



Akademie  
für Lehrerfortbildung  
und Personalführung

# Sichere Internetanbindung von Schulen



Qualifizierung für  
Systembetreuer

Laborübungen  
Juli 2010

## **Impressum**

Herausgeber: Akademie für Lehrerfortbildung und Personalführung  
Kardinal-von-Waldburg-Str. 6-7  
89407 Dillingen

Autoren: Georg Schlagbauer, Akademie Dillingen  
Markus Bader, Staatliche Berufsschule III Fürth  
Barbara Maier, Akademie Dillingen

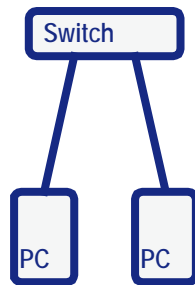
URL: <http://alp.dillingen.de/schulnetz>  
Mail: [schlagbauer@alp.dillingen.de](mailto:schlagbauer@alp.dillingen.de)  
Stand: Juli 2010

## Inhalt

Laborübung 01 - Analyse des Netzwerkverkehrs .....	4
Laborübung 02 - Verbindung zweier Netze .....	6
Laborübung 03 - Routing zwischen mehreren Netzen .....	10
Laborübung 04 - Anbindung an das Internet .....	12
Laborübung 05 - Einrichten einer Firewall .....	14
Laborübung 06 - Beschränkung des Internetzugangs auf einzelne Dienste .....	16
Laborübung 07 - Web-Zugriff über einen Proxy .....	18
Laborübung 08 - Zugriff aus dem Internet auf einen internen Server .....	20
Laborübung 09 - Zugriff aus dem Internet auf einen internen Server in der DMZ .....	22
Laborübung 10 - VPN-Verbindung in das Schulnetz .....	24
Laborübung 11 - IPSec-VPN zwischen zwei Netzen .....	28
Umgang mit einem Funkwerkrouter .....	32
Abschließende Aufgabe .....	34

## Laborübung 01 - Analyse des Netzwerkverkehrs

Zwei Computer sind über einen Switch verbunden. Der Netzwerkverkehr zwischen diesen beiden Computern soll protokolliert und analysiert werden. Um Nebeneffekte zu vermeiden, befinden sich keine weiteren Computer in diesem Netz.



### Aufgaben

1. Vergeben Sie den Computern statische IP-Adressen aus dem Bereich 192.168.0.0/24 und überprüfen Sie die Verbindung der beiden Computer auf IP-Ebene.
2. Richten Sie an einem der beiden Computer eine Freigabe ein und tauschen Sie über diese Freigabe Dokumente aus.
3. Analysieren Sie mit Hilfe des Netzwerkniffers Wireshark die Vorgänge im Netz:
  - ARP-Anfrage
  - Ping
  - Namensauflösung
  - SMB-Zugriff

### Hinweise

<code>arp -a</code>	Anzeige der ARP-Tabelle
<code>arp -d</code>	Löschen der ARP-Tabelle

### Protokolle

Unter Linux:	<code>/etc/protocols</code>
Unter Windows:	<code>C:\Windows\System32\drivers\etc\protocol</code>

### Ports/Portnummern

Unter Linux: /etc/services

Unter Windows: C:\Windows\System32\drivers\etc\services

<http://www.iana.org/assignments/port-numbers>

### Wireshark

<http://www.wireshark.org>

## Kontrollfragen zu Aufgabe 3

### ARP-Anfrage

Ziel-Mac-Adresse: \_\_\_\_\_

Quell-Mac-Adresse: \_\_\_\_\_

Welche Information wird angefragt? \_\_\_\_\_

### ARP-Antwort

Ziel-Mac-Adresse: \_\_\_\_\_

Quell-Mac-Adresse: \_\_\_\_\_

Wie lautet die angefragte Information? \_\_\_\_\_

### ICMP-Anfrage

In welches übergeordnete Protokoll ist das ICMP-Paket eingebettet? \_\_\_\_\_

### IP-Pakete

Ein IP-Paket wird an den IP-Stack übergeben. Woran erkennt der IP-Stack, an welches nachgeordnete Protokoll (z. B. TCP, UDP, ICMP) der Inhalt übergeben werden muss?

\_\_\_\_\_

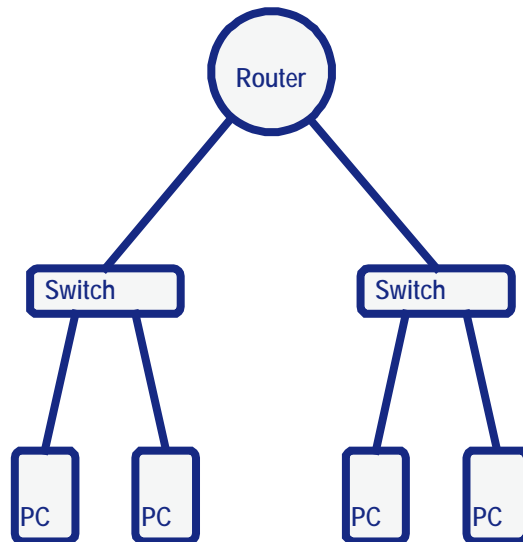
### Portnummern

Welchen Port verwendet die NetBIOS Namensauflösung? \_\_\_\_\_

Welche Ports werden für Windows-Freigaben verwendet? \_\_\_\_\_

## Laborübung 02 - Verbindung zweier Netze

Zwei Netze sollen über einen Router verbunden werden.



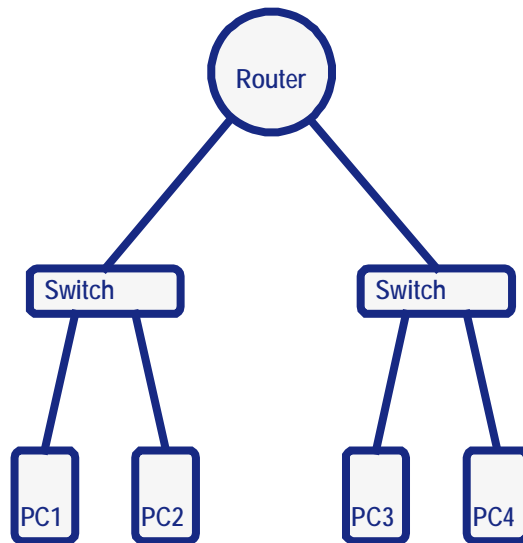
### Aufgaben

1. Tragen Sie in den oben dargestellten logischen Netzplan die IP-Adressen und Subnetzmasken der PCs und des Routers ein.
2. Verbinden Sie die Netze entsprechend der obigen Darstellung und konfigurieren Sie die Computer und den Router, so dass eine Kommunikation zwischen allen Computern möglich ist.
3. Pingen Sie von einem Computer aus alle anderen Computer an und werten Sie anschließend die ARP-Tabelle aus. Interpretieren Sie die Einträge.
4. Notieren Sie die Routingtabelle des Routers und interpretieren Sie diese.

Zieladresse	Subnetzmaske	Gateway	Schnittstelle	Metrik



### Ergänzende Übung



### Aufgaben

1. Beobachten Sie mit einem Netzwerkniffer einen Ping von PC1 zu PC4. Notieren Sie die MAC- und IP-Adressierungen der einzelnen Ping-Pakete (Ethernet-Frames).

#### Ethernet-Frame von PC1 zum Router

Ziel-MAC	Quell-MAC	Quell-IP	Ziel-IP

#### Ethernet-Frame vom Router zu PC4

Ziel-MAC	Quell-MAC	Quell-IP	Ziel-IP

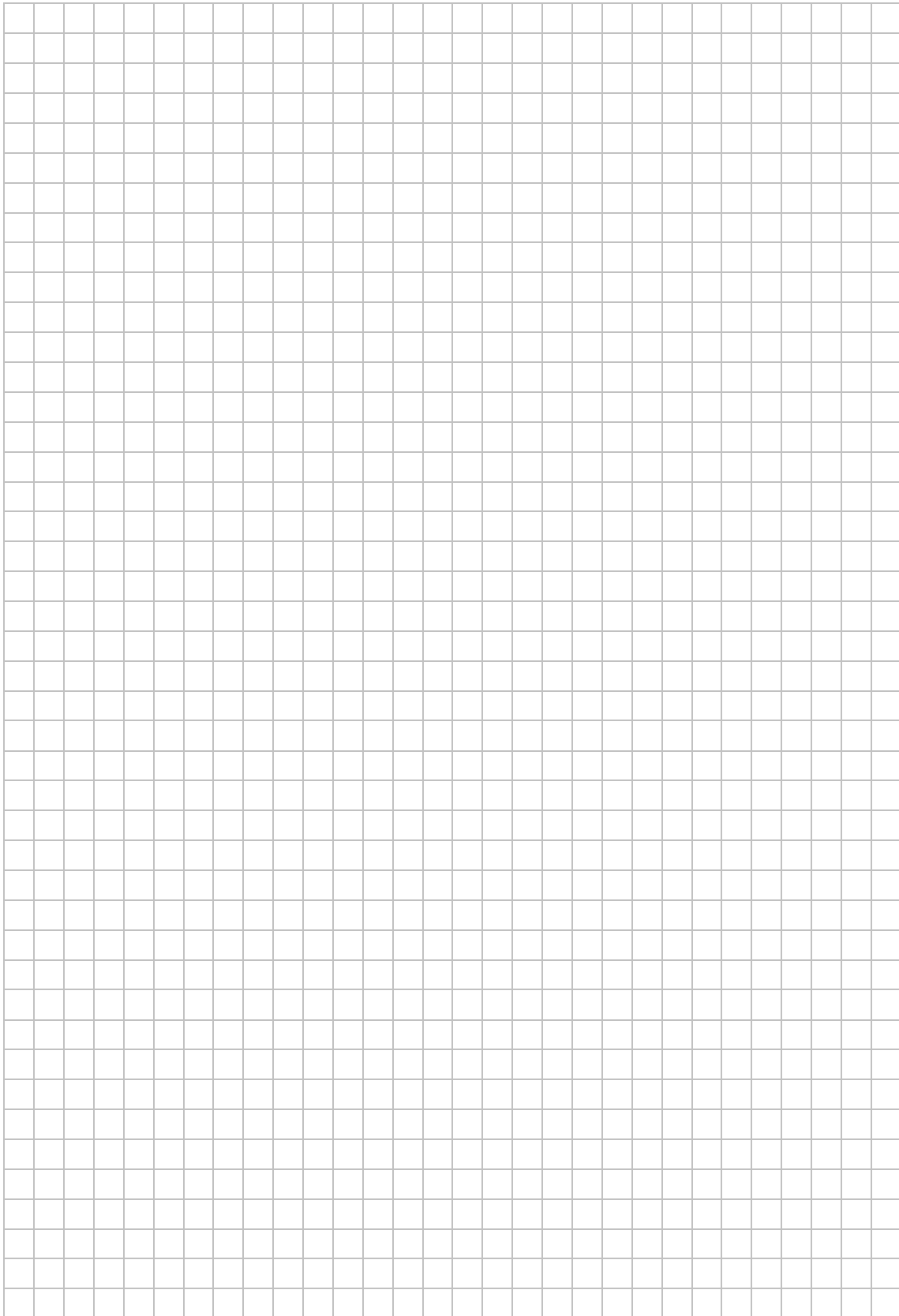
#### Ethernet-Frame von PC4 zum Router

Ziel-MAC	Quell-MAC	Quell-IP	Ziel-IP

#### Ethernet-Frame vom Router zu PC1

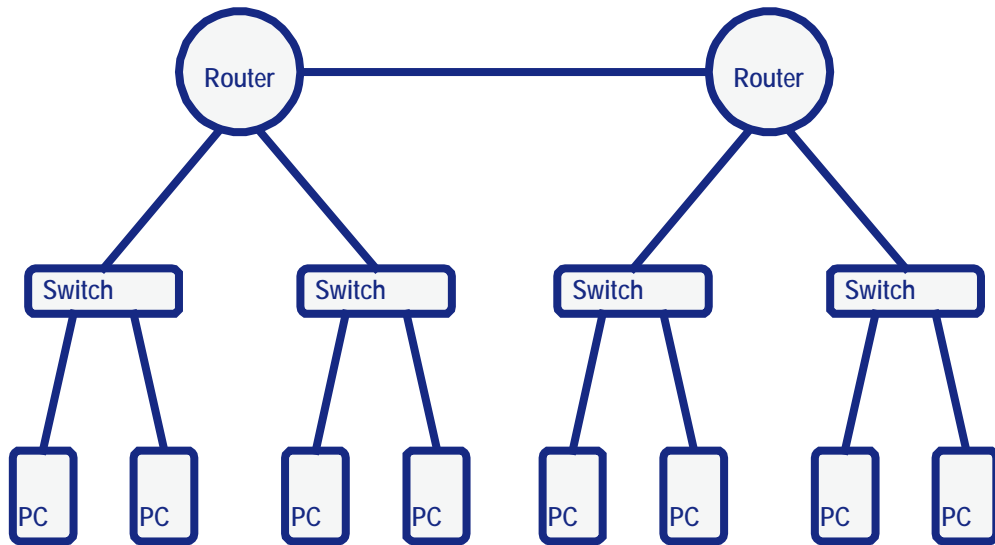
Ziel-MAC	Quell-MAC	Quell-IP	Ziel-IP

## Notizen



## Laborübung 03 - Routing zwischen mehreren Netzen

Mehrere Netze sollen über Router verbunden werden.



### Aufgaben

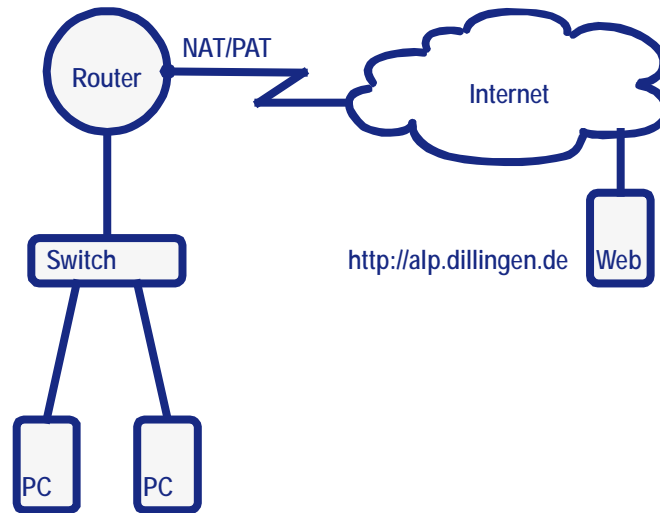
1. Fertigen Sie in Ihrer Gruppe anhand der obigen Skizze einen logischen Netzplan an und notieren Sie in diesem Netzplan alle relevanten IP-Einstellungen. Einigen Sie sich in Ihrer Gruppe wer für welches Netz und für welchen Router verantwortlich ist.
2. Konfigurieren Sie die Computer und Router entsprechend Ihrem Verantwortungsbereich und überprüfen Sie die Kommunikation zwischen allen Geräten.
3. Notieren Sie die Routingtabelle Ihres Routers und interpretieren Sie diese.

Zieladresse	Subnetzmaske	Gateway	Schnittstelle	Metrik



## Laborübung 04 - Anbindung an das Internet

Ein lokales Netz soll an das Internet oder an das Hausnetz angeschlossen werden.



### Aufgaben

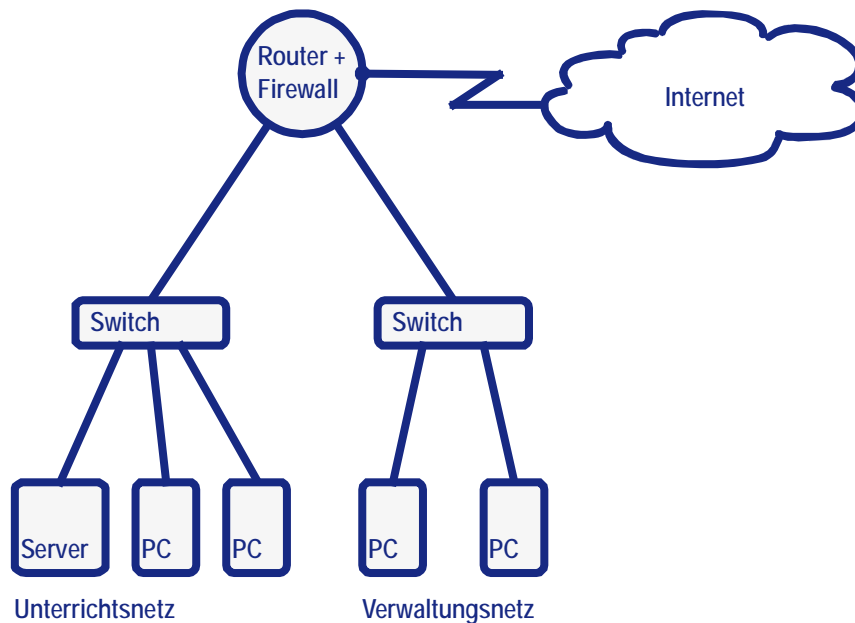
1. Beschriften Sie im obigen Netzplan die PCs, die Schnittstellen des Routers und gegebenenfalls den Webserver mit IP-Adressen.
2. Verbinden Sie den Router mit dem Internet bzw. dem Hausnetz und testen Sie, in wie weit die Verbindung funktioniert.
3. Aktivieren Sie am externen Interface die NAT/PAT-Funktion.
4. Surfen Sie im Internet auf die ALP-Webseiten. Lesen Sie anschließend am Router die Netzadressübersetzungstabelle aus und ergänzen Sie die nachstehende NAT-Tabelle:

Protokoll	Interne Adresse	Interner Port	Externe Adresse	Externer Port	Remote-Adresse	Remote Port
					194.95.207.10	80



## Laborübung 05 - Einrichten einer Firewall

Die Verwaltung der Schule und das pädagogische Netz sollen über denselben Zugangsrouten an das Internet angeschlossen werden. Der Informationsaustausch zwischen den beiden lokalen Netzen soll ausgeschlossen bzw. auf exakt festgelegte Szenarien beschränkt werden.



### Aufgaben

1. Schließen Sie ein zweites lokales Netz (z. B. Verwaltungsnetz) an den Router an, so dass beide Netze einen Internetzugang haben.
2. Zeigen Sie, dass beide lokale Netze gegenseitigen Zugriff aufeinander haben.
3. Richten Sie eine Firewall ein und unterbinden Sie jede Kommunikation zwischen dem Verwaltungsnetz und dem Unterrichtsnetz. Der Zugriff in das Internet soll aus beiden Netzen heraus möglich sein.
4. Öffnen Sie die Firewall so, dass der Zugriff vom Verwaltungsnetz in das Unterrichtsnetz möglich ist. Der Zugriff in die umgekehrte Richtung soll weiterhin durch die Firewall geblockt werden.

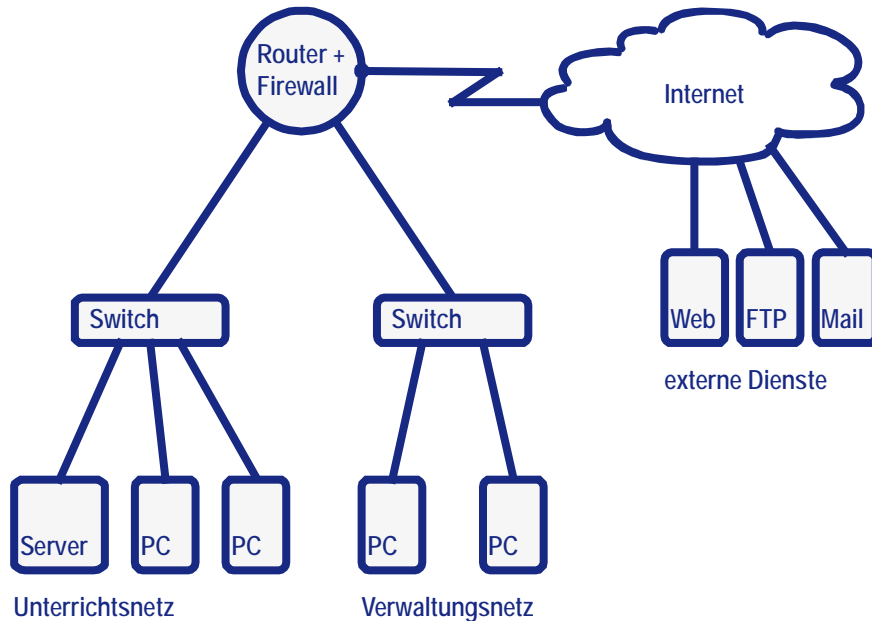
### Weiterführende Aufgabe

5. Beschränken Sie den Zugriff aus dem Verwaltungsnetz in das Unterrichtsnetz, so dass nur von einem Computer aus dem Verwaltungsnetz auf den Server im Unterrichtsnetz zugegriffen werden kann.
6. Beschränken Sie den Zugriff auf Ihren Router, so dass dieser nur von einem bestimmten Computer aus dem internen Netz konfigurierbar ist.



## Laborübung 06 - Beschränkung des Internetzugangs auf einzelne Dienste

Der Zugang zum Internet soll nach den Vorstellungen der Schule abgesichert werden. Es sollen deshalb nur die Dienste möglich sein, die im jeweiligen Netz benötigt werden.



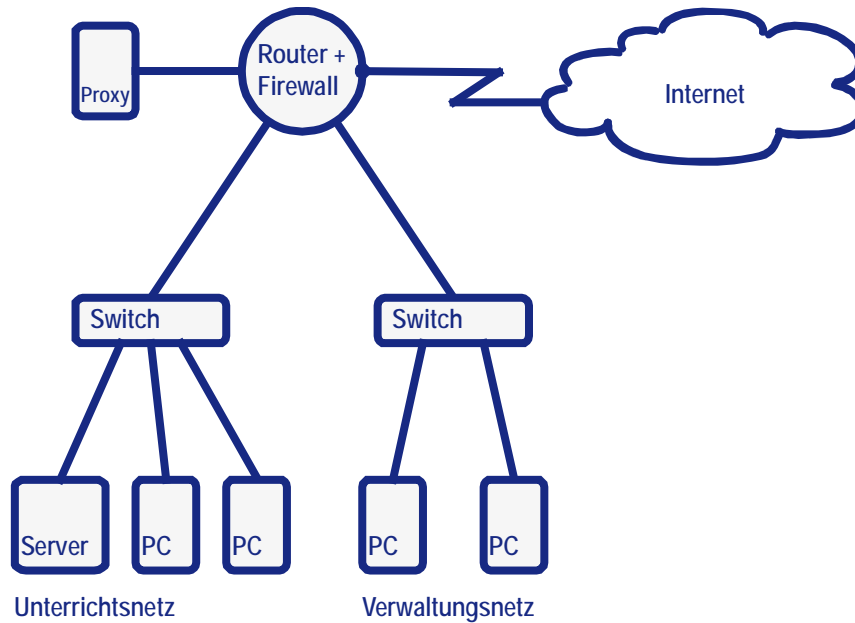
### Aufgaben

1. Beschränken Sie die Zugriffe vom Unterrichtsnetz in das Internet auf die Dienste http und https.
2. Zur Pflege des Webserver der Schule soll zusätzlich eine FTP-Verbindung zu diesem Webserver möglich sein. FTP-Verbindungen zu anderen Servern im Internet sind nicht erlaubt.
3. Ermöglichen Sie aus dem Verwaltungsnetz heraus die Nutzung von E-Mail (per SMTP, POP3 und IMAP).
4. Die Schulverwaltung verwendet ein Programm, das eine Verbindung zu einem Serverdienst im Internet aufbaut. Untersuchen Sie, welchen Port und welche Zieladresse dieses Programm verwendet und schalten Sie gezielt diese Verbindung frei.



## Laborübung 07 - Web-Zugriff über einen Proxy

Vom Unterrichtsnetz aus soll der Zugriff auf das Web nur über einen eingerichteten Proxy mit Content-Filterung möglich sein.



### Aufgaben

1. Testen Sie von einem Unterrichts-PC aus den Webzugriff über den Proxy und vergewissern Sie sich, dass beim Webzugriff über den Proxy der eingerichtete Content-Filter wirkt.
2. Sorgen Sie dafür, dass der Webzugriff über http und https nur noch über den Proxy funktioniert. Sperren Sie dazu alle anderen Zugriffsmöglichkeiten auf das Web.
3. Testen Sie Proxyserver mit verschiedenen Funktionalitäten:
  - Benutzerauthentifizierung
  - Protokollierung der Webzugriffe
  - Webfilter

### Hinweise

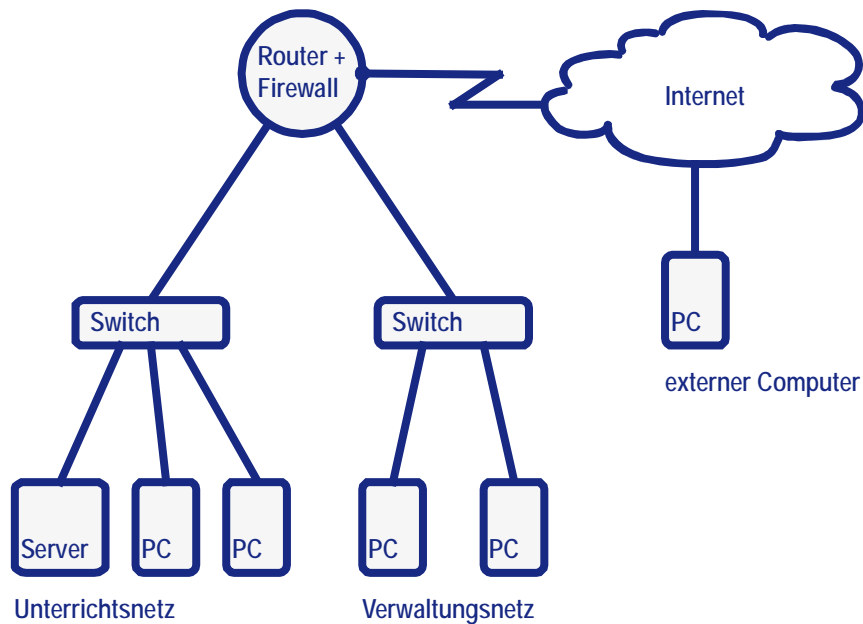
#### Normaler Proxy

Im Internet-Browser wird der Proxy eingetragen. Alle Webanfragen werden an den Proxy gesendet.



## Laborübung 08 - Zugriff aus dem Internet auf einen internen Server

Zur Remoteadministration soll auf einen internen Server zugegriffen werden.



### Aufgaben

1. Richten Sie am Router die Portweiterleitung so ein, dass über das RDP-Protokoll (TCP-Port 3389) auf den Server im Schulnetz zugegriffen werden kann.
2. Verbinden Sie sich von einem PC außerhalb Ihres Netzes über eine RDP-Verbindung mit Ihrem Schulserver.
3. Verschleiern Sie die Verbindung, indem Sie einen beliebigen anderen externen Port verwenden.

### Hinweise

#### Portweiterleitung (Port Forwarding)

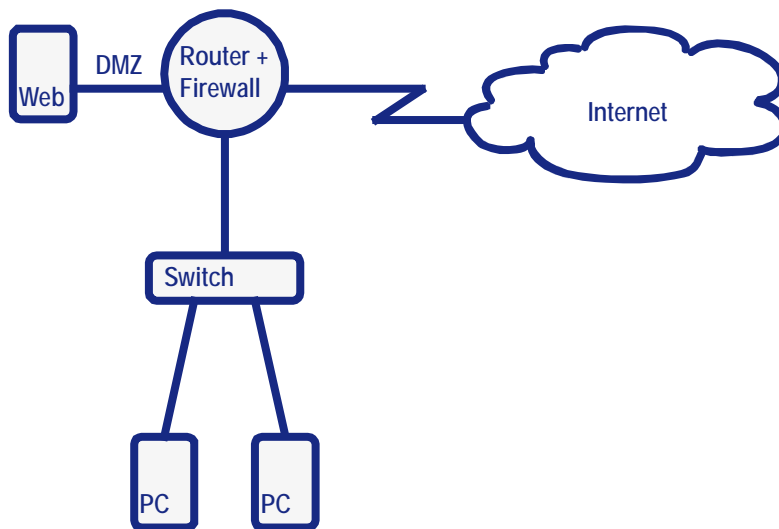
Um gezielt Verbindungen von außen zuzulassen (z. B. beim Betrieb eines öffentlich zugänglichen Webservers oder zur Fernadministration eines Servers), werden Zugriffe von außen auf bestimmte Ports der Zielrechner im internen Netz weitergeleitet.

Server, die von außen erreichbar sind, sind prinzipiell auch von außen angreifbar. Angriffe aus dem Internet erfolgen dabei üblicherweise, indem bekannte Sicherheitslücken der Serverdienste ausgenutzt werden oder durch ein automatisiertes Probieren von mehreren Tausend Benutzernamen- und Passwort-Kombinationen.



## Laborübung 09 - Zugriff aus dem Internet auf einen internen Server in der DMZ

Der Webserver der Schule soll aus dem Internet erreichbar sein.



### Aufgaben

1. Richten Sie eine DMZ (Demilitarisierte Zone) ein und installieren Sie auf einem Ihrer PCs einen Webserver in der DMZ. Richten Sie den Router so ein, dass ein Zugriff vom Internet aus auf den Webserver auf Port 80 möglich ist.

### Hinweise

Miniwebserver:

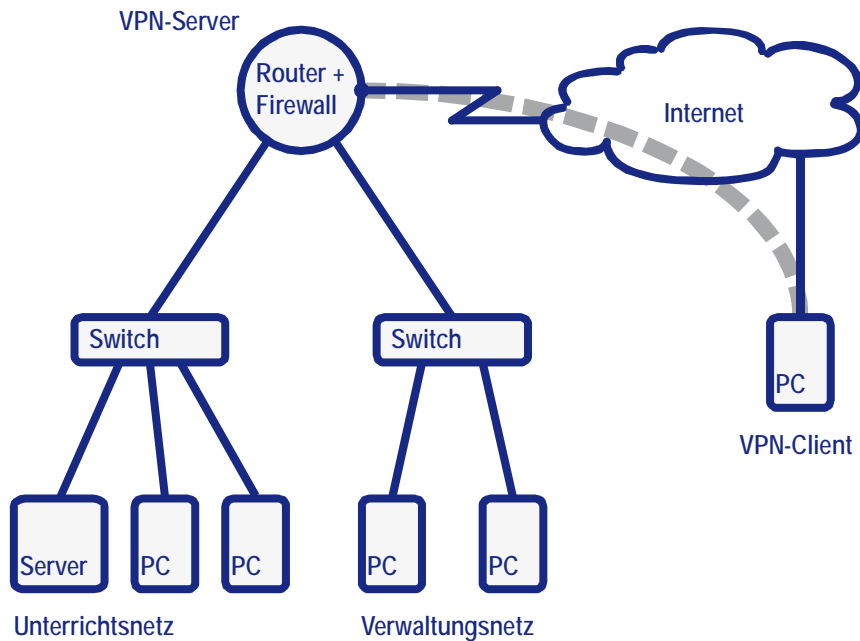
<http://www.aidex.de>

<http://www.pablosoftwaresolutions.com>



## Laborübung 10 - VPN-Verbindung in das Schulnetz

Von zu Hause aus soll eine gesicherte VPN-Verbindung (über das PPTP-Protokoll) in das Schulnetz eingerichtet werden.



### Aufgaben

1. Richten Sie den Router als PPTP-VPN-Server ein. Die Clients sollen bei der Verbindung eine IP-Adresse aus dem Unterrichtsnetz erhalten.
2. Bauen Sie von einem externen Client eine VPN-Verbindung auf und überprüfen Sie, auf welche internen Netze und PCs Sie zugreifen können.
3. Überprüfen Sie, auf welchem Weg der externe Client eine beliebige Internetverbindung aufbaut.

## Hinweise

Zur Umsetzung der Aufgaben kann folgende Konfiguration dienen:

Gerät/Schnittstelle	IP-Adresse	Subnetzmaske
PC-intern	172.20.0.100	255.255.0.0
PC-extern	10.36.16.x	255.255.255.0
PC-extern (VPN)	dhcp	dhcp
Router/extern	10.36.16.x	255.255.255.0
Router/intern	172.20.0.254	255.255.0.0
VPN-DHCP-Pool	172.20.0.10 - .0.20	255.255.0.0

Die IP-Adressen der externen Schnittstellen müssen an die Laborumgebung angepasst werden.

Bei VPN-Verbindungen von einem Client zu einem Einwahlserver wird am Client ein virtuelles Netzwerkinterface erstellt, das vom Einwahlserver nach dem Aufbau der Verbindung eine IP-Adresse erhält. Über dieses virtuelle Interface ist der Client Mitglied in einem anderen Netzwerk und kann auf die Clients und Ressourcen in diesem Netzwerk zugreifen.

### PPTP – Point to Point Tunneling Protocol

PPTP verwendet TCP-Port 1723 und das Protokoll GRE (Generic Routing Encapsulation).

### Authentifizierung

Client und Server müssen das gleiche Authentifizierungsprotokoll verwenden.

PAP	Password Authentication Protocol, Authentifizierung ohne Verschlüsselung
CHAP	Challenge Handshake Authentication Protocol, Verschlüsselte Authentifizierung
MS-CHAP v2	Microsoft-Implementierung von CHAP Version 2

### Troubleshooting

`debug ppp` & Überprüfung des Authentifizierungsvorgangs

### Weiterführende Hinweise

[http://www.funkwerk-ec.de/faq\\_bintec\\_228\\_pptp-verbinding\\_mit\\_fci\\_01\\_de.html](http://www.funkwerk-ec.de/faq_bintec_228_pptp-verbinding_mit_fci_01_de.html)

## VPN

VPN steht für „Virtual Private Network“ und meint damit eine virtuelle Verbindung zwischen zwei Computern oder Netzen über das Internet. Die Idee einer VPN-Verbindung ist es, dass z. B. ein Benutzer an seinem PC zu Hause Zugriff auf die Ressourcen am Arbeitsplatz hat.

Bei der VPN-Verbindung wird über das Internet eine verschlüsselte Verbindung (Tunnel) von einem VPN-Client zu einem VPN-Einwahlserver im Zielnetz aufgebaut. Dieser Server muss über eine öffentliche IP-Adresse aus dem Internet erreichbar sein.

Als Einwahlserver kann auch der Internetzugangsrouten dienen, falls dieser die Funktionalität unterstützt. Andernfalls werden am Internetzugangsrouten die entsprechenden Verbindungsanfragen zum VPN-Einwahlserver weitergeleitet (z. B. Port Forwarding).

Die Verschlüsselung erfolgt immer zwischen den beiden VPN-Kommunikationspartnern.

### Ziel einer VPN-Verbindung

Vertraulichkeit:	Der Inhalt der Nachricht ist geheim.
Authentizität:	Die Nachricht ist eindeutig vom angegebenen Absender.
Integrität:	Der Inhalt der Nachricht wurde nicht verändert.

### Site-to-End-VPN

Über einen VPN-Tunnel wird ein einzelner Computer in das Zielnetz eingebunden. Dieser Computer authentifiziert sich an einem Einwahlserver im Zielnetz und baut eine verschlüsselte Verbindung zu diesem Einwahlserver auf.

### Site-to-Site-VPN

Über einen VPN-Tunnel werden zwei Netze verbunden. Der Internetzugangsrouten in einem Filialnetz verbindet sich mit dem Einwahlserver im Unternehmensnetz. Die verschlüsselte Verbindung wird zwischen dem Internetzugangsrouten und dem Einwahlserver aufgebaut.

### End-to-End-VPN

Über einen VPN-Tunnel werden zwei Computer miteinander verbunden. Die verschlüsselte Verbindung wird zwischen den beiden Computern aufgebaut.

Eine Variante von End-to-End VPN-Verbindungen stellen auch externe Dienste, wie z. B. Hamachi oder Team-Viewer an, bei denen sich zwei Computer über einen vermittelnden Server im Internet verbinden.

## **VPN-Protokolle**

PPTP	Point to Point Tunneling Protocol (Layer 2)
L2TP	Layer 2 Forwarding (Layer 2)
IPSec	IP Security Protocol (Layer 3)
TLS/SSL	Transport Layer Security / Secure Sockets Layer (Layer 4-7), z. B. OpenVPN, SSL-Explorer
Proprietäre Protokolle (z. B. Hamachi, Teamviewer)	

### **PPTP**

Das PPTP-Protokoll ist in den Microsoft-Betriebssystemen bereits implementiert. Deshalb benötigt ein Windows-Client keine Zusatzsoftware, um sich mit einem PPTP-Einwahlknoten zu verbinden.

Der Verbindungsaufbau bei PPTP erfolgt über TCP Port 1723. Die Daten werden über das GRE-Protokoll (Generic Routing Encapsulation) verschlüsselt übertragen.

### **IPSec**

IPSec arbeitet auf der Schicht 3 des ISO/OSI-Modells. Die IP-Pakete werden verschlüsselt und in weitere IP-Pakete verpackt.

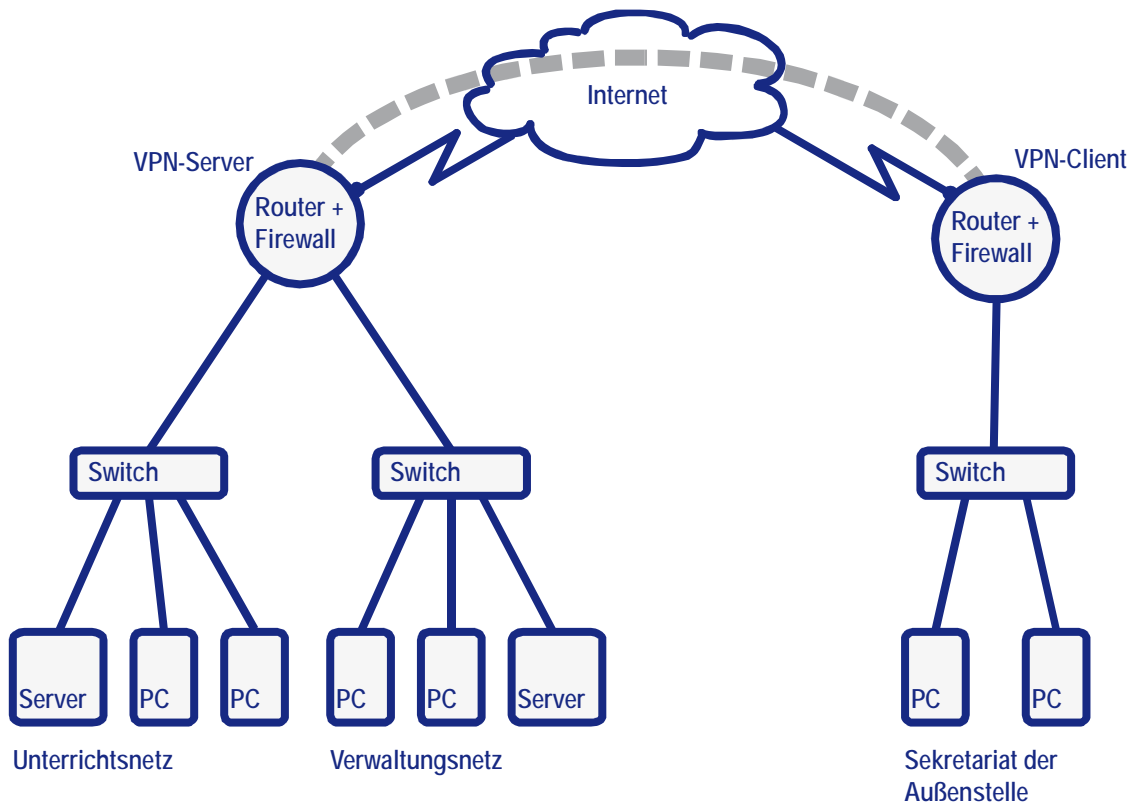
#### **Teilprotokolle von IPSec**

AH (Authentication Header)  
ESP (Encapsulation Security Payload)  
IKE (Internet Key Exchange)

## Laborübung 11 - IPSec-VPN zwischen zwei Netzen

Das Sekretariat der Außenstelle einer Schule soll über eine VPN-Verbindung an das Verwaltungsnetz der Schule angeschlossen werden. Die Außenstelle befindet sich an einem anderen Standort und ist über das Internet erreichbar.

Mit IPSec soll eine Site-to-Site-Verbindung zwischen dem Router der Schule und dem Router der Außenstelle hergestellt werden.



### Aufgaben

1. Richten Sie eine Grundkonfiguration der beiden Netze ein. Verzichten Sie zunächst auf Restriktionen durch eine Firewall. Beide Netze sollen Zugang zum Internet haben.
2. Richten Sie eine IPSec-Verbindung zwischen den beiden Routern ein (nutzen Sie dazu die Konfigurationshinweise) und ermöglichen Sie den Zugriff von der Außenstelle in das Verwaltungsnetz.

## Hinweise

### IPSec-Modi

Transportmodus: Host to Host - Kommunikation

Tunnelmodus: Site to Site - Kommunikation

### Konfiguration einer Site-to-Site-VPN unter IPSec mit PSK auf Bintec-Routern

Nach der Grundkonfiguration (Schnittstellen, IP-Adressen, Datum/Zeit) wird die eigentliche IPSec-VPN-Verbindung eingerichtet.

Diese besteht aus drei Schritten:

1. Verbindung zur Gegenstelle (IPSec-Peers)
2. Phase-1: Schlüsselaustausch
3. Phase-2: Datenübertragung

## Grundkonfiguration

### Router der Schule

Unterrichtsznetz:	192.168.1.0 /24
Gateway:	192.168.1.254
Verwaltungsnetz:	192.168.0.0 /24
Gateway:	192.168.0.254
Externe Schnittstelle:	10.36.16.x /24 (NAT)

### Router der Außenstelle

Sekretariat der Außenstelle:	192.168.100.0 /24
Gateway:	192.168.100.254
Externe Schnittstelle:	10.36.16.y /24 (NAT)

Datum und Uhrzeit müssen auf beiden Routern übereinstimmen. Die IP-Adressen der externen Schnittstellen müssen an die Laborumgebung angepasst werden.

## IPSec-Konfiguration

### Verbindung zur Gegenstelle (IPSec-Peers)

Bintec-Menü: VPN → IPSec → IPSec-Peers → Neu

	Router der Schule	Router der Außenstelle
Administrativer Status	Aktiv	Aktiv
Beschreibung	Verbindung zur Außenstelle	Verbindung zur Schule
Peer-Adresse	10.36.16.y	10.36.16.x
Peer-ID – FQDN:	Aussenstelle	Schule
Preshared Key	geheim	geheim
IP-Adressenvergabe	statisch	statisch
Standardroute	nicht markiert	nicht markiert
Lokale IP-Adresse	192.168.0.254	192.168.100.254
Routeneinträge	192.168.100.0/255.255.255.0	192.168.0.0/255.255.255.0
Erweiterte Einstellungen		
Startmodus	auf Anforderung	immer aktiv
Phase-1-Profile	* <i>Profilname aus Phase 1</i>	* <i>Profilname aus Phase 1</i>
Phase-2-Profile	* <i>Profilname aus Phase 2</i>	* <i>Profilname aus Phase 2</i>

\* nach Konfiguration der Phase-1- und -2-Profile werden die Profile hier eingetragen  
Bei allen weiteren Einstellungen kann die Vorgabe belassen werden.

### Phase-1: Schlüsselaustausch

Bintec-Menü: VPN → IPSec → Phase-1-Profile → Neu / Phase-1-Parameter (IKE)

	Router der Schule	Router der Außenstelle
Beschreibung	<i>Profilname</i>	<i>Profilname</i>
Proposals	AES-256 / MD5	AES-256 / MD5
DH-Gruppe	2 (1024 Bit)	2 (1024 Bit)
Lebensdauer	14400 Sekunden	14400 Sekunden
Authentifizierungsmethode	Preshared Keys	Preshared Keys
Modus	aggressiv	aggressiv
Lokaler ID-Typ	Full Qualified Domain Name	Full Qualified Domain Name
Lokaler ID-Wert	Schule	Aussenstelle
Erweiterte Einstellungen		
NAT-Transversal	aktiv	aktiv

Bei allen weiteren Einstellungen kann die Vorgabe belassen werden.



## Umgang mit einem Funkwerkrouter

### Konfigurationszugang

Die Konfiguration eines Routers kann über verschiedene Zugriffsmöglichkeiten erfolgen:

- Webinterface (http oder https)
- Telnet oder SSH
- SNMP (Simple Network Management Protocol)
- Konsole (serielle Schnittstelle; Terminal-Emulator)

### Konsolenverbindung

Eine Konsolenverbindung hat den Vorteil, dass sie unabhängig von Netzwerkeinstellungen funktioniert. Diese Möglichkeit bieten in der Regel nur professionelle Router.

Zur Kommunikation dienen Terminal-Emulatoren z. B.:

- Hyper Terminal
- Putty
- Tera Term

Damit ein Computer und ein Router miteinander über die serielle Schnittstelle kommunizieren können, müssen die Übertragungsparameter beider Geräte übereinstimmen.

Bits pro Sekunde (Baudrate)	9600
Datenbits	8
Parität	Keine
Stoppbits	1
Flusssteuerung	Keine

Die Baudrate (Speed) beschreibt die Geschwindigkeit der Übertragung.

Durch die Angabe der Datenbits wird festgelegt, wie viele Bits pro Zeichen übertragen werden.

Das Paritätsbit dient zur Erkennung von Fehlern bei der Datenübertragung.

Das Stoppbit legt fest, wie lange nach dem Senden eines Zeichens gewartet werden soll, bis das nächste Zeichen übertragen wird.

Durch die Flusssteuerung stimmen sich die zwei Geräte ab, ob der jeweils andere gerade bereit zum Datenempfang ist.

### Standardzugang im Auslieferungszustand

Login: admin  
Password: funkwerk

### Zurücksetzen des Funkwerkroueters in den Auslieferungszustand

Nach dem Starten des Routers muss der Bootvorgang durch drücken der Leertaste (Space-Taste) unterbrochen werden:

```
Press <sp> for boot monitor or any other key to boot system
```

Danach erscheint ein Auswahlmenü:

```
(1) Boot System
...
(4) Delete Configuration
```

### Ausgewählte Kommandozeilenbefehle

halt	Neustart
setup	Halbgrafische Bedienoberfläche
netstat -i	Anzeige der Interfaces
netstat -r	Routingstabelle
cmd=save	Speichern der Konfiguration
ipNatTable	Anzeigen der NAT-Tabelle
t 0	Timeout (autologout) abschalten
nslookup	DNS-Namensauflösung
ping	Diagnosewerkzeug auf IP-Ebene
ifconfig -h	Zeigt alle Parameter zum Befehl ipconfig an
debug all &	Das & lässt eine weitere Eingabe zu.
exit	Abmelden
?	Hilfe

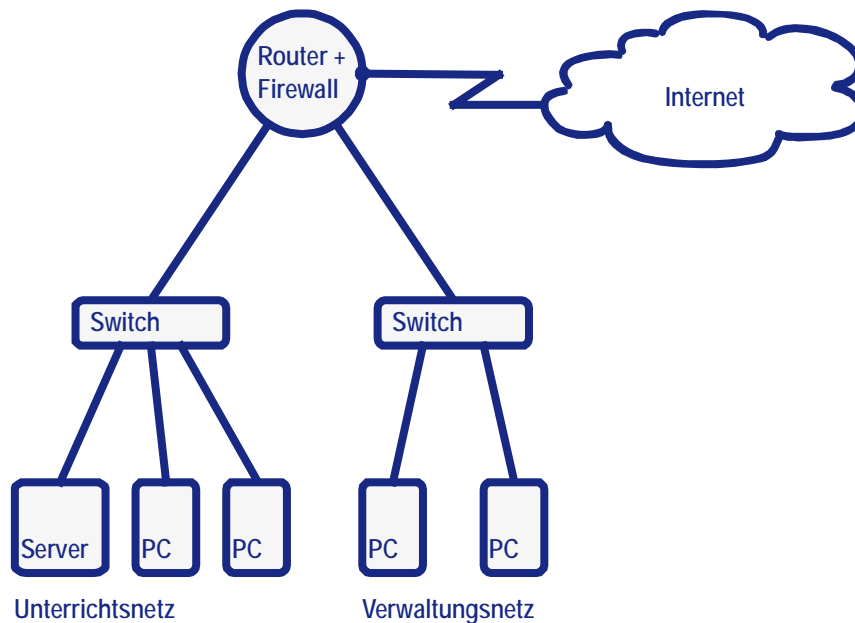
### Web-Zugriff

Die Konfiguration des Routers erfolgt in der Regel über die Web-Oberfläche. Nach dem Zurücksetzen des Routers bzw. in der Standardkonfiguration ist der Router auf der interne Schnittstelle (en1-0, Port 1-4) unter der IP-Adresse 192.168.0.254 erreichbar.

```
Login: admin
Password: funkwerk
```

## Abschließende Aufgabe

Unterrichts- und Verwaltungsnetz der Schule sind zwei getrennte Netze, zwischen denen kein Zugriff möglich sein soll. Beide Netze nutzen einen gemeinsamen Internetzugang. Der Internetzugang aus dem Unterrichtsnetz heraus soll nur über einen Content-Filter möglich sein.



### Aufgaben

1. Richten Sie die beiden Netze so ein, dass der Internetzugang funktioniert. Der Router soll dabei als DHCP-Server und DNS-Relay für die angeschlossenen Netze fungieren.
2. Aktivieren Sie die Firewall, so dass zunächst alle Verbindungen über den Router hinweg blockiert werden.
3. Ermöglichen Sie beliebige Verbindungen aus dem Verwaltungsnetz ins Internet.
4. Ermöglichen Sie aus dem Unterrichtsnetz heraus TCP-Verbindungen auf Port 3128 zum Server 10.36.104.53 (Proxy mit Filter) und testen Sie die Funktionalität. Andere Verbindungen sollen aus dem Unterrichtsnetz heraus nicht möglich sein.

### Zusatzaufgabe

5. Ermöglichen Sie einem externen Client den RDP-Zugriff auf den Server im Unterrichtsnetz.