Akademie
für Lehrerfortbildung
und Personalführung

Grundlagen der Schulvernetzung

SCHULNETZ

Qualifizierung von Systembetreuerinnen und Systembetreuern

INHALT

IMPRESSUM

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

Autoren: Georg Schlagbauer, Akademie Dillingen
Barbara Maier, Akademie Dillingen
Peter Botzenhart, Akademie Dillingen

URL: https://alp.dillingen.de/schulnetz
Mail: schlagbauer@alp.dillingen.de
Stand: Juli 2021

LABORÜBUNG 01 - ANALYSE EINES NEUEN COMPUTERS

Szenario

Ein Computer soll hinsichtlich seiner Ausstattung und Funktionsfähigkeit analysiert werden.

Vorbereitung

- Ein PC mit installiertem Betriebssystem
- ggf. BIOS-Passwort

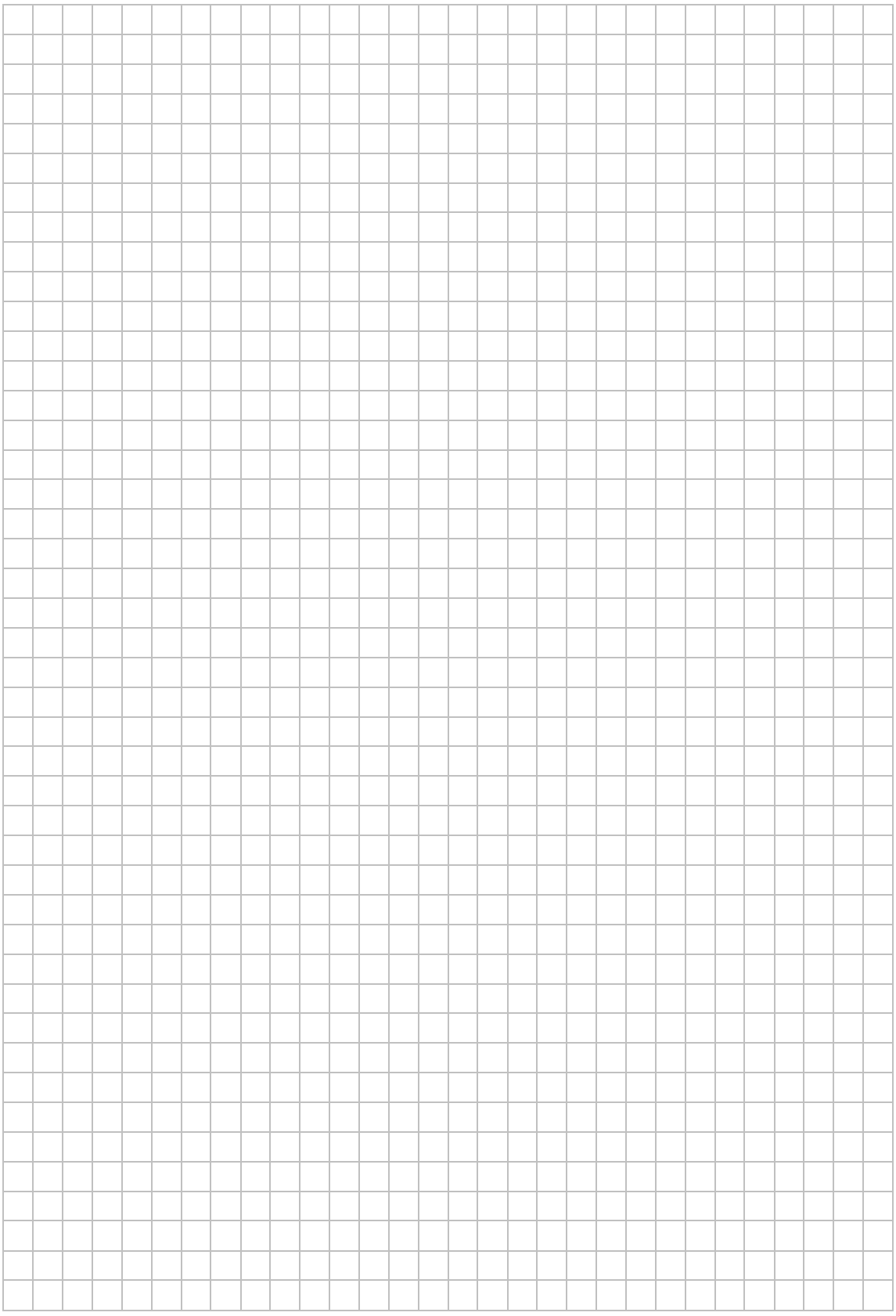
Aufgaben

1. Identifizieren Sie die von außen sichtbaren Schnittstellen (Netzwerkanschluss, USB, Grafikschnittstellen).
2. Informieren Sie sich über die Möglichkeiten, den Bootvorgang zu unterbrechen, um in das Setup zu gelangen oder um die Bootreihenfolge zu beeinflussen. Notieren Sie die verschiedenen Bootmöglichkeiten des Computers (z. B. Festplatte, CD/DVD, USB, Netzwerk).
3. Stellen Sie fest, ob der Computer im BIOS- oder UEFI-Modus bootet.

Weiterführende Aufgaben

4. Identifizieren Sie die von außen sichtbaren Schnittstellen (z. B. Netzwerkanschluss, USB) und die nicht sichtbaren Schnittstellen (z. B. WLAN, Bluetooth, Mobilfunk) Ihres Notebooks, Tablets oder Smartphones.

Ihre Notizen



HINWEISE

Aufrufen des BIOS-/UEFI-Setup und des Bootmenüs

Beim Hochfahren eines PCs wird in der Regel im unteren Bildschirmbereich angezeigt, mit welcher Taste oder Tastenkombination das BIOS-/UEFI-Setup aufgerufen werden kann und wie die temporäre Bootreihenfolge, z. B. Starten von USB-Stick, PXE-Boot, Festplatte geändert werden kann. Je nach BIOS-/UEFI-Hersteller unterscheiden sich die Angaben z. B. F1, F2, ESC, ENTF, Strg+Alt+Esc, ….

Dauerhafte Änderung der Bootreihenfolge

Im BIOS/UEFI können einzelne Boot-Medien aktiviert bzw. deaktiviert werden und die Bootreihenfolge dauerhaft eingestellt werden.

Auswahl des Boot-Modus (BIOS/UEFI)

Der BIOS-Modus (Legacy-Modus, Booten über Master Boot Record (MBR)) ist der traditionelle Boot-Modus. Das BIOS ist für die Erkennung der Hardware-Komponenten, für die Konfiguration der Hardware sowie für den Start des Betriebssystems verantwortlich. Seit 2012 wird bei allen Computern (im Regelfall) der BIOS-Nachfolger UEFI eingesetzt. Der UEFI-Modus (Booten über GUID Partition Tables (GPT)) bietet zusätzliche Möglichkeiten z. B. Unterstützung größerer Festplatten, mehr Partitionen, Secure Boot, vereinfachte Parallelinstallation von Windows und Linux.

Eine genauere Übersicht über die Unterschiede zwischen BIOS und UEFI finden Sie in der Schulnetz-Veröffentlichung *„BIOS und UEFI – Einführung und Unterschiede“* unter https://schulnetz.alp.dillingen.de/materialien/UEFI.pdf.

Secure-Boot

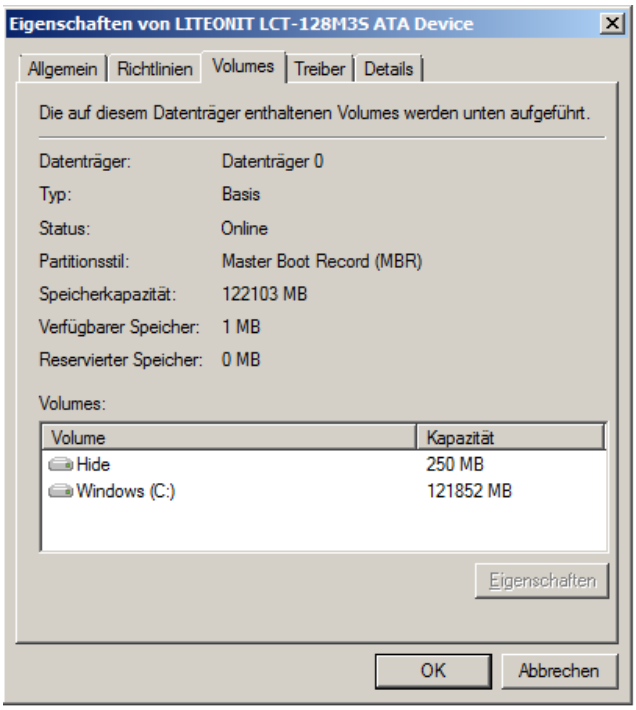
Secure-Boot verhindert das Booten von externen Medien. Aktiviertes Secure-Boot verhindert die Umstellung auf den Legacy-BIOS-Modus. Eventuell ist für das Einschalten des Secure-Boots das Setzen eines Passworts im UEFI erforderlich.

Virtualisierung

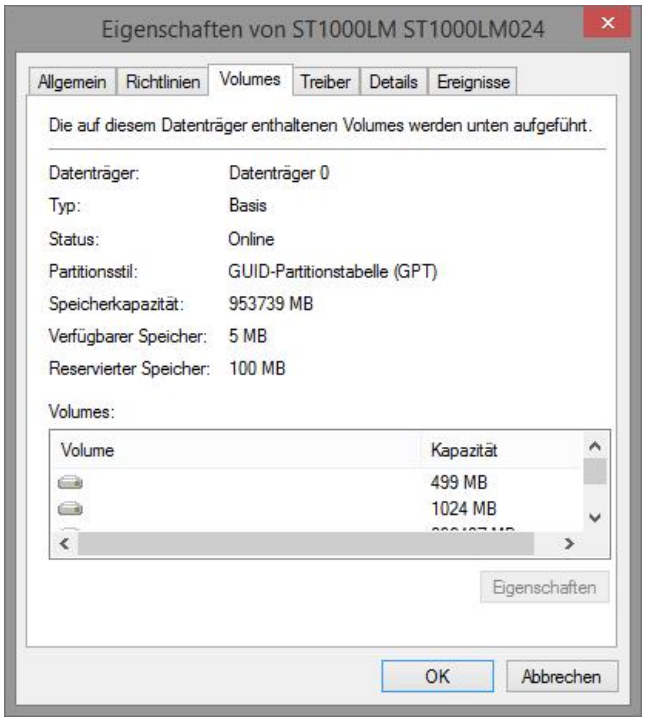
Einige Virtualisierungssysteme (z. B. Microsoft Hyper-V) erfordern es, dass die CPU die Virtualisierung unterstützt. Aktuelle Prozessoren unterstützen das in der Regel.

Anzeige des Boot-Modus unter Windows

Unter Windows lässt sich in der Datenträgerverwaltung erkennen, welcher Boot-Modus auf dem System verwendet wird.



Im BIOS-Legacy-Modus ist die Partitionierung der Festplatte im MBR festgelegt.

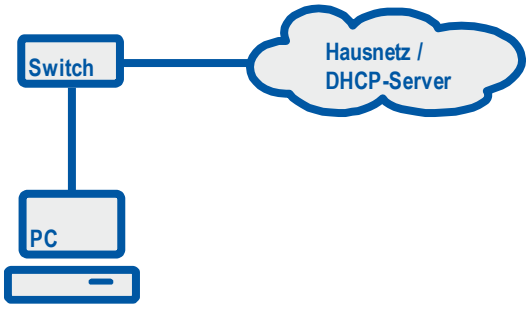


Im UEFI-Modus ist die Partitionierung der Festplatte in der GUID-Partitionstabelle festgelegt.

LABORÜBUNG 02 - ANBINDUNG AN DAS HAUSNETZ PER DHCP

Szenario

Ein Computer wird an ein lokales Netz angeschlossen. Die per DHCP erhaltenen Netzwerkeinstellungen sollen ermittelt werden.

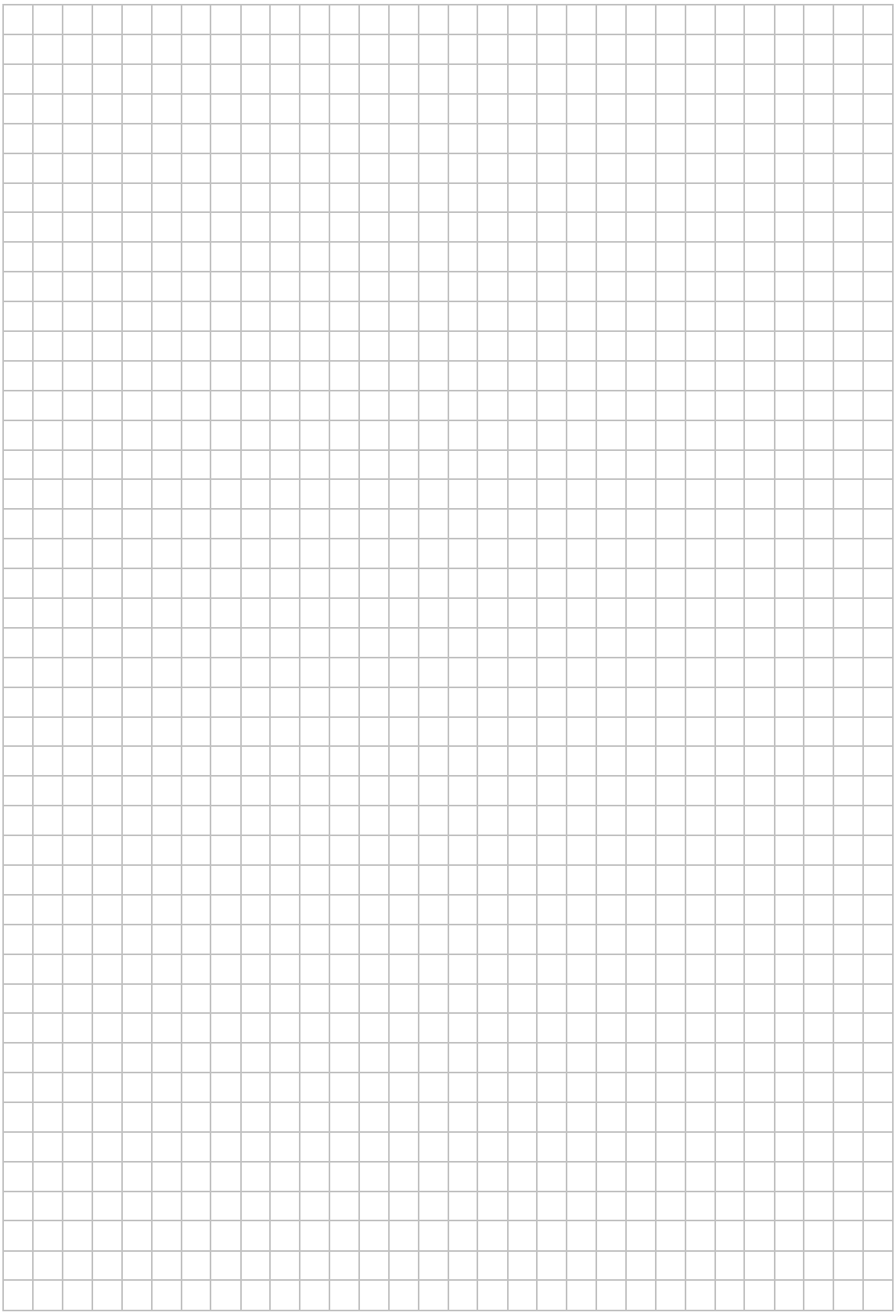


Aufgaben

1. Konfigurieren Sie ggf. Ihren Computer so, dass dieser per DHCP die IP-Konfiguration erhält.
2. Notieren Sie sich die Netzwerkeinstellungen Ihres Computers:

   - IP-Adresse
   - Subnetzmaske
   - Standardgateway
   - DNS-Server
   - DHCP-Server
   - MAC-Adresse
3. Überprüfen Sie die Erreichbarkeit des Standardgateways und eines Web-Servers im Internet auf IP-Ebene (z. B. `ping alp.dillingen.de`).
4. Überprüfen Sie die Namensauflösung verschiedener Webseiten mit unterschiedlichen DNS-Servern (z. B. nslookup).
5. Überprüfen Sie die Erreichbarkeit Ihres Nachbarcomputers auf IP-Ebene. (Beachten Sie ggf. die Firewall-Einstellungen des Nachbarcomputers).
6. Interpretieren Sie die Ausgaben von `ipconfig` in folgenden Fällen:
   a) Am Computer ist kein Netzwerkkabel angeschlossen.
   b) Der Computer ist an einem Switch angeschlossen, der DHCP-Server ist aber nicht erreichbar.

Ihre Notizen



HINWEISE

Netzwerkkonfiguration unter Windows

Systemsteuerung – Netzwerk und Internet – Netzwerk- und Freigabecenter

`ipconfig`	Anzeige der lokalen IP-Einstellungen
`ipconfig /all`	Ausführliche Konfigurationsinformationen
`ipconfig /release`	Die aktuelle DHCP-Zuweisung für alle Netzwerk-Schnittstellen (Interfaces) wird freigegeben.
`ipconfig /renew`	Die DHCP-Zuweisung aller Netzwerk-Schnittstellen wird erneuert.

Netzwerkkonfiguration unter Linux

`ifconfig`	Anzeige der lokalen IP-Einstellungen
`dhclient`	Erneuerung der DHCP-Zuweisung

Verbindungstest mit ping (IPv4)

`ping <IP-Adresse>`	Verbindungstest auf IP-Ebene
`ping 127.0.0.1`	Testet die korrekte Implementierung des TCP/IP-Stack auf dem eigenen Rechner.
`ping localhost`	Testet die korrekte Implementierung des TCP/IP-Stack und die korrekte Namensauflösung auf dem eigenen Rechner.
`ping 192.168.1.10`	Überprüft eine Verbindung auf IP-Ebene zu einem Rechner mit der angegebenen IP-Adresse.
`ping alp.dillingen.de`	Überprüft die Namensauflösung und die Verbindung auf IP-Ebene zu einem Rechner mit der angegebenen IP-Adresse.

Namensauflösung mit nslookup

`nslookup <name>`	Abfrage eines DNS-Namens (eingetragener DNS-Server wird verwendet)
`nslookup <name> <DNS-Server>`	Abfrage eines DNS-Namens mit Angabe des zu verwendenden DNS-Servers

`nslookup alp.dillingen.de`

IP-Adresse – MAC-Adresse – ARP-Protokoll

Jede Netzwerkkarte besitzt eine weltweit eindeutige MAC-Adresse. Diese MAC-Adresse wird zur Kommunikation im lokalen Netz benötigt. Die Abfrage nach der MAC-Adresse erfolgt mit dem Address Resolution Protocol (ARP). Auf eine ARP-Anfrage muss ein Computer selbst bei eingeschalteter Firewall antworten.

`arp -a`	Liest die Tabelle mit den Zuordnungen von IP-Adressen zu MAC-Adressen im lokalen Netz auf.
`arp -d`	Die Einträge in der arp-Tabelle werden gelöscht.

Verbindung zum Nachbarcomputer bei eingeschalteter Firewall

In einem lokalen Netz kann grundsätzlich jeder Computer mit jedem anderen Computer kommunizieren. Auch wenn ein Computer die lokale Windows-Firewall (z. B. ohne Ausnahmen) aktiviert hat und dadurch auf einen ping scheinbar nicht mehr reagiert, findet trotzdem eine Kommunikation über das arp-Protokoll statt.

`ping <Nachbarcomputer>`	keine Reaktion (100 % Verlust, wenn Firewall aktiv)
`arp -a`	Anzeige der IP-Adresse und der MAC-Adresse des Nachbarcomputers.

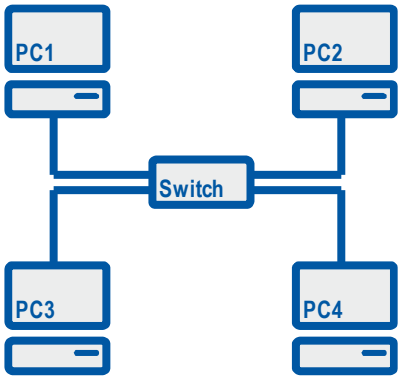
APIPA-Adressen

Um auch ohne DHCP-Server mit dynamisch zugewiesenen IP-Adressen kommunizieren zu können, werden zufällig ausgewählte Adressen aus dem APIPA-Adressbereich 169.254.0.0/16 (Automatic Private IP Addressing) verwendet. APIPA-Adressen deuten darauf hin, dass der DHCP-Server nicht erreichbar ist oder auf den seltenen Fall, dass es einen IP-Adressen-Konflikt gibt

LABORÜBUNG 03 - LOGIK DER IP-ADRESSIERUNG

Szenario

Mehrere Computer sollen miteinander vernetzt werden. Die Erreichbarkeit der Computer bei unterschiedlichen IP-Einstellungen wird getestet.



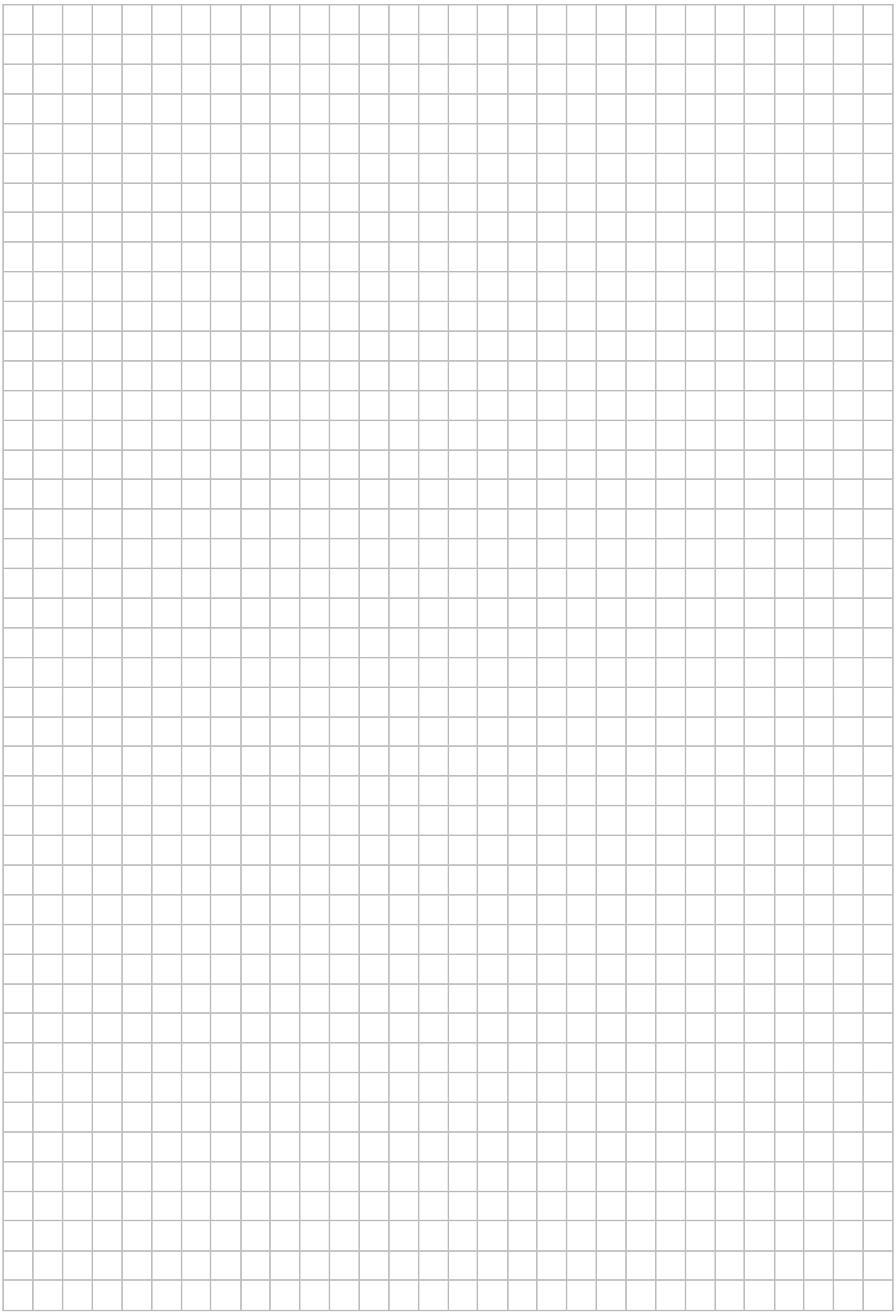
Vorbereitung

- Switch
- geeignete Twisted-Pair-Kabel
- 3 oder 4 Computer zum Vernetzen

Aufgaben

1. Verbinden Sie jeweils 3 oder 4 Computer über einen Switch und überprüfen Sie am Signalzustand der LEDs, ob ein Link vorhanden ist.
2. Vergeben Sie IP-Adressen aus dem Netzwerk 192.168.1.0/24 und testen Sie die Verbindung der Computer auf IP-Ebene. Sorgen Sie dafür, dass der ping nicht durch die Firewall blockiert wird.
3. Ordnen Sie einem Rechner eine IP-Adresse aus dem Netzbereich 192.168.2.0/24 zu und testen Sie die Verbindungen auf IP-Ebene.
4. Ändern Sie die Subnetzmaske an allen Rechnern auf 255.255.0.0 ab und testen Sie die Verbindungen.

Ihre Notizen



HINWEISE

Aufbau einer IP-Adressen

Eine IP-Adresse (IPv4) besteht aus 4 Byte = 32 Bit (in Zukunft aus 16 Byte; IPv6). Jedes Byte kann einen Wert zwischen 0 und 255 annehmen. Für die Darstellung in Dezimalform wird die IP-Adresse in vier Oktette unterteilt.

	1. Oktett	2. Oktett	3. Oktett	4. Oktett
IP-Adresse	192	168	1	10

IP-Adresse und Subnetzmaske

Eine IP-Adresse enthält einen Netzanteil und einen Hostanteil. Der Netzanteil dient der Wegfindung, der Hostanteil der Zustellung zu einem bestimmten Computer im Zielnetz. Die Trennung von Netz- und Hostanteil erfolgt mit Hilfe der Subnetzmaske.

Wird z. B. der IP-Adresse 192.168.1.10 die Subnetzmaske 255.255.255.0 zugeordnet, so bedeutet dies, dass sich der Computer im Netz 192.168.1.0 befindet und die "Hausnummer" 10 besitzt. Die Subnetzmaske 255.255.255.0 kann auch mit /24 (Anzahl der binären 1-bits) abgekürzt werden.

	Netz-Anteil			Host-Anteil
IP-Adresse	192	168	1	10
Subnetzmaske	255	255	255	0

Kommunikation zwischen Computern

Computer, die sich im gleichen Netz befinden, können direkt miteinander kommunizieren. Computer in unterschiedlichen Netzen benötigen einen Router, der die Datenpakete von einem Netz in das andere Netz weiterleitet.

Klasseneinteilung von IP-Adressen

In der Vergangenheit wurden IP-Adressen in Klassen (A, B, C) aufgeteilt. Diese Unterscheidung ist durch die Verwendung von Subnetzmasken überflüssig geworden.

Private IP-Adressen

Bestimmte IP-Adressen sind für die Nutzung innerhalb von LANs vorgesehen. Diese privaten IP-Adressen stehen weltweit allen Nutzern zur Verfügung. Da eine IP-Adresse immer eindeutig sein muss, werden diese Adressen nicht im Internet verwendet.

Privater Adressbereich	Standard-Subnetzmaske
10.0.0.0 - 10.255.255.255	255.0.0.0
172.16.0.0 - 172.31.255.255	255.255.0.0
192.168.0.0 - 192.168.255.255	255.255.255.0

Multicast-Adressen

Um mehrere Computer gleichzeitig ansprechen zu können (z. B. bei Videoübertragungen oder beim Klonen mehrerer Computer), weisen diese Programme den beteiligten Computern zusätzlich eine Multicast-Adresse zu.

Adressbereich: 224.0.0.0 - 239.255.255.255

Loopback-Adressen

Mit einer Loopback-Adresse wird der eigene Computer angesprochen. Üblicherweise wird dazu die Adresse 127.0.0.1 verwendet.

Loopback-Adressen: 127.0.0.1 - 127.255.255.254

Broadcast Adressen

Die Kommunikation innerhalb eines Netzes erfordert auch Rundspruch-Nachrichten an alle Geräte. Broadcasts werden von Routern nicht an andere Netze weitergeleitet. Innerhalb eines Netzes spricht man deshalb von einer Broadcast-Domäne. Als Broadcast-Adresse ist immer die letzte IP-Adresse des Netzwerkadressbereiches definiert.

Broadcast-Adresse des Netzes 192.168.1.0/24:	192.168.1.255
Allgemeine Broadcast-Adresse:	255.255.255.255

APIPA- oder Zeroconf-Adressen

Um auch ohne DHCP-Server mit dynamisch zugewiesenen IP-Adressen kommunizieren zu können, werden zufällig ausgewählte Adressen aus dem APIPA-Adressbereich 169.254.0.0/16 (Automatic Private IP Addressing) verwendet. APIPA-Adressen deuten darauf hin, dass der DHCP-Server nicht erreichbar ist oder auf den seltenen Fall, dass es einen IP-Adressen-Konflikt gibt

IPv6 Adressen

Aufgrund der herrschenden Adressknappheit im Internet wurde bereits vor Jahren der Nachfolger IPv6 konzipiert. Dadurch soll das Problem des knappen Adressraums gelöst werden. Jedes Gerät mit einer aktiven Netzwerkschnittstelle weist sich automatisch für diese Schnittstelle eine IPv6 Adresse zu.

IPv6 Adressen bestehen nicht wie IPv4 Adressen aus 4 Oktetten, sondern aus 8 Blöcken (getrennt durch Doppelpunkte) zu je 16 Bit. Das entspricht einer Länge von 128 Bit. Wegen der sperrigen Darstellung im Binärformat greift man auf eine Darstellung im Hexadezimalformat (HEX) zurück. Eine Verkürzung der Darstellung ist möglich.

Eine Beispielhafte IPv6 Adresse könnte so aussehen:

2001:0DB8:AC47:0000:FEC0:8303:A0C8:DC18.

Die ersten 64 Bit bilden das Präfix, die letzten 64 Bit bilden den Interface-Identifier („Host-Anteil“).

Kabelgebundene Netzwerkgeräte

Hub

Hubs bieten die Möglichkeit der einfachen Verbindung von Geräten per LAN-Kabel. Sie leiten die Nachrichten einfach an alle angeschlossenen Geräte weiter. In heutigen Netzwerken sollten sie nicht mehr eingesetzt werden.

Switch

Switche bilden heute die zentralen Netzwerkknoten. Sie leiten anhand der MAC-Adresse die Nachrichten zielgerichtet an die angeschlossenen Geräte weiter. Dadurch wird der Netzwerkverkehr im Vergleich mit einem Hub deutlich reduziert.

Router

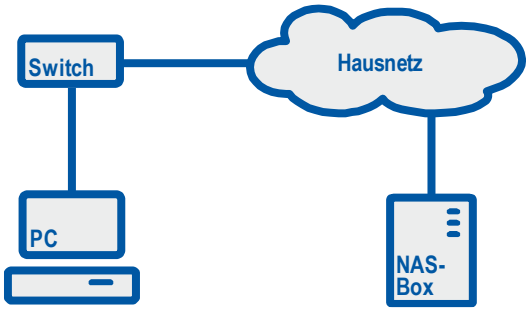
Zur Verbindung von unterschiedlichen Netzwerken werden Router eingesetzt. Im Gegensatz zu Switchen arbeiten Router mit IP-Adressen. Sie kennen sowohl die an sie angeschlossenen Netze als auch ihre Nachbarn.

Ihre Notizen

LABORÜBUNG 04 - EINRICHTEN EINES DATENSPEICHERS AUF EINER NAS-BOX

Szenario

Auf einer NAS-Box werden Freigaben erstellt, auf welche Lehrer und Schüler mit unterschiedlichen Rechten zugreifen können.



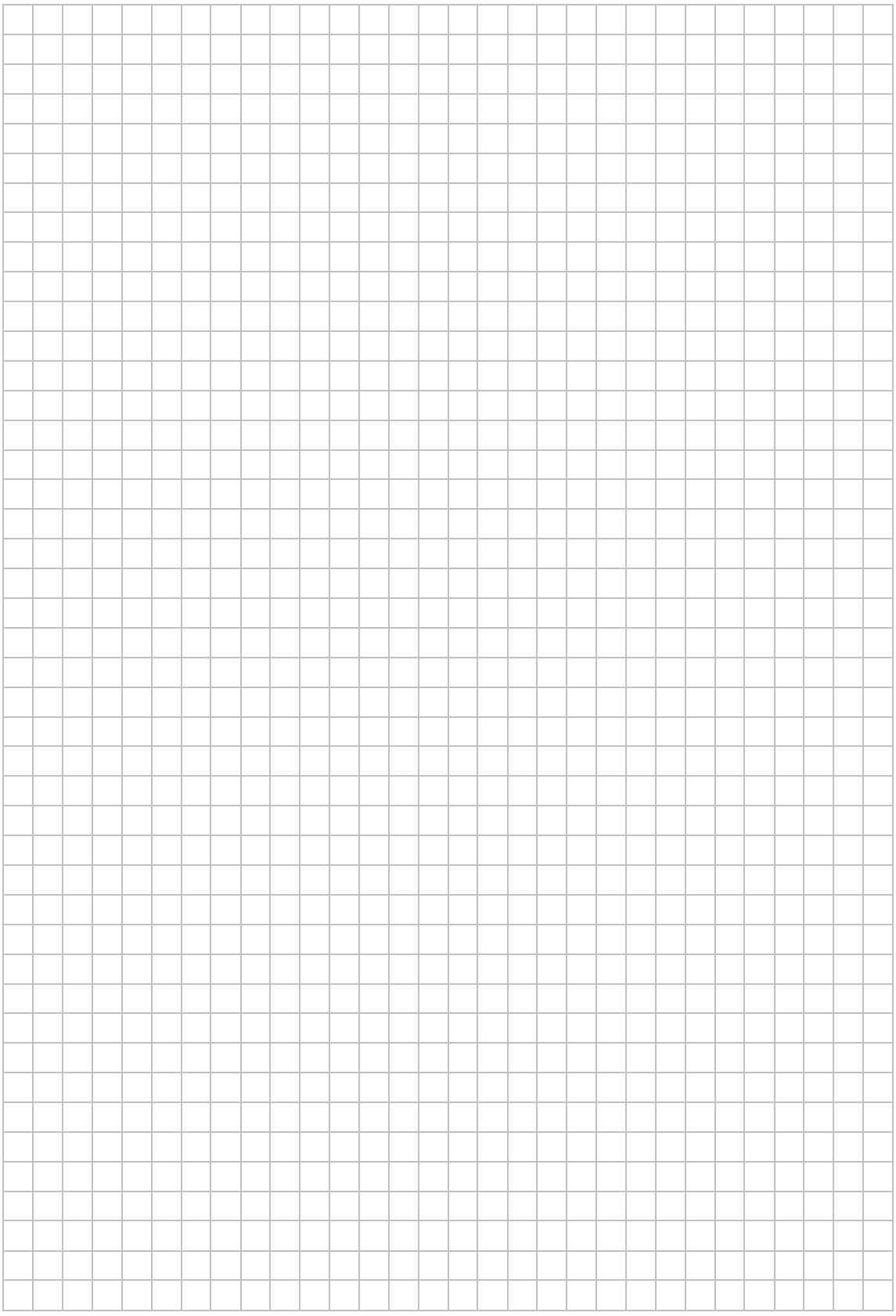
Aufgaben

1. Überprüfen Sie die Verbindung zum zentralen Datenspeicher (NAS) auf IP-Ebene.
2. Erstellen Sie auf der NAS-Box Benutzer, ggf. Benutzergruppen (z. B. Lehrer, Schüler) und einige Freigaben (z. B. Austausch, Vorlagen). Vergeben Sie den Benutzern bzw. Benutzergruppen verschiedene Zugriffsrechte (keine Rechte, Leserechte, Schreibrechte).
3. Greifen Sie von Ihrem Computer auf die Freigaben des zentralen Datenspeichers zu und überprüfen Sie Ihre Zugriffsrechte mit unterschiedlichen Benutzeraccounts. Testen Sie dabei auch unterschiedliche Zugriffsmethoden auf die Freigaben (z. B. Windows-Explorer, Netzlaufwerk verbinden, `net use` auf Kommandozeile).
4. Testen Sie den Zugriff auf die NAS-Box mit unterschiedlichen Benutzeraccounts über einen Web-Browser.

Weiterführende Aufgaben

5. Testen Sie mit einem Tablet oder Ihrem Smart Phone den Zugriff auf die NAS-Box. Verwenden Sie dazu geeignete Apps (z. B. Qfile für Android oder iOS).
6. Erstellen Sie ein Foto mit dem Smartphone und speichern Sie dieses auf der NAS-Box ab.

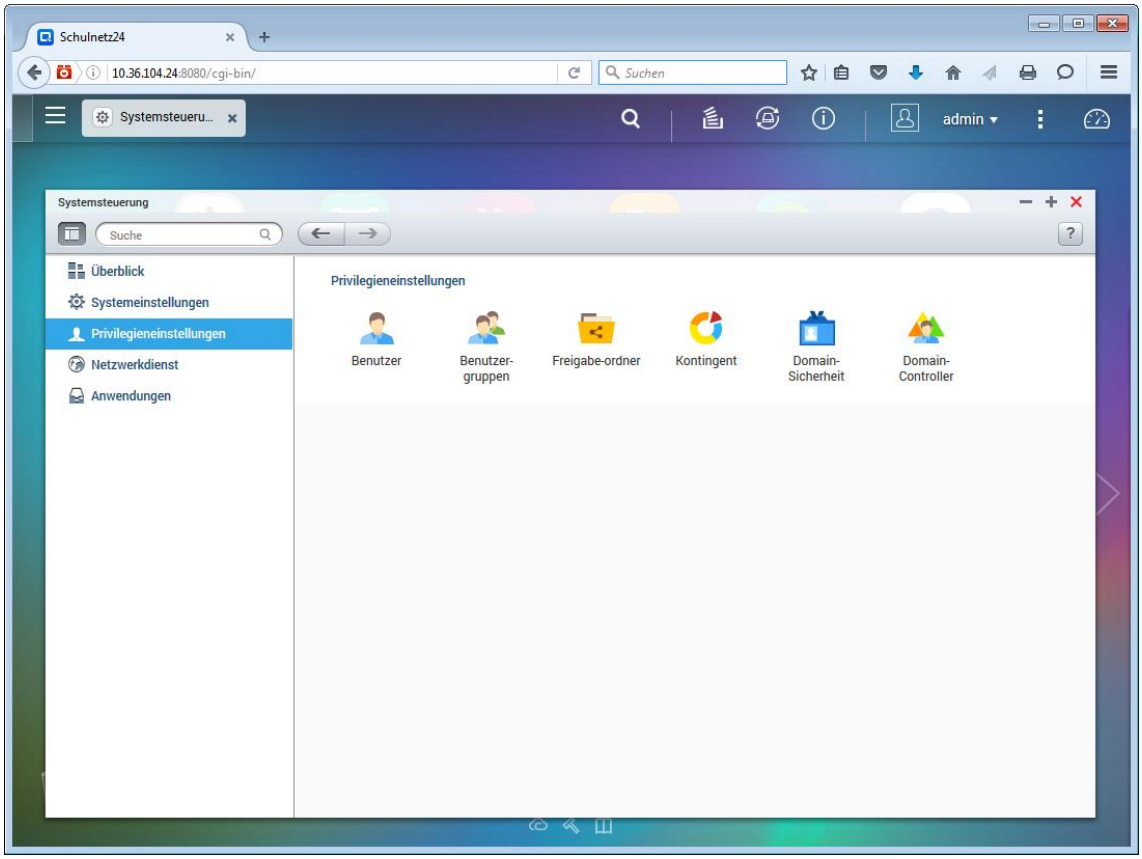
Ihre Notizen



HINWEISE

Einrichten von Freigaben auf einer NAS-Box

Über die Systemsteuerung der NAS-Box lassen sich Benutzer, Benutzergruppen und Freigaben mit unterschiedlichen Rechten einrichten.

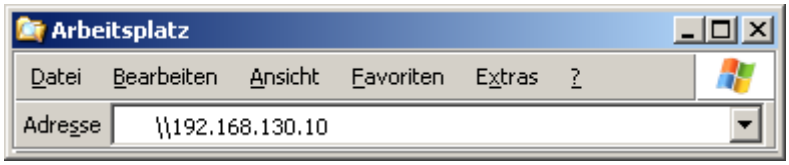


Zugriff auf eine NAS-Box mit Smartphones

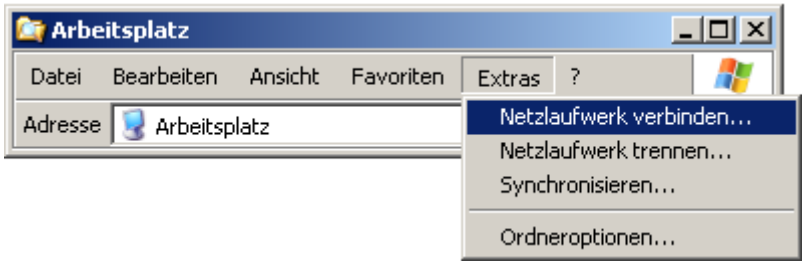
Da Smartphones keinen komfortablen Tastaturzugang besitzen, ist es praktikabel mit speziellen Apps den Zugang dauerhaft einzurichten (z. B. ES Datei Exporer, Qfile bei QNAP-NAS, DS file bei Synology-NAS).

Zugriffe auf SMB-Freigaben unter Windows

Adresszeile im Windows-Explorer



Netzlaufwerk verbinden im Windows-Explorer



Netzlaufwerk verbinden auf der Kommandozeile

`net use` *`Laufwerk:`* `\\`*`servername`*`\`*`freigabename`*

`net use x: \\192.168.130.10\Daten`

Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden.

`net use x: \\192.168.130.10\Daten /user:Lehrer`

Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden. Zur Authentifizierung wird der Benutzername (Lehrer) übergeben.

`net use x: \\192.168.130.10\Daten /user:Lehrer 12345`

Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden. Zur Authentifizierung werden der Benutzername (Lehrer) und das Passwort (12345) übergeben.

`net use x: \\192.168.130.10\Daten /persistent:yes`

Die Laufwerksverbindung x: wird erstellt und bei der nächsten Anmeldung am lokalen System automatisch wieder hergestellt.

Trennen von SMB-Verbindungen

SMB-Verbindungen sind oft sehr dauerhaft. Windows „merkt“ sich den Zugriff auf eine Freigabe und versucht, sich beim nächsten Zugriff mit den gespeicherten Anmeldeinformationen zu verbinden. Deshalb kann es bei den einzelnen Tests notwendig sein, sich am lokalen Computer abzumelden und neu anzumelden.

Windows-Explorer

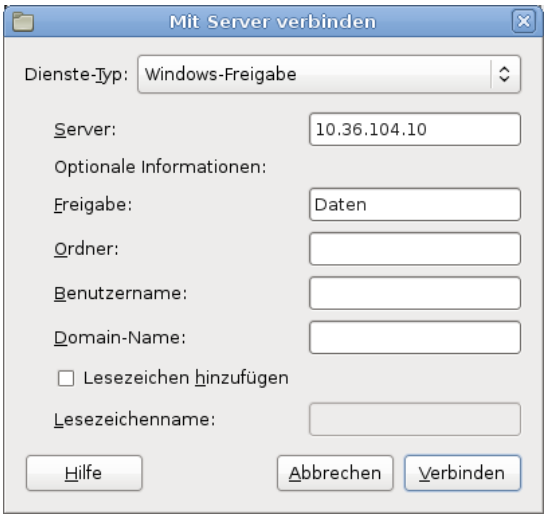
Extras – Netzlaufwerk trennen

Kommandozeile

`net use *Laufwerk*: /delete`	
`net use x: /delete`	Das Netzlaufwerk x: wird getrennt
`net use * /delete`	Alle Netzlaufwerke werden getrennt

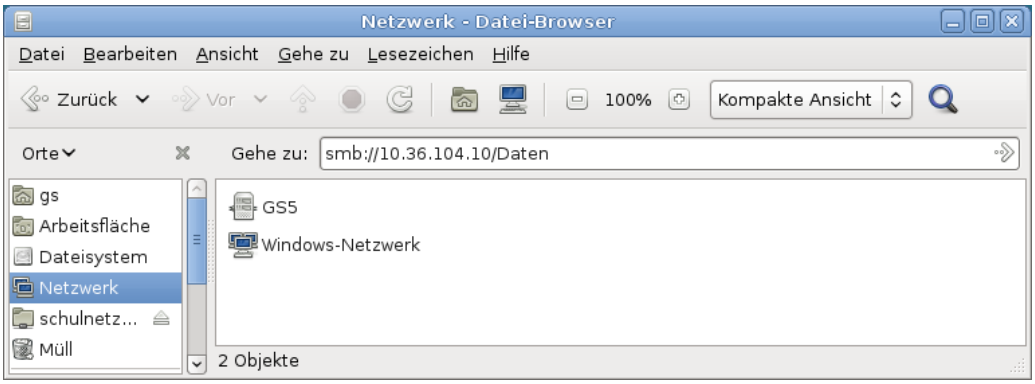
Zugriffe auf SMB-Freigaben unter Linux (Gnome)

Menü: Orte – Verbindung zu Server



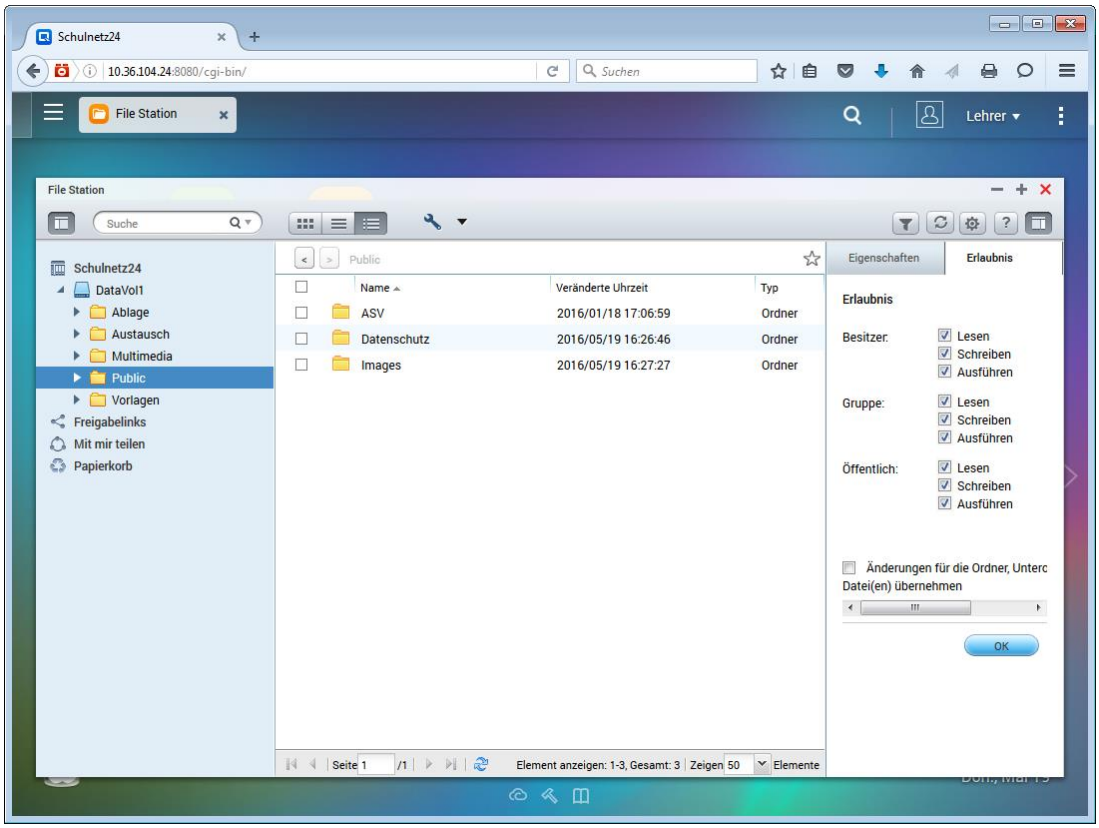
Nautilus-Adressleiste

```
smb://ip-Adresse
smb://ip-Adresse/freigabe
smb://user@<ip-Adresse>
```



Die Adressleiste beim Dateibrowser Nautilus muss ggf. mit <Strg>+L eingeblendet werden.

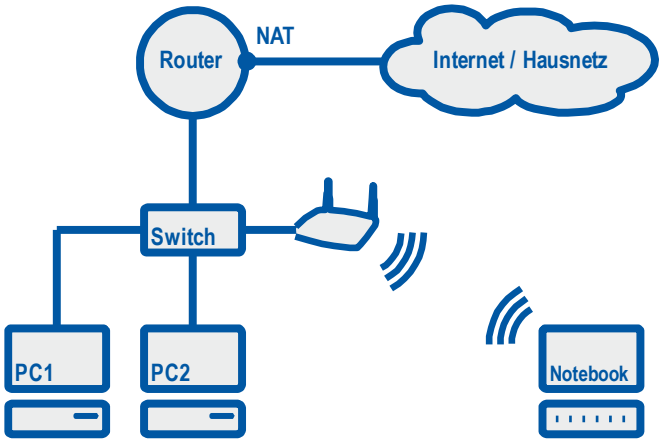
Web-Zugriff auf die Freigaben der NAS-Box



LABORÜBUNG 05 - WLAN-ANBINDUNG VON MOBILEN ENDGERÄTEN

Szenario

Notebooks oder andere mobile Geräte sollen über WLAN in das bestehende Netzwerk eingebunden werden und Zugriff auf das Internet erhalten.



Aufgaben

1. Stellen Sie einen Konfigurationszugang zum Access Point über das Webinterface oder über eine Konfigurationssoftware her.
2. Konfigurieren Sie den Access Point so, dass die mobilen Geräte Zugriff auf das Internet erhalten.
3. Sichern Sie die Verbindung mit WPA2 (PSK) ab.

HINWEISE

WLAN bietet die Möglichkeit zur Einbindung vornehmlich von mobilen Endgeräten. WLAN bietet seit mehr als 20 Jahren die Möglichkeit zur drahtlosen Kommunikation und ist im Standard IEEE 802.11 festgelegt.

WLAN verwendet zwei verschiedene Frequenzbereiche, einmal das 2,4 GHz Spektrum und andererseits das 5 GHz Spektrum. Die genannten Frequenzbereiche werden auch von anderen Nutzern belegt. WLAN ist aus diesem Grund ein Shared Medium. Es kann zu Störungen und Leistungsminderungen kommen. In der Schule sollten beide Spektren ausgesendet werden, um die höchstmögliche Kompatibilität zu gewährleisten.

Für den Standard 802.11 gibt es verschiedene Normen, zu erkennen an den Kleinbuchstaben nach dem Standard (a-x). Die Normen unterscheiden sich in der maximal möglichen Bandbreite. Der neueste Standard ist 802.11ax (WiFi 6). In einer Schule sollte mindestens 802.11ac (WiFi 5) verwendet werden, um eine ausreichende Bandbreite zu gewährleisten.

Bei WLAN-Problemen bietet es sich, dass man eine WLAN-Messung vornimmt und u. a. die Ausleuchtung durch die Access-Point überprüft.

Access-Points sollten, wenn möglich, immer mit einem Netzwerkkabel direkt an einen Switch angeschlossen werden. Auf den Einsatz von Repeatern zur Erweiterung des Signalradius sowie die Installation von Mesh-WLAN sollte verzichtet werden.

Zur besseren Verwaltung von Access-Points können WLAN-Controller installiert werden. Dadurch können die Access-Points zentral verwaltet werden.

Drahtlose Netzwerkgeräte

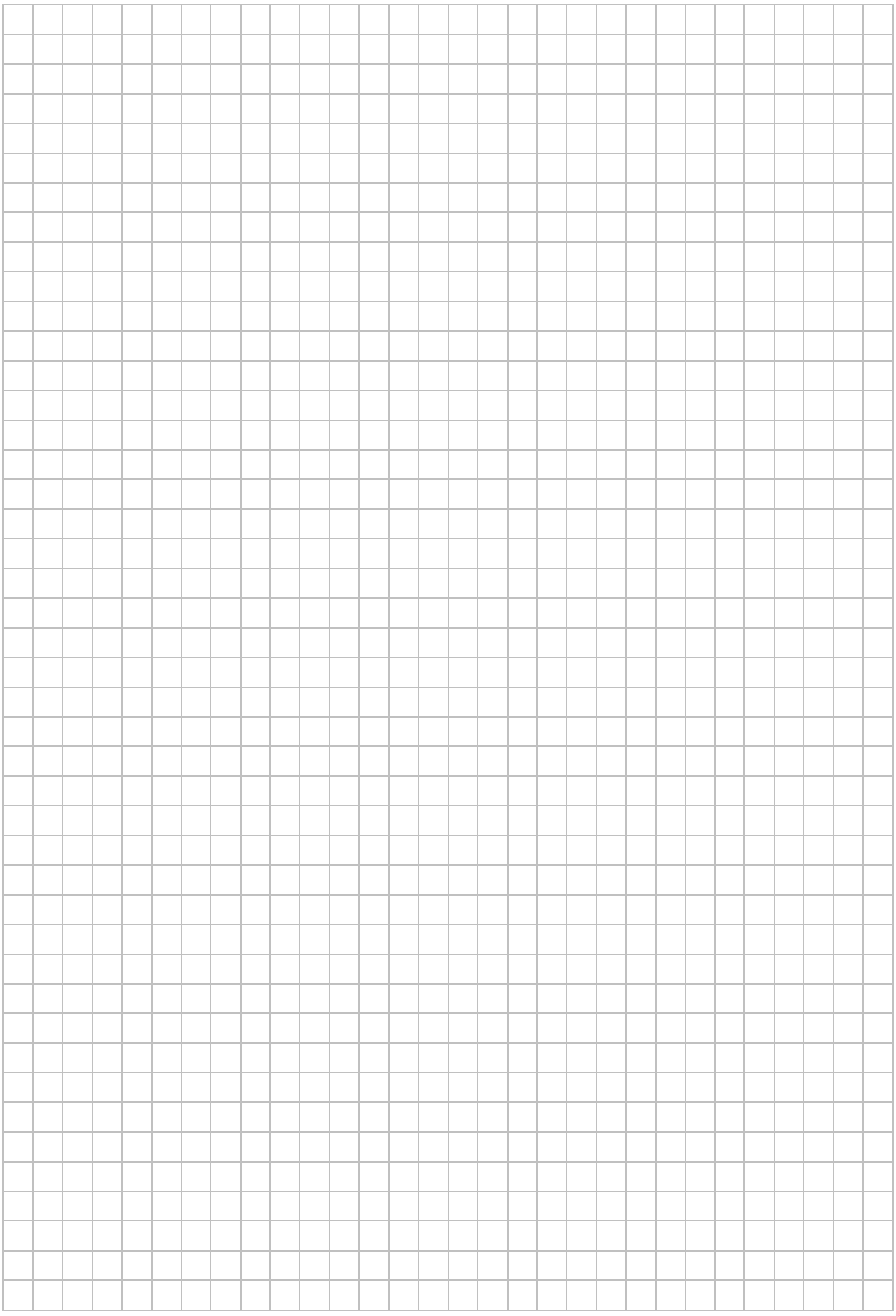
Access-Point

Access-Points sollten mit einem Netzwerkkabel an einen Switch angeschlossen werden. Access-Points können sowohl das 2,4 GHz und auch das 5 GHz Frequenzband ausstrahlen (Dual-Modus). Zudem können mehrere SSID gleichzeitig ausgestrahlt werden.

Repeater

Bei einem Repeater handelt es sich um einen Signalverstärker oder –aufbereiter. Er dient nur zur Vergrößerung der Reichweite eines Signals. Allerdings halbiert sich die Datenübertragungsrate des Funknetzes hinter dem Gerät, da der Repeater sowohl mit den Clients, als auch mit dem Access-Point kommuniziert.

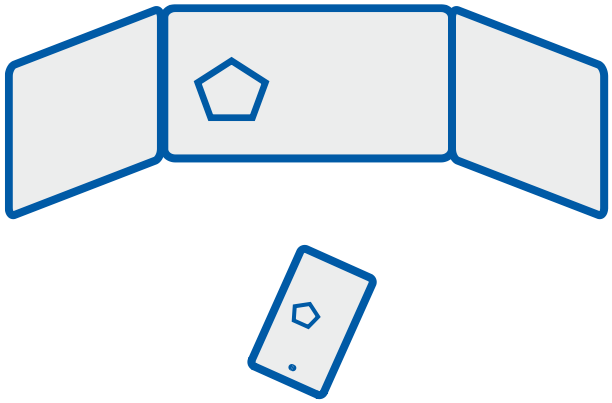
Ihre Notizen



LABORÜBUNG 06 - DRAHTLOSE BILDÜBERTRAGUNG AUF EINEN BEAMER

Szenario

Der Bildschirminhalt eines Tablets oder Smartphones soll auf einen Beamer drahtlos übertragen werden.



Vorbereitung

Miracast-Adapter bzw. Apple-TV

Aufgaben

1. Stellen Sie den Bildschirm Ihres Notebook, Tablet oder Smartphone am Beamer dar.
2. Öffnen Sie mit Ihrem Mobilgerät gleichzeitig eine WLAN-Verbindung ins Hausnetz bzw. ins Internet.
3. Übertragen Sie ein Video, das Sie live über das Internet beziehen, mit Bild und Ton auf den Beamer.

HINWEISE

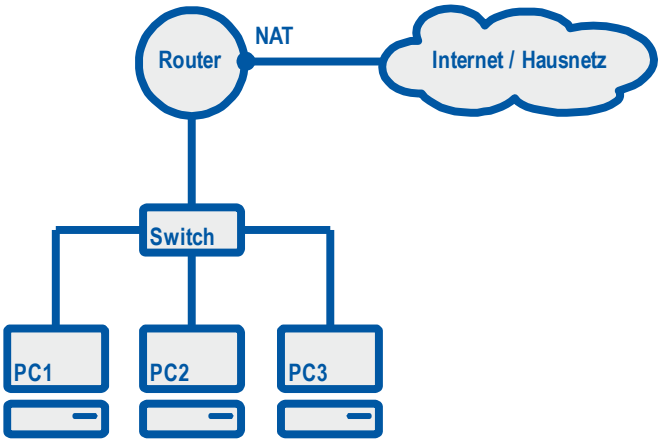
Die Bildübertragung von mobilen Endgeräten ist ausführlich in einer eigenen Dokumentation dargestellt:

https://alp.dillingen.de/schulnetz/materialien/Bildschirmuebertragung.pdf

LABORÜBUNG 07 - INTERNETANBINDUNG ÜBER EINEN ROUTER

Szenario

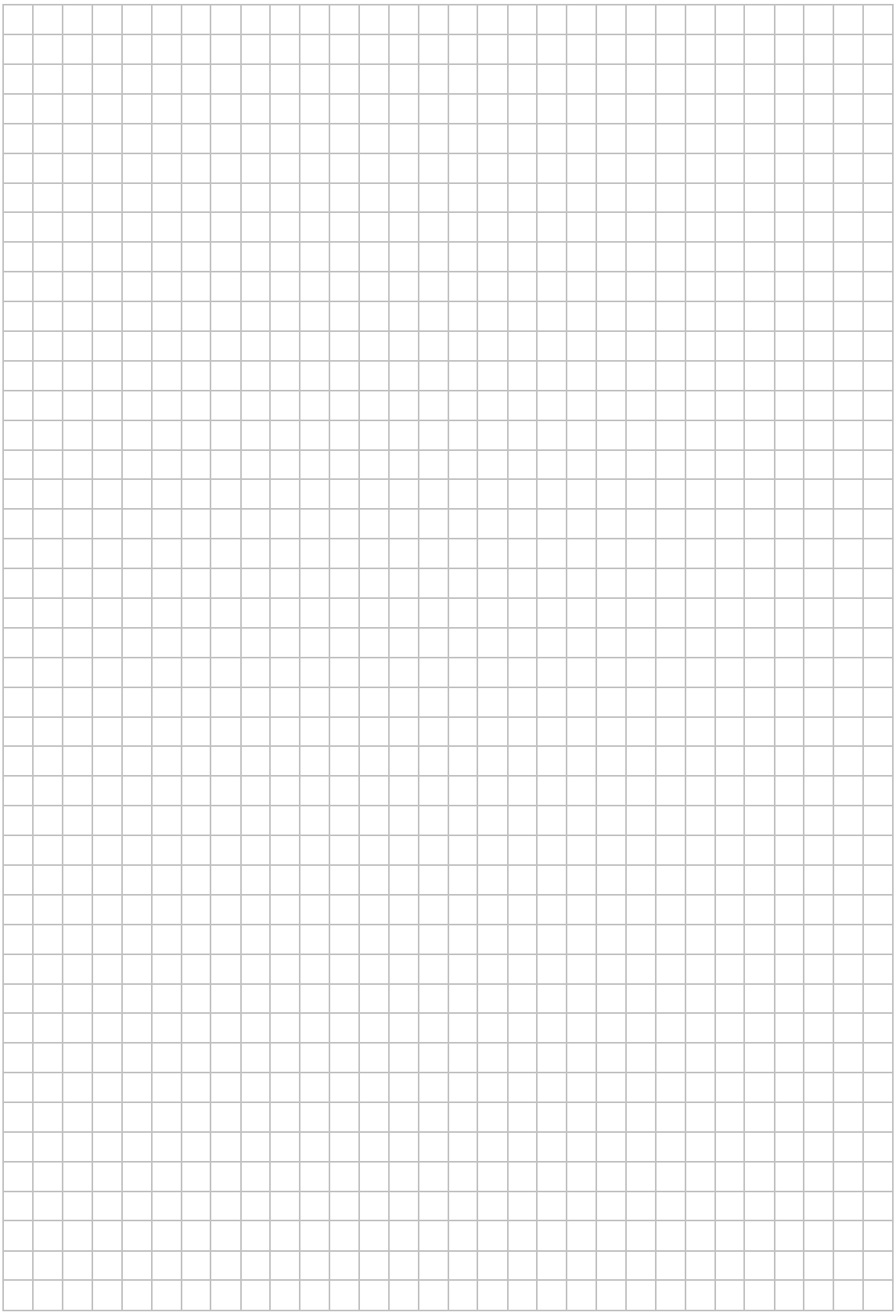
Mehrere Computer sollen über einen Router an das Hausnetz (bzw. über DSL an das Internet) angebunden werden.



Aufgaben

1. Stellen Sie einen Konfigurationszugang zum Router über das Webinterface her.
2. Konfigurieren Sie den Router so, dass die Verbindung der Computer des internen Netzes mit dem Internet bzw. Hausnetz funktioniert.
   - Wählen Sie dazu IP-Adressen aus einem privaten IP-Adressbereich, der nicht mit dem IP-Adressbereich des Hausnetzes kollidiert.
   - Ermöglichen Sie den Clients den Zugang zum Internet, indem Sie am externen Interface NAT/PAT aktivieren.
   - Konfigurieren Sie den Router als DHCP-Server und DNS-Relay für das interne Netz.

Ihre Notizen



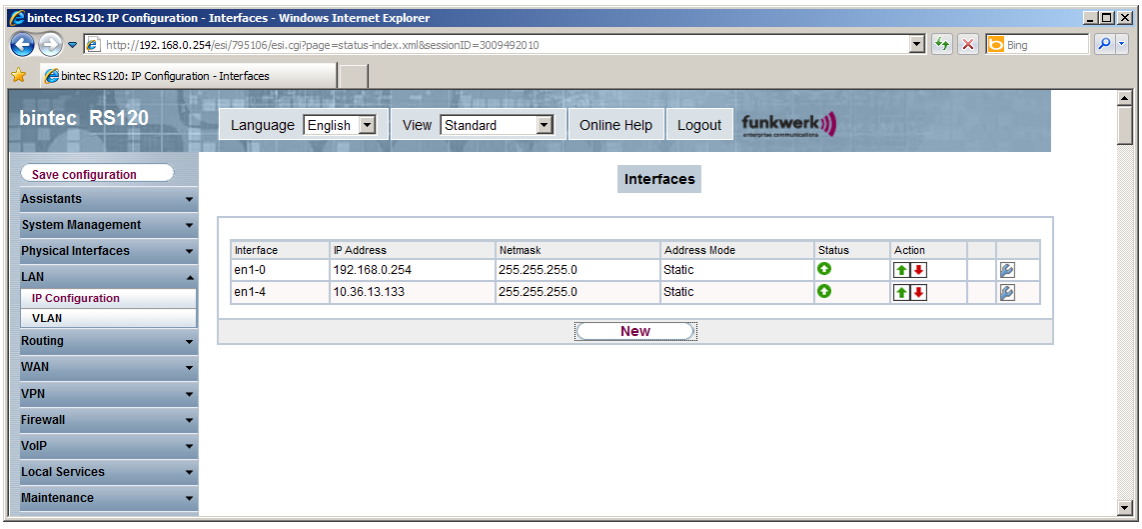
HINWEISE

Empfohlene Vorgehensweise bei der Konfiguration eines Routers

- Zurücksetzen des Routers
- Grundkonfiguration des Routers
- Konfiguration zusätzlicher Dienste (DNS, DHCP)
- Konfiguration der Firewall

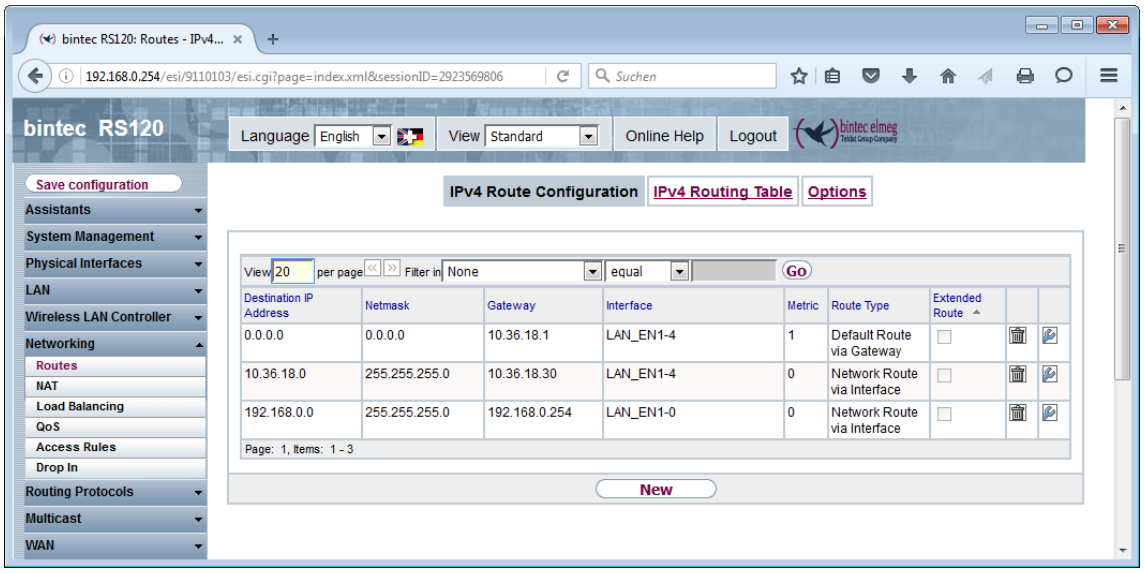
Konfiguration der Schnittstellen

Üblicherweise sind mindestens zwei Schnittstellen (eine interne und eine externe Schnittstelle) zu konfigurieren. An der externen Schnittstelle kann der Router die IP-Adresse gegebenenfalls auch per DHCP aus erhalten.



Routing / Default Route

Die Default Route (Standard-Route) definiert einen festgelegten Weg für Datenpakete, deren Zielnetze nicht explizit in der Routingtabelle stehen. Wird dem Router die Default Route nicht per DHCP zugewiesen, muss sie statisch eingetragen werden.

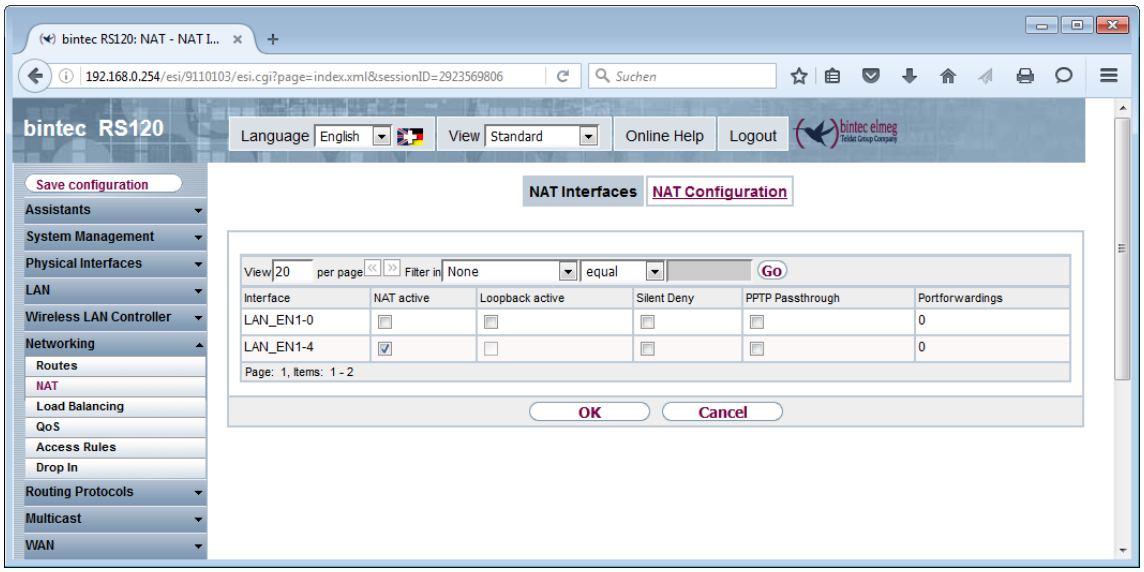


Network Address Translation (NAT)

Damit ein Computer im lokalen Netz mit Computern im Internet kommunizieren kann, ersetzt der Router die privaten Quelladressen aller IP-Pakete, die das lokale Netz verlassen, mit einer öffentlichen IP-Adresse (Netzadressübersetzung).

In der Regel wird mehreren Computern mit privaten IP-Adressen eine öffentliche IP-Adresse zugewiesen. Durch die gemeinsame Nutzung einer öffentlichen IP-Adresse durch mehrere Computer werden zur Differenzierung der Kommunikationsstränge noch Portnummern herangezogen.

Am externen Interface muss NAT aktiviert werden.



DHCP-Server

Durch einen DHCP-Server (**D**ynamic **H**ost **C**onfiguration **P**rotocol) können Clients ohne manuelle Konfiguration in ein bestehendes Netzwerk eingebunden werden. Ein DHCP-Server kann eine Vielzahl von Einstellungen an den Client übermitteln. Üblicherweise werden einem Client folgende Einstellungen zugewiesen:

- IP-Adresse und Netzwerkmaske
- Default-Gateway
- DNS-Server
- evtl. WINS-Server (für Microsoft Windows Clients)

DNS-Relay

Ist in einem Netz kein DNS-Server vorhanden, kann der Router als DNS-Relay eingerichtet werden. Beim Client wird der Router als DNS-Server eingetragen. Der Router nimmt die DNS-Anfragen der Clients entgegen und reicht diese an einen ihm bekannten DNS-Server weiter.

Der Router selbst kann die DNS-Konfiguration auch dynamisch per DHCP erhalten. (Dies ist bei DSL-Anschlüssen üblich.)

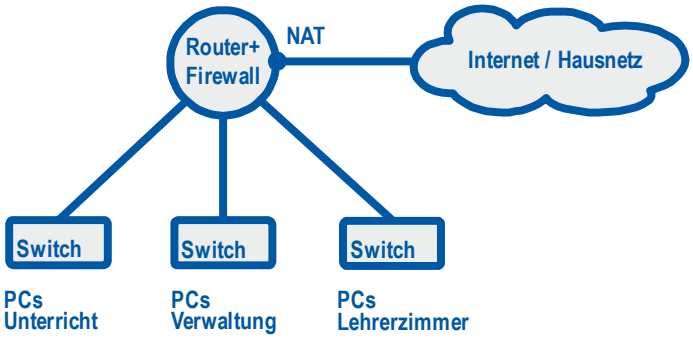
Konfiguration der Firewall

An einem Router können beim Übergang von einem Netz in ein anderes Netz Firewall-regeln definiert werden.

LABORÜBUNG 08 - KONZEPTION VON SCHULNETZEN

Szenario

Ein Schulnetz soll von Beginn an neu geplant oder weiterentwickelt werden.



Aufgaben

1. Formulieren Sie die Vorstellungen Ihrer Schule, wie mit Computern beziehungsweise mit den digitalen Medien gearbeitet werden soll.
2. Formulieren Sie aus den Vorstellungen heraus den Bedarf und die Anforderungen für Ihre Schule.
3. Planen Sie für Ihre Schule eine logische Netzstruktur und ein Nutzungskonzept.

Vorstellungen der Schule

Wie und womit soll in der Schule gearbeitet werden?

Beispiele

- Schüler sollen ihre eigenen mobilen Geräte im Unterricht einsetzen können.
- Tablets und Smartphones sollen spontan im Unterricht verwendet werden.
- Lehrer (ggf. auch Schüler) sollen ihre mobilen Geräte am Beamer zeigen können
- Der Unterricht soll in einer Lernplattform (z. B. mebis) abgebildet werden
- Die Nutzung des Internets mit mobilen Geräten durch Lehrer oder Schüler soll jederzeit möglich sein.
-
-

Bedarf und Anforderungen

Beispiele:

- Alle Klassenzimmer sollen mit WLAN ausgestattet sein.
- Internetzugriffe der Schüler sollen über einen Webfilter laufen. Eine Protokollierung der Internetzugriffe ist nicht notwendig.
- Arbeitsplätze der Lehrkräfte (Lehrerzimmer) sollen netzwerktechnisch vom übrigen Unterrichtsnetz getrennt sein.
-
-

Konzeption von Schulnetzen

Die Konzeption von Schulnetzen ist ausführlicher in der Handreichung „Systembetreuung – Einführung und Orientierung“ dargestellt.

http://alp.dillingen.de/schulnetz/materialien/Systembetreuung.pdf

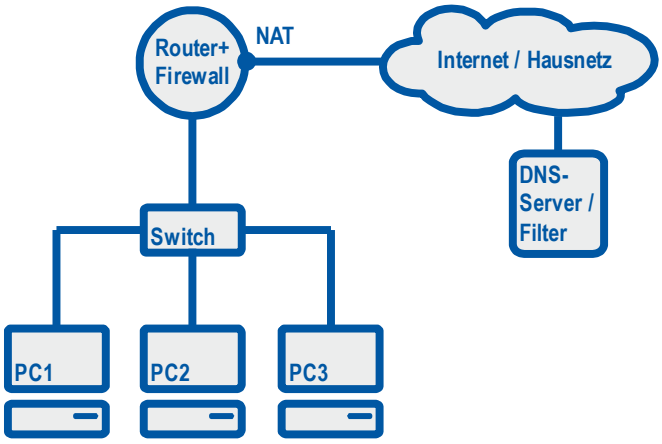
WEITERFÜHRENDE LABORÜBUNGEN

Ihre Notizen

LABORÜBUNG 09 - BESCHRÄNKUNG DES INTERNET-ZUGANGS ÜBER EINEN WEBFILTER

Szenario

Der Zugang zum Internet soll nur über einen Web-Filter möglich sein.



Aufgaben

1. Konfigurieren Sie einen lokalen PC so, dass dieser einen DNS-Dienst nutzt, der unerwünschte Webseiten ausblendet (z. B. freie DNS-Server bei OpenDNS oder die DNS-Filter der Akademie für Lehrerfortbildung).
2. Richten Sie den DNS-Dienst mit Webfilter am Router ein, so dass dieser DNS-Dienst von allen PCs im Netz verwendet wird.

Weiterführende alternative Aufgabe

3. Installieren Sie im lokalen Netz einen Web-Proxy, der eine Filterlösung anbietet. (z. B. Openschoolproxy). Tragen Sie am Browser des Computers den Proxy ein und testen Sie die Funktionalität.

Ihre Notizen

Webfilter

Bei Einsatz eines Webfilters können die Zugriffe auf einzelne Webseiten erlaubt oder verboten werden. Die angebotenen Webfilter arbeiten üblicherweise mit URL-Filterlisten. Die Anbieter dieser Filterlisten versuchen dabei möglichst alle Webseiten zu erfassen und jede Webseite einer oder mehrerer Kategorien zuzuordnen (z. B. Spiele, Gewalt, Bildung, …). Dem Filter wird dann mitgeteilt, welche Kategorien geblockt werden sollen.

Verschiedene Implementierungen von Webfiltern

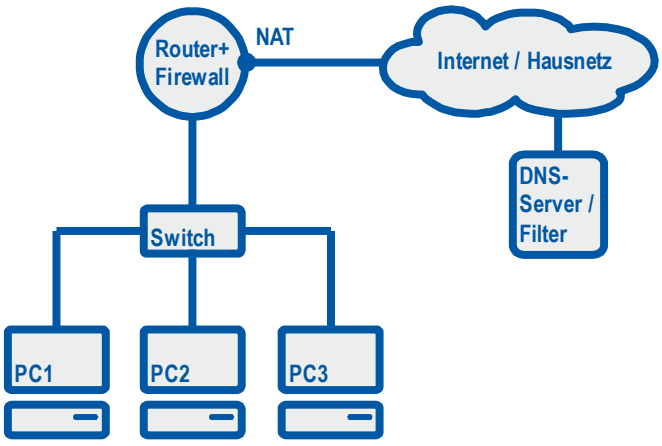
Am lokalen PC

Am lokalen PC wird eine Kinderschutzsoftware (z. B. FragFINN, NetNanny, Family Protection) installiert, die einzelne Internetseiten erlaubt oder blockiert. Geeignet ist dieses Verfahren für den Computer zu Hause.

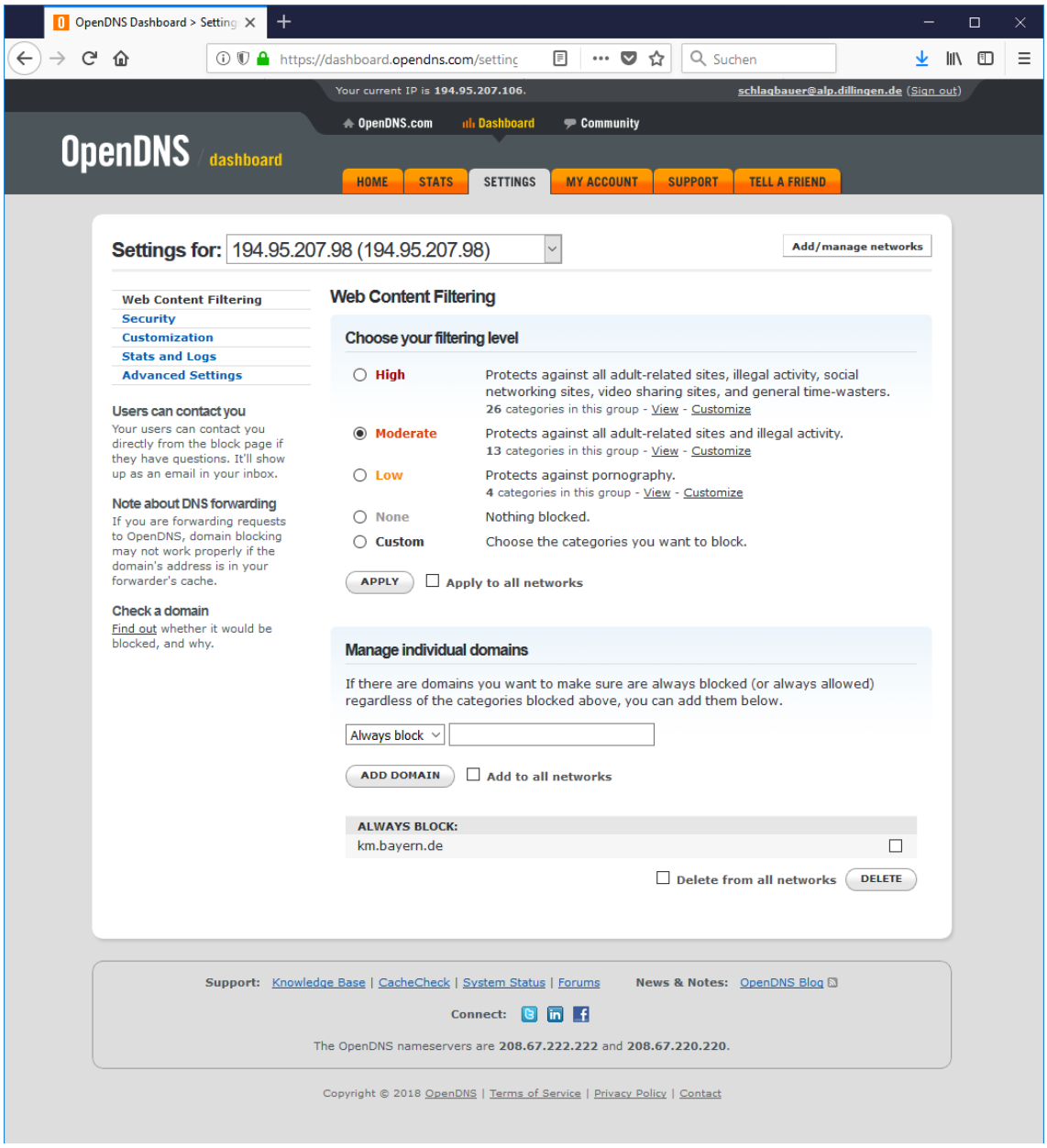
Sperrung von Internetseiten durch den Provider

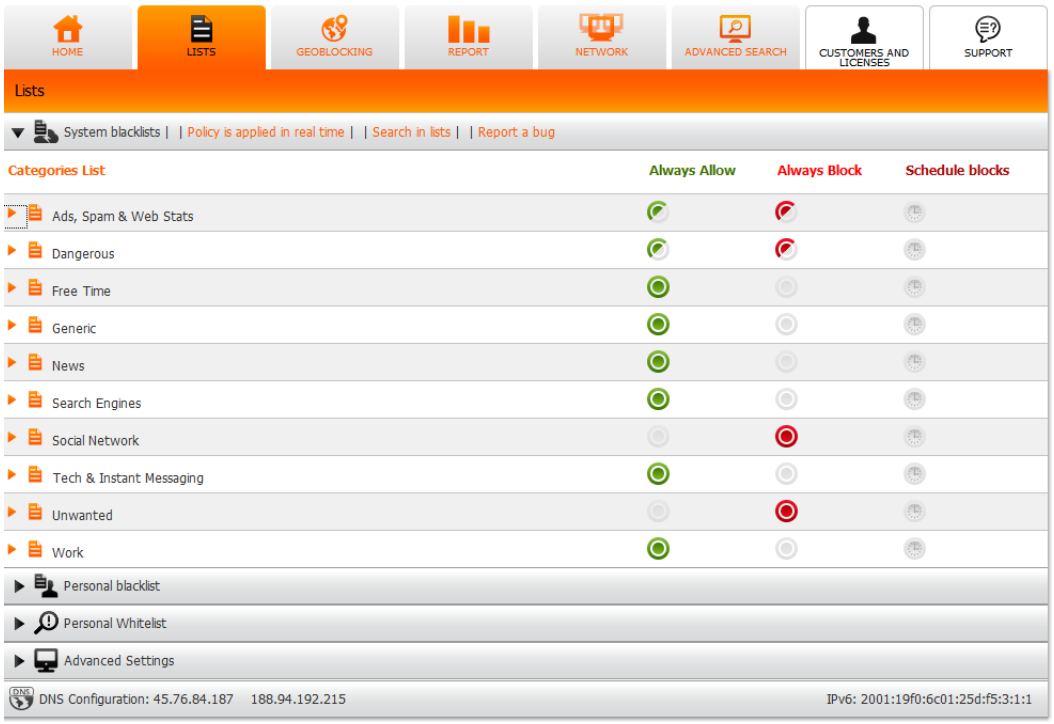
Der Internetzugangs-Provider hat grundsätzlich die Möglichkeit, einzelne Internetseiten zu sperren (z. B. durch eine Firewall oder durch eine Umleitung der Adressen auf eine andere Webseite). Dies wird z. B. bei BayernWLAN so gehandhabt (zentraler Jugendschutzfilter). Eine individuelle Einstellung des Jugendschutzfilters ist dabei üblicherweise nicht vorgesehen.

DNS-Filter



Einige DNS-Dienstanbieter (z. B. OpenDNS oder FlashStart) bieten eine sehr einfach zu handhabende Filterlösung. Die Schule kann auf der Webseite des Anbieters die zu sperrenden Kategorien auswählen. Bei einer DNS-Anfrage der Schule wird für eine zu blockierende URL eine Webseite zurückgeliefert, die auf die Sperrung hinweist. Eine Differenzierung innerhalb der Schule ist nur durch die Wahl des DNS-Servers möglich.





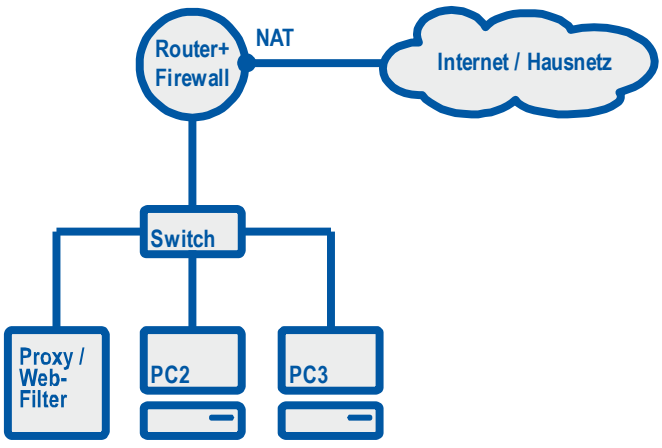
Auswahl der zu sperrenden Kategorien auf der Webseite des DNS-Anbieters Flashstart. Flashstart bietet auch Geoblocking mit an.

DNS-Filter der Akademie für Lehrerfortbildung in Dillingen

Die Akademie bietet drei verschieden eingestellte DNS-Server zur kostenlosen Nutzung durch Schulen an:

- Stufe 1: Filterung von Malware: 194.95.207.171
- Stufe 2: Filterung von Malware und pornografischen Seiten: 194.95.207.172
- Stufe 3: Filterung von Malware, pornografischen Seiten und noch weitergehende Inhalte: 194.95.207.173

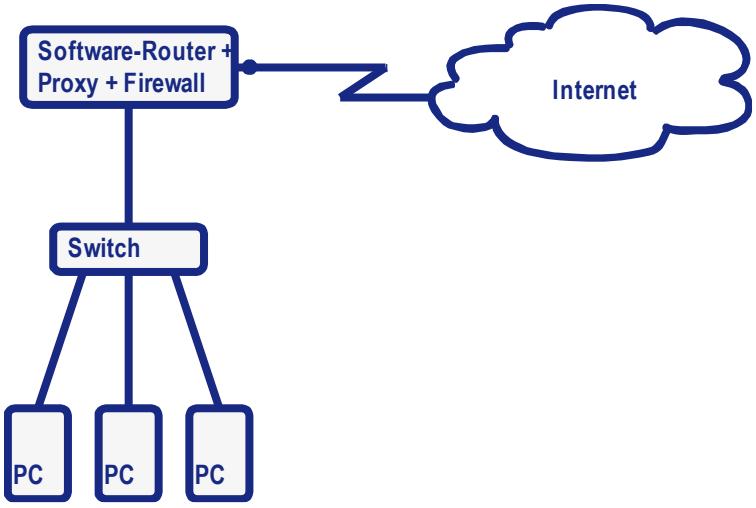
Filterung über einen Proxy



Ein Proxy (Stellvertreter) ist ein Serverdienst, der auf der Anwendungsebene arbeitet. Proxys gibt es für verschiedene Internet-Anwendungen, z. B. für http, ftp, smtp. Am bekanntesten sind die Web-Proxy (z. B. Squid). Ein Client baut dabei keine direkte Verbindung zum Internet auf, sondern sendet seine Anfrage an den Proxy. Dieser sendet daraufhin eine eigenständige Anfrage an den Webserver und leitet die Antwort an den Client weiter. Der Webserver im Internet sieht als Absender nur den Proxy und nicht den anfragenden Client.

Wird der Webzugriff über einen Proxy geleitet, kann dieser sehr differenziert (z. B. auf Benutzerebene) Zugriffe zulassen oder blockieren. Nachteilig an einer Proxy-Lösung ist, dass viele Apps auf mobilen Geräten nur schwer damit umgehen können.

Transparenter Proxy



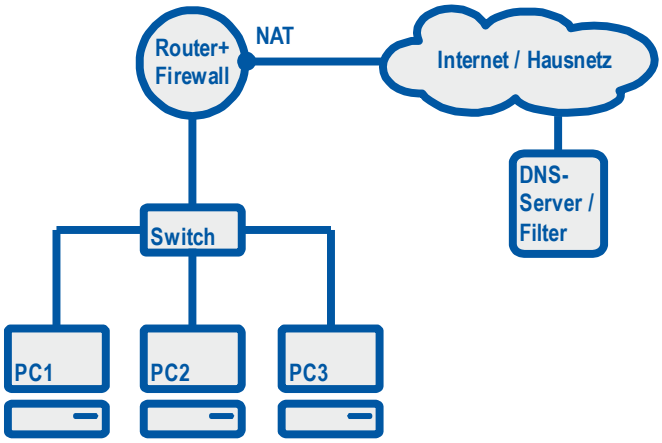
Läuft der Internetzugang über einen Software-Router (UTM-Appliance, z. B. IPCop, IPFire, PFSense oder darauf aufbauende Lösungen), kann auf dem Software-Router ein Proxy installiert werden, der auch als transparenter Proxy betrieben werden kann.

Am Web-Browser muss der transparente Proxy nicht eingetragen werden, deshalb kommen mobile Geräte besser damit klar. Nachteilig an dieser Lösung ist, dass verschlüsselte Webseiten Probleme bereiten. Wenn diese über den Proxy geleitet werden, erkennt der lokale Browser einen Angriffsversuch (Man in the Middle-Angriff).

LABORÜBUNG 10 - FIREWALL-EINSTELLUNGEN AM ROUTER

Szenario

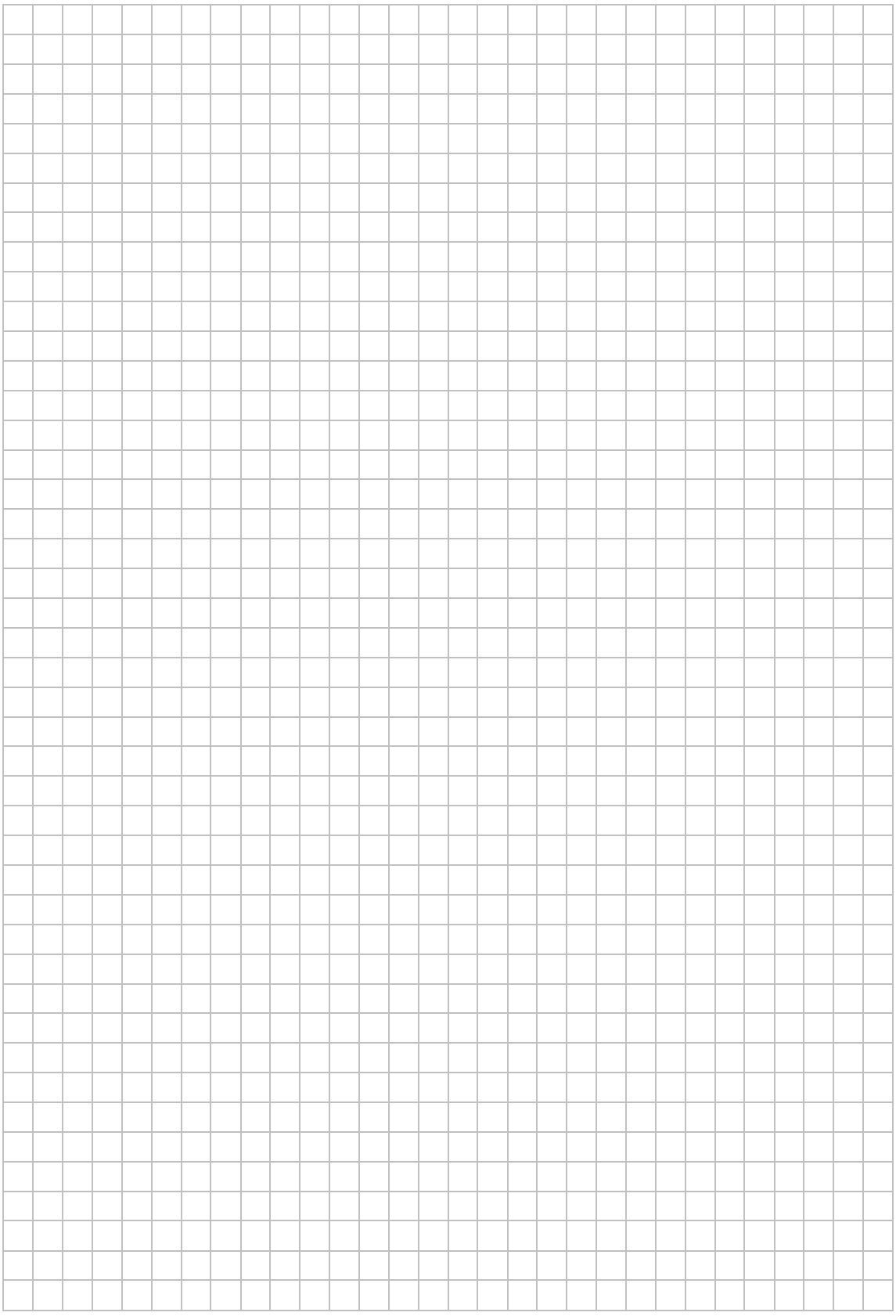
Am Router soll die Firewall so eingerichtet werden, dass der vorgesehene Webfilter nicht umgangen werden kann.



Aufgaben

1. Richten Sie das von Ihnen verwaltete Netz so ein, dass der Internetzugang funktioniert. Der Router soll dabei als DHCP-Server und DNS-Relay fungieren.
2. Richten Sie am Router eine Firewall ein, so dass der Zugriff zum Internet nur noch über den vorgesehen DNS-Server möglich ist.

Ihre Notizen



HINWEISE

Firewall

Eine Firewall beschränkt mögliche Verbindungen, indem einzelne Pakete nicht weitergeleitet sondern verworfen werden. Mit Firewallregeln lässt sich der Datenverkehr sehr detailliert regeln.

Firewallregeln

Eine Firewallregel besteht aus Filterkriterien und einer zugehörigen Aktion. Die Filterkriterien sind Quelle, Ziel und Dienst (z. B. DNS oder http). Die möglichen Aktionen sind Zugriff, Verweigern und Zurückweisen.

Quelle und Ziel können Schnittstellen, IP-Netze oder einzelne IP-Adressen sein. Mögliche Dienste sind alle Layer-3 und Layer-4-Protokolle (z. B. IP, ICMP, TCP, UDP) und über die TCP- und UDP-Ports definierten Standardanwendungen (z. B. http, DNS, smtp).

Mögliche Aktionen sind:

- Zugriff (Access) — Pakete werden weitergeleitet.
- Verweigern (Deny) — Pakete werden verworfen.
- Zurückweisen (Reject) — Pakete werden verworfen, der Absender erhält eine Information

Beispiele für Firewall-Regeln

Filterkriterien			Aktion
Quelle	**Ziel**	**Dienst**	
Lokales Netz	8.8.8.8	DNS	Access
Lokales Netz	Router	DHCP	Access
Lokales Netz	Internet	icmp	Access
Lokales Netz	Internet	http	Access
Lokales Netz	Internet	https	Access

Die Firewallregeln werden von oben nach unten abgearbeitet. Wenn das Filterkriterium greift (d. h. wenn Quelle, Ziel und Dienst mit einem ankommenden IP-Paket übereinstimmen) wird die festgelegte Aktion angewendet. Alle nachfolgenden Regeln werden für dieses IP-Paket nicht mehr beachtet.

Üblicherweise trägt man in eine Firewall nur die Wege oder Verbindungen ein, die erlaubt sein sollen. Alles andere ist automatisch verboten (implicit deny).

Stateful Inspection Firewall

Bei einer Stateful Inspection Firewall muss für Antwortpakete keine eigene Regel definiert werden. Antwortpakete sind automatisch erlaubt, wenn diese zu einer bestehenden Verbindung passen. Details zu Firewalltypen sind in der Broschüre „Sichere Internetanbindung von Schulen“ (http://alp.dillingen.de/schulnetz/materialien) erläutert.