindeutig ist. Eine Ausnahme bilden dabei die privaten Netzwerke. Kommuniziert ein Rechner eines privaten Netzwerkes mit dem Internet, muss seine (private) IP-Adresse am Gateway auf eine eindeutige Adresse umgesetzt werden. Als Sendeadresse wird die Adresse des Gateways eingesetzt. Auf dem Rückweg muss das Gateway dann wissen, welchem internen Rechner die Antwort zugestellt werden muss. Diesen Vorgang nennt man *Network Address Translation* (NAT) oder *IP Masquerade*. Um nun auf einen Dienst, den ein Rechner im privaten Netz anbietet, auch vom Internet aus zugreifen zu können, muss der Dienst formal am Gateway angesprochen werden. Das Gateway muss dann wissen, an welchen internen Rechner die Anfragen delegiert werden müssen (*port forwarding*).

3.5 HTTP-Proxy

Um eine gewisse Sicherheit im internen Netz zu gewährleisten, kann es für normale Client-Rechner verboten sein, über den NAT-Dienst Verbindung mit dem Internet aufzunehmen. Um aber dennoch über HTTP auf Internetseiten zugreifen zu können, steht in solchen Netzen ein „Stellvertreter" (*proxy*) zur Verfügung.

Über die Proxyeinstellung, die in entsprechend admistrierten Netzen dem Browser (InternetExplorer, Firefox, ...) automatisch zur Verfügung gestellt wird, sendet der Browser des Client-PC seine HTTP-Anfragen an den Proxy-Rechner. Dieser nimmt über das Gateway Kontakt mit dem Webserver im Internet auf und liefert die angeforderten Inhalte zurück an den Client. Bei diesem Vorgang ist es möglich, die Netzinhalte zu filtern.

3.6 Lightweight Directory Access Protocol (LDAP)

Für eine unternehmensweite Authentifizierungsverwaltung werden in Unternehmen Verzeichnisdienste eingesetzt. Dabei handelt es sich um einen Serverdienst, der die Daten sämtlicher Netzwerke, Rechner, Benutzer und Gruppen des Unternehmens speichert und bei jeder Netzwerkanmeldung überprüft, ob die aktuelle Rechner-Benutzer-Kombination die erforderliche Berechtigung besitzt. Die wichtigsten Verzeichnisdienste sind:

- NIS, NIS+ (früher *yellow pages (yp)*)
- Novell Directory Services (NDS), eDirectory
- OpenLDAP
- Active Directory

Bis auf NIS basieren alle auf der X.500-Spezifikation, auf dem LDAP-Protokoll.

Will sich ein Nutzer an einem Rechner einloggen, so überprüft das System zum einen die lokal hinterlegten Nutzer, zum anderen fragt es den oder die Verzeichnisdienste, ob der sich einloggende Nutzer bekannt ist. Die möglichen Verzeichnisdienste müssen zuvor vom Administrator im System hinterlegt sein. Bei Windows-Systemen haben sich für diese Vorgänge eigene Begriffe etabliert:

- Verzeichnisdienst = „Domänencontroller" oder „Active Directory"

- Verzeichnisdienst im Client-System hinterlegen = „Rechner in die Domäne nehmen"

Über die Windows-Domäne werden allerdings mehr Systemeigenschaften als nur der Login gesteuert:

- Welchen Proxy soll soll der Browser verwenden?
- Welche Drucker stehen zur Verfügung?
- Welche Netzlaufwerke sollen standardmäßig zur Verfügung stehen?

3.7 Remote Desktop Protocol (RDP)

Sollen an einem Client-Rechner graphische Programm bedient werden, die selbst aber auf einem Server laufen, gibt es dafür verschiedene Möglichkeiten der Darstellung:

- Verwendung einer Client-seitigen Anwendung (Applikation), die der Anwender erst installieren muss.

  Beispiel: Facebook als App.

  Vorteil: geringstes Datenvolumen, da proprietäre Schnittstelle

- Verwendung eines Web-Browsers als „Universal-Client". Der Server stellt das gewünschte Programm als HTTP-Dienst (Web-Applikation) zur Verfügung.

  Beispiel: Facebook über den Browser

  Vorteil: Keine Installation am Client nötig

- Übertragung der graphischen Daten der gewünschten Anwendung vom Server zum Client, die dort vom Client-seitigen Windowmanager in den Bildschirm eingebunden werden.

  Nachteil: Nur auf Linux-Systemen möglich

- Übertragung eines kompletten Bildschirms vom Server zum Client (RDP).

  Nachteil: Sehr hohes Datenaufkommen, benötigt hohe Server-seitige Rechenleistung

Ein Server, von dem per RDP komplette Bildschirminhalte abgerufen werden können, nennt sich auch *terminal server*.

Auf der anderen Seite ermöglicht ein Terminalserver die zentrale Verwaltung von Anwendungen, was im Schulkontext sehr nützlich ist. Anwendungen können zentral installiert werden und stehen sofort allen Anwendern zur Verfügung. Ein weiterer Vorteil ist, dass am Client weniger Rechenleistung benötigt wird, also nur ein *thin client* benötigt wird (s.a. Kap. 4.4).

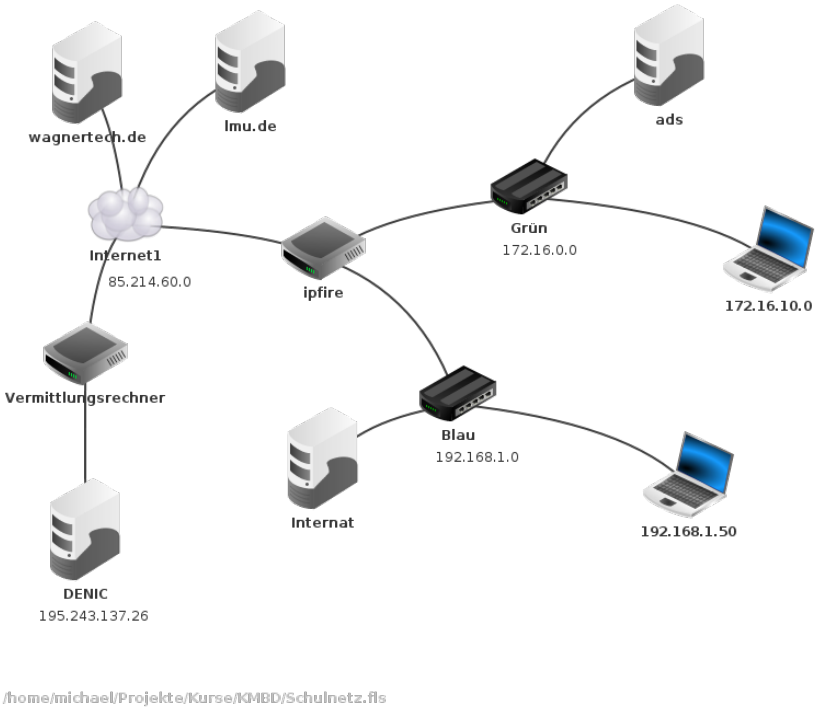

Abbildung 3: Filius - Schulnetz

4 Schulinfrastruktur

4.1 Projekthintergrund

An dieser Stelle wird als typische Schulinfrastruktur „Linuxmuster"[8] vorgestellt. Die Netztopologie ist an vielen Schulen ähnlich, auch wenn oft Windows statt Linux eingesetzt wird.

> linuxmuster.net ist eine umfassende Komplettlösung für den Betrieb schulischer Netzwerke. Sie wird von Lehrkräften und Dienstleistern für die speziellen Anforderungen in der Schule entwickelt.
>
> Koordination bei Pflege und Weiterentwicklung von linuxmuster.net wird in einem gemeinnützigen Verein organisiert.[9]

Mit der Lernsoftware „Filius" ist es möglich Netzfunktionen im „Sandkasten" auszuprobieren. In der vorbereiteten Datei ist ein Netz aufgebaut, das in Grundzügen dem „Musternetz" entspricht. Das grüne Netz ist das Schulnetz, in dem die Rechner für Lehrer und Schüler hängen. Die Zutrittsverwaltung erfolgt typischerweise über einen LDAP-Server/Domänen-Controller. Dieser fehlt im Beispiel. Das blaue Netz ist für den Anschluss privater Geräte. Die Geräte dieses Netzes müssen in den Firewall-Einstellungen des Routers freigeschaltet werden. Siehe Abbildung 3.

[8] `http://www.linuxmuster.de`
[9] `http://www.linuxmuster.net/de/home/` (27.10.2017)

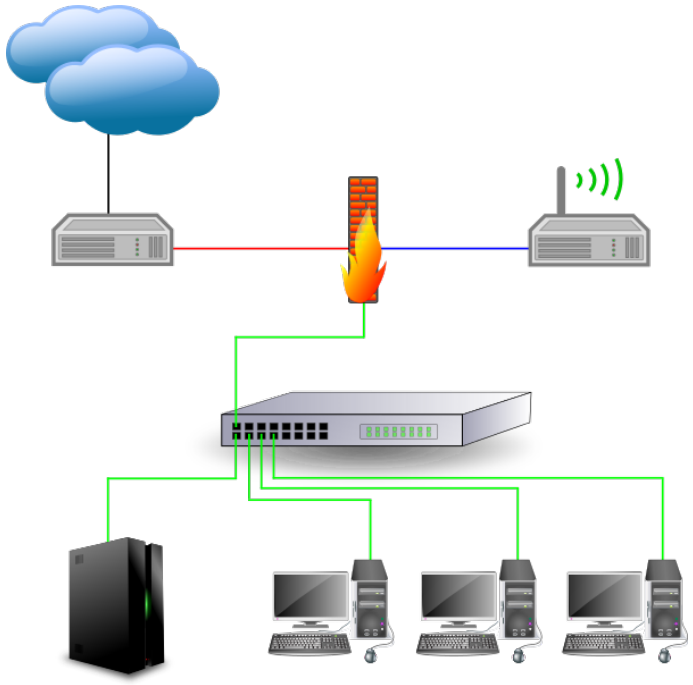

Abbildung 4: Muster-Netz

4.2 Der Router ipfire

Im Musternetz werden drei Netze unterschieden (s. Abb. 4):

- rot: Das Internet (WAN)
- grün: Das Schulnetz (LAN)
- blau: Ein weiteres LAN, in dem aber die schulspezifischen Dienste nicht zur Verfügung stehen (ggf. für Hausmeister, Küche, Internat).

4.3 Der Server

In „normalen" Schulumgebungen werden die verschiedenen Server *virtualisiert*, d.h. auf einem physischen leistungsfähigen Server werden verschiede virtuelle Server betrieben.

Der Linuxmuster-Server beinhaltet viele Funktionen:

- DNS-Server
- DHCP-Server
- LDAP-Server
- Mail-Server
- Webserver für die Bedienung
- Datei-Server
- Setup für die Clients

4.4 Die Clients

Bei *Linuxmuster* sind die Clients „dick" (*thick clients*) ausgelegt. Die Clients sind vollwertige Rechner. Dieses Konzept hat Vor- und Nachteile:

- Die Clients sind teuerer und (meist) größer.
- Das System *skaliert*, d.h. es ist eine beliebige Anzahl von Clients möglich.
- Der Server wird beim Anschluss weiterer Clients nur unwesentlich mehr belastet.
- Damit die Clients stets denselben Softwarestand haben, werden diese beim Start mit einem zentralen Abbild synchronisiert.

Das alternative Konzept verwendet *thin clients*, die selbst nur eine RDP-Verbindung zum Server halten (*terminal server*). Dieser muss dann Rechenleistung für die ganze Schule zur Verfügung stellen.

5 Weitere Aufgaben

Mit folgenden Aufgaben werden die Auswirkungen des Ausfalls bestimmter Netzwerkdienste illustriert.

DHCP, DNS, Routing

Aufgabe:

Im grünen Netz werden die Funktionen DHCP und DNS durch den ads-Server zur Verfügung gestellt. Um zu demonstrieren, wie sich ein Serverausfall auswirkt sollen nun folgende Schritte durchgeführt werden:

- Verwenden Sie einen Client im grünen Netz.
- Ermitteln Sie mit `host lmu.de` die IP-Adresse dieses Rechners und notieren Sie sich diese.
- Beenden Sie den DNS-Server und den DHCP-Server auf dem ads-Rechner.
- Ermitteln Sie die Route zum `lmu.de`-Rechner, einmal indem Sie im `traceroute`-Befehl den Rechnernamen, einmal indem Sie die IP-Adresse verwenden.
- Versuchen Sie mit dem Webbrowser die Internetseite von `lmu.de` anzuschaun: Einmal indem Sie `lmu.de` in den Browser eingeben, einmal mit der IP-Adresse.
- Verbinden Sie einen weiteren Linux-Client mit dem grünen Netz und versuchen Sie dasselbe.
- Schalten Sie DHCP- und DNS-Server auf ads wieder ein.

Zur Erklärung: Der erste Client über DHCP die Adressen von DNS-Server und Gateway bekommen. Wenn die Namensauflösung über DNS ausfällt, kann die Route immer noch auf Basis der IP-Adressen ermittelt werden. Der zweite Client bekommt aber über DHCP keine Adressen mitgeteilt und kennt daher das Gateway nicht, über das er ins Internet käme.

Aufgabe:

Eine andere Ausfallmöglichkeit ist der Übergang ins Internet.

- Der Ausfall der Internetverbindung wird dadurch simuliert, dass die IP-Adresse der roten Schnittstelle am ipfire verändert wird. Damit können keine Pakete zurückgeroutet werden.
- Prüfen Sie mit `ipconfig`, ob der Client mit den richtigen DNS- und Gateway-Daten versorgt wurde.
- Prüfen Sie am Client im grünen Netz mit `host ads` die schulinterne Namensauflösung.
- Prüfen Sie mit `host lmu.de` die Auflösung eines Internet-Namens.
- Prüfen Sie mit `ping 85.214.60.111` die Verbindung zum Internet.

Firewall

Das blaue Netz ist durch restriktive Regeln in der Firewall des ipfire geschützt. Ihr neuer Client im blauen Netz hat zwar die Adressen von DNS-Server und Gateway erhalten, es funktioniert aber fast nichts.

Aufgabe:

- Fügen Sie dem blauen Netz einen weiteren Client hinzu.
- Prüfen Sie mit `ping <IP-Adresse>`, ob DNS-Server und Gateway erreichbar sind.

  Die Firewall ist so eingestellt, dass `ping`-Verkehr grundsätzlich erlaubt ist.
- Prüfen Sie mit `host lmu.de`, ob der Name aufgelöst werden kann.
- Prüfen Sie mit `ping 85.214.60.111`, ob `lmu.de` erreichbar ist.
- Versuchen Sie mit dem Webbrowser die Internetseite von `lmu.de` anzuschaun: Einmal indem Sie `lmu.de` in den Browser eingeben, einmal mit der IP-Adresse.
- Öffnen Sie im ipfire die Firewallregeln und fügen Sie für Ihre IP eine Regel wie für den bestehenden Client hinzu. Führen Sie obige Prüfungen erneut aus.

Webserver

Mit Internetseiten lassen sich Inhalte verknüpfen. Damit kann einer Klasse die Möglichkeit gegeben werden, das Ergebnis von Gruppenarbeiten medial aufzubereiten. In der 7. Klasse des derzeitigen

```
<html>
<title>Titel der Seite</title>
<meta http-equiv="Content-Type" content="text/html;charset=UTF-8">
<body>
<h1>&Uuml;berschrift Ebene 1</h1>
<h2>&Uuml;berschrift Ebene 2</h2>
<p>Ein Absatz</p>
<p>
Noch ein Absatz, mit
<a href="http://wagnertech.de">Absoluter Referenz</a>
</p>
<p>
Noch ein Absatz, mit
<a href="/klassen/8a/index.html">Referenz auf demselben Server</a>
</p>
</body>
</html>
```

Abbildung 5: Aufbau einer statischen HTML-Seite

gymnasialen Lehrplans lernen Schüler solche Seiten zu erstellen. Damit lässt sich diese Fähigkeit auch für andere Fächer nützen. In der folgenden Übung soll nun simuliert werden, wie verschiedene Schüler ihren Beitrag zu einer gemeinsamen Präsentation leisten können.

Statische Webserver suchen gemäß der übergeben URL die zugehörige Datei im Dateisystem und geben diese an den Aufrufer zurück. Endet die URL ohne Dateinamen, so wird nach der Datei `index.html` gesucht. Das Basisverzeichnis heißt beim Filius-Webserver `/webserver`. Abb. 5 zeigt den Aufbau einer statischen HTML-Seite.

Aufgabe:

In dieser Übung sollen gegenseitig verlinkte Internetseiten erzeugt werden. Einstieg soll die URL `http://schulserver/8a` sein. Die hier hinterlegte Seite soll zu den Seiten der Schüler verweisen. Die Seiten der Schüler sollen auch untereinander verlinkt sein.

- Richten Sie im Schulnetz einen Schulserver ein. Dieser soll den Namen `schulserver` mit der festen IP `172.16.0.150` bekommen. Verbinden Sie den Rechner mit dem grünen Netz.
- Installieren Sie den Webserver, einen Text-Editor und den Datei-Explorer.
- Ergänzen Sie im DSN-Server des ads den Eintrag für den Schulserver.
- Legen Sie unterhalb des Verzeichnisses `/webserver` das Verzeichnis `8a` und darin zwei Verzeichnisse für zwei Schüler.[10]
- Erstellen Sie Internetseiten für zwei Schüler und legen Sie diese die entsprechenden Verzeichnisse. Die Seiten sollen je eine externe Referenz, als auch eine Referenz auf die je andere Seite enthalten.

- Verlinken Sie die Dateien der Schüler mit der `8a/index.html`.

Anmerkung: Bei einem solchen Vorgehen sind die erstellten Internetseiten „Intranetseiten", d.h. von außen nicht erreichbar.

6 Glossar

AP	*access point*, Sender für ein WLAN
ARPANET	*advanced research projects agency network*, ein Computer-Netzwerk und wurde ursprünglich im Auftrag der US-Luftwaffe ab 1968 entwickelt. Es ist der Vorläufer des heutigen Internets. Kennzeichen waren die teilvermaschte Netztopologie und die paketvermittelten Netze.
DNS	*domain name service*, setzt Domainnamen in IP-Adressen um.
Ethernet	System aus Kabeln und Switchen zum Aufbei eines Computernetzes
HTTP	*hypertext transfer protocol*, Internet-Protokoll zum Abruf von Texten, die ihrerseits Verweise auf andere Texte haben können (*Hypertexte*).
IMAP	*internet message access protocol*, Protokoll, mit ein Mail-Client E-Mails mit einem Server austauscht.
IP	*internet protocol*
LAN	*local area net*, privates Netz
LDAP	*lightweight directory access protocol*, Protokoll zur Verwaltung von Authorisierungsdaten
RDP	*remote desktop protocol*, Protokoll zur Übertragung des Bildschirminhalts auf einen anderen Rechner
Router	Rechner, der zwei (der mehr) Netze miteinander verbindet.
Routing	Die Suche des Datenwegs zum gewünschneten Netzelement
Server	Rechner innerhalb eines Netzes, der Dienste für andere Rechner zur Verfügung stellt.
SMTP	*simple mail transfer protocol*, Protokoll zum Versenden von E-Mails
URL	*uniform resource locator*, Bezeichnungsstandard für Netzwerkressourcen
WAN	*worldwide area net*, öffentliches Netz
Webserver	Server, der Internetseiten über das HTTP-Protokoll zur Verfügung stellt.
WLAN	*wireless local area net*, auf Funktechnik basierendes privates Netz
WLAN Router	Kombination aus Router und AP

[10] Diese Formulierung umfasse männliche, weibliche und sonstige Schüler.

7 Quellen

Suse 10	S. Kersken, SUSE Linux 10.x, Galileo Computing 2006.
TCP/IP	ICN TI Enabling. Kurs ICP/IP Grundlagen. Siemens 1999.
Wikipedia	http://wikipedia.de. Stichworte und Abrufzeitpunkt in den Fußnoten.