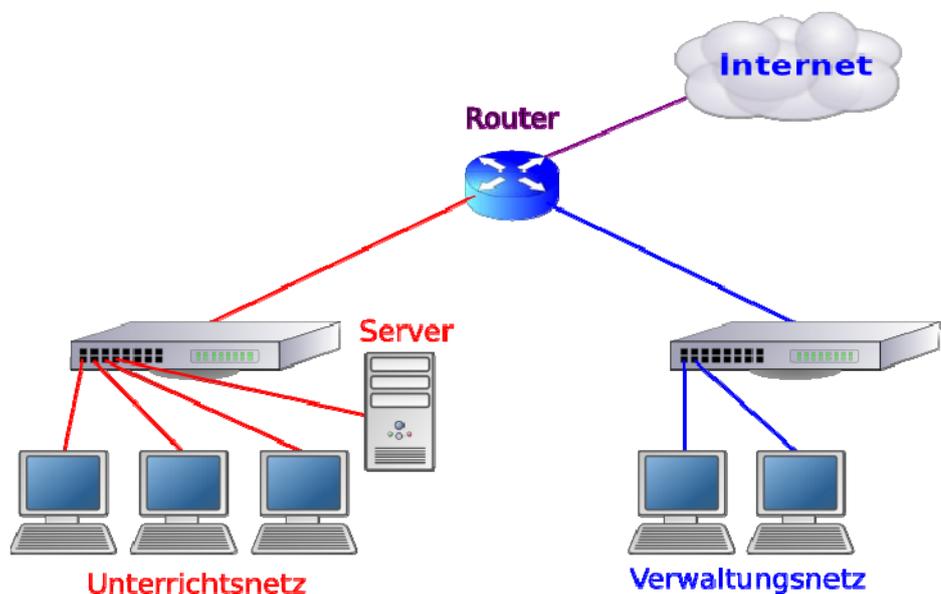


## Überlegungen zur Struktur eines Schulnetzes

**Kurzbeschreibung** Viele Schulen arbeiten heute mit einem Computernetzwerk, das unterschiedlichen Anforderungen genügen muss. Bereits durch eine entsprechende Struktur des Netzwerkes lassen sich manche dieser Anforderungen erfüllen, wie der folgende Text aufzeigen soll.

### Prinzipieller Aufbau



Meist besteht das Schulnetz aus zwei Teilen, dem Unterrichtsnetz und dem Verwaltungsvernetz, die mit unterschiedlichen Anforderungen verbunden sind. Da von beiden Netzen ein Zugang zum Internet benötigt wird, gibt es einen Router, der die beiden Netze mit dem Internet verbindet.

**Anforderungen an das Schulnetz** Das Unterrichtsnetz stellt den Schülern und Lehrern Ressourcen für den Einsatz von Computer und Internet im Unterricht zur Verfügung. Hierbei hat man es mit wechselnden Benutzern an den Arbeitsstationen zu tun. Diese erwarten, eine vordefinierte Arbeitsumgebung vorzufinden. Beim Einsatz des Internets und anderer Medien sind die Vorgaben des Jugendmedienschutzes zu beachten.

## Überlegungen zur Struktur eines Schulnetzes

Auch für das Verwaltungsnetz muss ein Internetzugang zur Verfügung gestellt werden. Auf dieser Seite hat man jedoch nur wenige Benutzer mit festen Arbeitsplätzen.

Es wird erwartet, dass beide Teilnetze gegenüber Angriffen von innen wie von außen geschützt werden. Weiterhin ist sicher zu stellen, dass kein Zugriff aus dem Unterrichtsnetz auf das Verwaltungsnetz möglich ist.

**Neue Herausforderungen** Neben diesen Anforderungen treten inzwischen neue Herausforderungen auf:

- Viele Kollegen bringen inzwischen ihre privaten Notebooks mit in die Schule und möchten die Infrastruktur des Schulnetzes, wie Drucker, Internetzugang, Datenspeicher, etc. nutzen. Auf diese privaten Computer hat die Systembetreuung keinen administrativen Zugriff. Sie kann auch nicht sicherstellen, dass diese virenfrei sind und hat keinen Einfluss auf die installierten Programme. Das gleiche Problem besteht bei Schülernotebooks.
- Da es inzwischen Programme gibt, so genannte Portable Applications, die nicht mehr installiert werden müssen, muss nicht mehr ein privater Computer ans Netzwerk angeschlossen werden, es genügt bereits ein USB-Stick an einem Schulcomputer. Damit lassen sich z. B. Server starten, die eine eigene Netzwerkinfrastruktur aufbauen, in die die Systembetreuung keinen Einblick hat und keine administrativen Rechte besitzt. Die Infrastruktur wird im Allgemeinen auch nur temporär bestehen, so dass sie schwer aufzuspüren ist.

**Fazit** Nachdem die Systembetreuung nach den obigen Überlegungen nur begrenzten, bis gar keinen Einfluss auf die Arbeitsplatzrechner hat, muss man akzeptieren, dass es nur mit großem Aufwand oder bisweilen gar nicht möglich ist, einen Arbeitsplatzrechner entsprechend abzusichern. Weiterhin stehen an der Schule - im Gegensatz zum Berufsleben - kaum wirksame Sanktionsmöglichkeiten, wie z.B. eine Abmahnung, zur Verfügung.

**Konsequenzen** Auf Grund der oben geschilderten Problematik sollte man sich beim Arbeitsplatz im Schulnetz lediglich darauf beschränken, eine konstante Ausgangskonfiguration zu gewährleisten. Dies lässt sich mit einer so genannten Wächterkarte oder einer entsprechenden Software erreichen. Außerdem muss für einen Virenschutz gesorgt werden.

Alle anderen Maßnahmen müssen an anderen Stellen im Netzwerk durchgeführt werden. Da verhindert werden muss, dass andere Personen direkten Zugang zu den Geräten haben, sollte als erste Maßnahme eine örtliche Trennung zwischen den Arbeitsplatzrechnern des Unterrichtsnetzes und den anderen Netzwerkkomponenten durchgeführt werden. Weiterhin sollten die im Netzwerk verwendeten Ad-

## Überlegungen zur Struktur eines Schulnetzes

Administratorpasswörter nicht mit den Passwörtern auf dem Arbeitsplatzrechner übereinstimmen.

Im Folgenden wird nun aufgezeigt, wie sich durch weitere infrastrukturelle Überlegungen die Anforderungen an ein Schulnetz umsetzen lassen. Hierbei sollen im ersten Punkt die Möglichkeiten des Routers betrachtet werden.

### Router-konfiguration

Der Router verbindet Unterrichts- und Verwaltungsnetz und ermöglicht für beide Teile den Zugang zum Internet. Wie im Folgenden beschrieben, lassen sich durch eine entsprechende Konfiguration des Routers bereits viele Sicherheitsanforderungen an das Schulnetz umsetzen.

- **Aktivierung von NAT** (Network Address Translation)

Durch diese Option werden beim Datenverkehr aus dem Schulnetz ins Internet die lokalen Adressen durch die Routeradresse ersetzt. Außerdem akzeptiert der Router dadurch nur Datenpakete aus dem Internet, die zu einer Anfrage aus dem Schulnetz gehören. Durch diese Maßnahme erhält man einen guten Schutz vor Angriffen aus dem Internet.

- **Deaktivierung von UPnP** (Universal Plug and Play)

UPnP ermöglicht die Konfigurierung des Routers durch externe Programme. Ist diese Option aktiviert, lässt sich von den Arbeitsplatzrechnern sehr einfach der Router umkonfigurieren. In diesem Fall werden damit alle Sicherheitsüberlegungen zunichte gemacht. Daher ist diese Möglichkeit zu deaktivieren.

- **Konfiguration der Firewall**

Ein wichtiges Instrument, um die Anforderungen an ein Schulnetz zu erfüllen, ist die Firewall des Routers. Daher sollte ihre Konfiguration sorgsam geplant werden. Die Firewall kann Verbindungen zu anderen Netzen oder einzelnen Computern sperren oder zulassen. Außerdem können auch die Verbindungen für einzelne Dienste (http, ftp, Mail, ... ) geregelt werden.

Ein bewährte Vorgehensweise ist es, zuerst die gesamte Kommunikation über den Router zu sperren. Dadurch verhindert man bereits den Zugriff auf das Verwaltungsnetz aus dem Unterrichtsnetz heraus.

Benötigte Kommunikationswege werden dann explizit geöffnet. Für das Verwaltungsnetz kann so ein Zugriff auf das Unterrichtsnetz eingerichtet werden, wenn dies benötigt wird. Auf die gleiche Weise können die Wege ins Internet für die benötigten Dienste geöffnet werden.

## Überlegungen zur Struktur eines Schulnetzes

Der Zugang aus dem Unterrichtsnetz sollte sehr restriktiv gestaltet werden. Meist werden nur die Dienste http und https für den Unterricht benötigt. Daher sollten auch nur diese freigegeben werden.

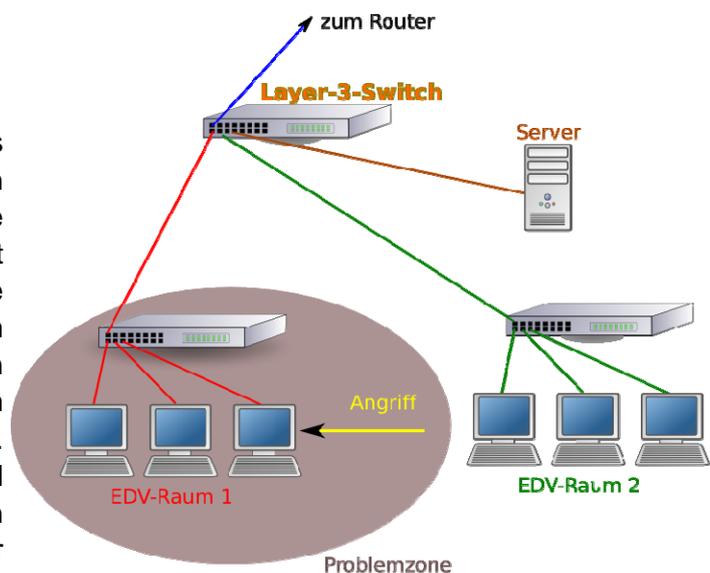
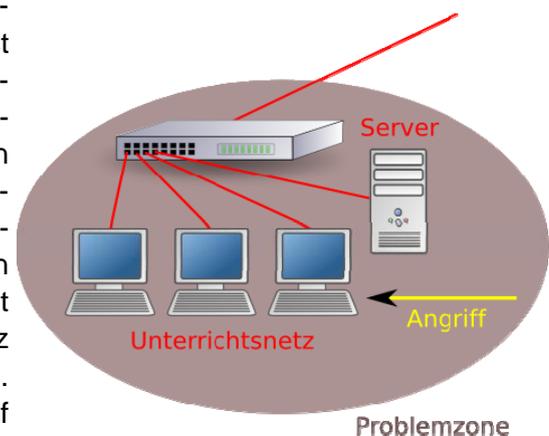
Verwendet man einen Proxyserver mit Webfilter, sollte der Zugang ins Internet nur auf diesen einen Rechner freigegeben werden. Damit verhindert man ein Umgehen des Webfilters. Wird außerdem der Router als DNS-Server genutzt und der DNS-Dienst in der Firewall nicht geöffnet, können die Jugendmedienschutzvorkehrungen der Schule kaum umgangen werden.

### Strukturierung des Unterrichtsnetzes

Angriffe von außen lassen sich durch die entsprechende Routerkonfiguration gut abwehren. Problemfälle im Unterrichtsnetz können jedoch durch diese Maßnahmen nicht beeinflusst werden. Da wie oben beschrieben die Arbeitsplatzrechner nicht gesichert werden können, sollte wenigstens versucht werden, die Auswirkungen einzuschränken. In der bisherigen Konfiguration ist das gesamte Unterrichtsnetz von einem Problem betroffen. Wird ein Schadprogramm auf einem Rechner gestartet oder z. B. eine Schleife durch Verbindung zweier Netzwerksteckdosen erzeugt, so wirkt sich dies auf das gesamte Unterrichtsnetz aus. Da sich diese Probleme kaum abstellen lassen, sollte versucht werden, ihren Wirkungsbereich einzuschränken und mehr oder weniger auf einen Unterrichtsraum zu beschränken. Dann hat man auch eine Chance, diese Probleme auf

„pädagogischem“ Wege zu lösen.

Hierzu wird das Unterrichtsnetz in mehrere Teilnetze aufgeteilt. Nicht mehr alle Räume gehören zu einem Netz bzw. hängen an einem zentralen Switch. In diesem Fall wird für jeden Raum ein eigener Switch verwendet



## Überlegungen zur Struktur eines Schulnetzes

und von dort geht dann eine Verbindung an einen zentralen Switch. Hierbei muss ein so genannter Layer-3-Switch verwendet werden, der in der Lage ist, Netze zu trennen und damit eine Routing- und Firewallfunktion bietet. Dadurch lassen sich, wie beim Router, die Übergänge zwischen den einzelnen Netzen regeln. Bei einem Problem im EDV-Raum 1 werden damit die anderen Bereiche des Unterrichtsnetzes nicht beeinträchtigt und das Problem lässt sich lokalisieren.

**Weiterführende Informationen** [http://alp.dillingen.de/schulnetz/materialien/Sichere\\_Internetanbindung\\_1.pdf](http://alp.dillingen.de/schulnetz/materialien/Sichere_Internetanbindung_1.pdf)

**Bildquellen** Die Grafiken wurden mit Elementen von [OpenClipart.org](http://OpenClipart.org) gestaltet.

**Autor** Werner Müller, Gymnasium Wertingen