Beratung und Support
Technische Plattform
Support-Netz-Portal




paedML® – stabil und zuverlässig vernetzen

Unsupported HowTo

Netzerweiterungen

Stand 14.09.2016 – Aktualisierung und Anpassung an den dritten Netzbrief

paedML® Linux

Version: 6.0

paedML® Die Musterlösung für schulische Computernetze

LMZ Landesmedienzentrum Baden-Württemberg

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111

70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ

Roland Walter

Endredaktion

Doreen Edel.

Bildnachweis Titelbilder:

Thinkstock

Weitere Informationen

www.support-netz.de
www.lmz-bw.de

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2016

Inhaltsverzeichnis

Vorwort

Die vorliegende Anleitung behandelt folgende Themen:

1. **Trennung verschiedener Netzsegmente** gemäß Netzbrief des Kultusministeriums vom September 2015. Hierin werden die Rahmenbedingungen für das sogenannte „Lehrernetz“ beschrieben. Die Umsetzung erfolgt über die Einrichtung von VLANs, welche die Netze „Pädagogisches Netz“ und „Lehrernetz“ logisch voneinander trennen.
2. **Erweiterung des „Pädagogischen Netzes“ um ein „Class-B-Netz“**, über das ein größerer IP-Adressraum zur Verfügung gestellt wird.
3. Zusätzlich wird beschrieben, wie Sie **weitere Subnetze**, zu ihrem Pädagogischen Netz hinzufügen.

Die Themenbereiche können sowohl getrennt voneinander, als auch zusammen betrachtet werden.

Es sind hierdurch verschiedene neue Netzwerkkonfigurationen möglich:

- Einrichtung des „Lehrernetzes“ und logische Trennung des Netzwerkverkehrs zwischen „Lehrer-“ und „Pädagogischem Netz“.
- Einrichtung des „Lehrernetzes“ und logische Trennung des Netzwerkverkehrs zwischen „Lehrer-“ und „Pädagogischem Netz“ mit Umstellung des „Pädagogischen Netzes“ auf einen größeren IP-Adressraum.
- Erweiterung des „Pädagogischen Netzes“ auf einen größeren IP-Adressraum ohne „Lehrernetz“.
- In Kapitel 10 „Netzerweiterung um eigene Netze“ wird beschrieben, wie Sie Ihr individuelles schulisches Netz umsetzen können.

Es kann aber weiterhin die Netzwerkkonfiguration der paedML Linux im Auslieferungszustand betrieben werden. In dem Fall stehen 198 IP-Adressen zur Verfügung, die an Geräte im „Pädagogischen Netz“ vergeben werden können. **Für diese Konfiguration sind keine Anpassungen notwendig.**

Aufbau des Dokuments

1. Einführung in die Trennung der Netze
2. Übersicht über die Netze der paedML Linux
3. Vorbereitende Arbeiten
4. Einrichtung und Trennung von Netzen
5. Aufnahme von Rechnern in weitere Netze
6. Netzerweiterung um eigene Netzsegmente

Zielgruppe	Schwierigkeitsgrad
Dienstleister erfahrene Administratoren	mittel bis schwer

1. Einführung in die Trennung von Netzsegmenten

Das hier beschriebene Verfahren der Trennung von Netzsegmenten muss nur dann durchgeführt werden, wenn Sie Rechner im pädagogischen Netz haben, in dem personenbezogene Daten verarbeitet werden sollen, die aus Datenschutzgründen nicht von Schülern eingesehen werden dürfen.

Ein Beispiel hierfür wäre ein Rechner im Lehrerzimmer, der über das pädagogische Netz in die paedML eingebunden ist. Auf diesem Gerät wird beispielsweise von Lehrkräften Unterrichtsmaterial bearbeitet und bereitgestellt. Auf dem Gerät sollen gleichzeitig Bewertungen oder Benotungen von Schülerarbeiten verarbeitet werden.

Im Netzbrief[1] des Kultusministeriums Baden-Württemberg vom September 2015 wird eine Trennung der schulischen Netze in drei Segmente empfohlen:

> *„Das Kultusministerium empfiehlt aufgrund des technologischen Fortschritts und der Anforderungen von Schulen die Einrichtung einer **dreistufigen Netzinfrastruktur**, welche aus einer lokalen informationstechnischen **Arbeitsumgebung für die Schulleitung**, einer **Umgebung für die Lehrkräfte** und einer informationstechnischen **Unterrichtsumgebung** besteht. Zwischen diesen Netzen dürfen unter bestimmten Bedingungen Übergänge eingerichtet sein. Die Einrichtung von sog. VLANs (virtuellen Netzen) oder die Nutzung von Virtuellen Maschinen ist zulässig.“*
>
> *Netzbrief vom September 2015, Seite 2*

Die Trennung der einzelnen Netzbereiche ist notwendig, um den Zugriff Unbefugter auf personenbezogene Daten auszuschließen.

[1] http://www.it.kultus-bw.de/site/pbs-bw-new/get/params_Dattachment/1905858/Netzbrief%202%20v1.pdf

> *„In Schulen werden die unterschiedlichsten personenbezogenen Daten verarbeitet. So erfolgt an Schulen neben der Speicherung personenbezogener Daten, die im Unterricht benötigt werden, auch die Verarbeitung von Daten der Schülerinnen, Schüler und Sorgeberechtigten bis hin zu Bewertungen und Beurteilungen von Schülern im Rahmen der Schulverwaltung. Ferner werden auch personenbezogene Daten der Lehrkräfte im Sinne der Personalverwaltung (z. B. dienstliche Beurteilungen) verarbeitet.*
>
> *Wesentliches Ziel bei der Gestaltung der Netzinfrastruktur an Schulen ist es, diese unterschiedlichen personenbezogenen Daten besonders zu schützen. Dabei ist insbesondere sicherzustellen, dass nur diejenigen Personen auf solche personenbezogene Daten zugreifen können, die zur Erfüllung ihrer dienstlichen Aufgaben unbedingt erforderlich sind.“*
>
> *Ebenda, Seite 1/2.*

In der Praxis sieht es also so aus, dass eine Trennung von „Verwaltungsnetz“, dem neuen „Lehrernetz“ und den „Pädagogischen Netz“ hergestellt werden muss, um unerlaubten Datenzugriff zu unterbinden. Dies kann sowohl physikalisch, also über eine auf Hardware-Ebene getrennte Netzwerkinfrastruktur, als auch logisch über die Einrichtung von VLANs geschehen.

Ein Beispiel für eine VLAN-Infrastruktur finden Sie unter http://www.it.kultus-bw.de/site/pbs-bw-new/get/params_Dattachment/1916479/3VLANs.pdf .

Die folgende Tabelle bietet eine Übersicht über die drei Netze:

Netzwerk	**Berechtigter Personenkreis**	**Aufgaben**
„**Arbeitsumgebung Schulleitung**“ (Verwaltungsnetz)	Verwaltung, Direktion	▪ Schulverwaltungssoftware ▪ Verwaltung von Daten der Schüler und Schülerinnen, der Sorgeberechtigten und der Lehrkräfte ▪ Erledigung von hoheitlichen Aufgaben wie der Zeugniserstellung
„**Arbeitsumgebung Lehrkräfte**“ (Lehrernetz)	Lehrer	▪ Unterrichtsvorbereitung ▪ Eingabe von Bewertungen oder Benotungen
„**Unterrichtsumgebung**“ (Pädagogisches Netz)	Lehrer, Schüler	▪ Durchführen des Unterrichts

Tabelle 1 – Übersicht über Netze in der Schule

Das Lehrernetz kann als eine Art „Zwischenbereich“ zwischen Pädagogischem Netz und Schulverwaltung verstanden werden. Von dort aus darf auf freigegebene Ressourcen der beiden anderen Netze zugegriffen werden, um Daten auszutauschen.

> *„Vom Lehrernetz aus ist ein geregelter Zugriff in Richtung auf das Schulverwaltungsnetz auf ausgewählte Ressourcen zulässig, wenn sichergestellt ist, dass keine personenbezogenen Daten vom Schulverwaltungsnetz dabei im Lehrernetz physikalisch abgelegt werden können.“*
>
> *Ebenda, Seite 3*

Um den Zugriff aus dem Lehrernetz in das Verwaltungsnetz netzbriefkonform zu realisieren, sind Kenntnisse bezüglich der lokal individuellen Verwaltungsnetz-Implementierung erforderlich.

Bitte wenden Sie sich diesbezüglich an Ihren vor Ort zuständigen Dienstleister!

> *„Ein Zugriff durch Lehrkräfte vom Lehrernetz aus auf die Unterrichtsumgebung ist zulässig. Jeglicher Schülerzugriff auf das Lehrernetz ist unzulässig. Ein Zugriff vom Klassenzimmer aus auf dieses Netz ist zu verhindern.“*
>
> *Ebenda, Seite 3*

Zugriffe zwischen dem Lehrernetz und dem Pädagogischem Netz werden – unter Berücksichtigung der paedML Standards – in der vorliegenden Anleitung behandelt.

Neben der Dreiteilung des schulischen Netzes ist aber auch weiterhin möglich, dass in der Schule nur zwei Netze (Verwaltungsnetz und Pädagogisches Netz) betrieben werden.

> *„Alternativ ist auch eine Netzinfrastruktur zulässig, die lediglich aus zwei Netzen besteht. Dabei ist jedoch zu beachten, dass nur die Umgebung für die Schulleitungsumgebung und Lehrkräfte zusammengefasst sein dürfen. Die Unterrichtsumgebung muss getrennt realisiert sein, ein Übergang in das andere Netz ist nicht zulässig.“*
>
> *Ebenda, Seite 4*

Trennung der Datenablage vom Pädagogischen Netz und Verschlüsselung

> *Zeugnisse, Lernstandsberichte, Halbjahresinformationen und vergleichbare Dokumente dürfen in der **Unterrichtsumgebung** generell nicht verarbeitet werden.*
>
> *Ist jedoch beabsichtigt, weitere personenbezogene Daten von Schülern in der Unterrichtsumgebung zu verarbeiten, beispielsweise laufende Leistungsbeurteilungen (Einteilung in Niveaustufen oder der Einsatz von Kompetenzrastern), müssen zwingend die folgenden technischen Datenschutzmaßnahmen getroffen werden.*
>
> - *Eine **Datenspeicherung in der Unterrichtsumgebung ist unzulässig**. Die Datenspeicherung muss in einem eigenen Netz (auch VLAN) auf einem eigenen Server (auch virtueller Server) erfolgen. Ein auf die notwendigen Dienste begrenzter, dedizierter Zugriff vom pädagogischen Netz aus auf diesen Server ist auf Applikationsebene zulässig. Durch ein Berechtigungssystem ist sicherzustellen, dass jeder Benutzer nur Zugang zu den für ihn bestimmten Daten erhält. Die Datenspeicherung kann auch außerhalb des Schulnetzes, beispielsweise bei einem Dienstleister, erfolgen; in diesem Fall sind auch die Vorgaben für eine sog. Auftragsdatenverarbeitung nach § 7 LDSG zu beachten.*
> - *Als Identitätsnachweis ist für jeden Nutzer eine **Zwei-Faktoren-Authentifizierung** erforderlich, die aus der Kombination von zwei verschiedenen voneinander unabhängigen Komponenten (Faktoren) besteht. Zusätzlich zum üblichen Passwort ist der Besitz eines "elektronischen Schlüssels" erforderlich. Denkbar wäre die Verwendung von Hardwaretokens oder von Einmal-Passwörtern (timebased one-time-Passwort, nach dem TOTP- bzw. OTP-Verfahren). Bei der Verwendung eines Einmalpassworts muss die Passworterzeugung zwingend auf einem zweiten Gerät erfolgen. Alternativ könnte auch eine TAN-Liste verwendet werden.*
> - *Jede unverschlüsselte Übermittlung dieser personenbezogenen Daten im Unterrichtsnetz ist unzulässig. Die übertragenen Daten müssen vollständig **Ende zu-Ende** verschlüsselt sein, d.h. sie werden auf dem gesamten Weg zwischen Server und Empfänger verschlüsselt.*
>
> *Ebenda, Seite 4/5 (keine Hervorhebungen im Original)*

Dieses Zitat verdeutlicht nochmals, dass personenbezogene Daten NICHT im Pädagogischen Netz abgelegt werden dürfen!

Die Verarbeitung im Unterrichtsnetz (Pädagogisches Netz) ist prinzipiell möglich, wobei Daten nicht im Unterrichtsnetz gespeichert werden dürfen. Für die Übertragung der Daten aus dem Unterrichtsnetz ist eine verschlüsselte Ende-zu-Ende-Verbindung mit „Zwei-Faktoren-Authentifizierung“ zwingend erforderlich.

Beachten Sie die folgenden Hinweise für die Einrichtung eines Lehrernetzes!

1. Eine Grundvoraussetzung für die Realisierbarkeit eines sicheren Lehrernetzes ist die Verfügbarkeit von physikalisch zutrittsbeschränkten Lehrerarbeitsplätzen im Schulgebäude. In der Praxis sind dies zum Beispiel Rechner in einem abschließbaren Lehrerzimmer, zu welchem Schüler und sonstige unbefugte Dritte keinen unbeaufsichtigten Zugang haben.
2. Ein netzwerktechnischer "Abhörschutz" von Lehrerarbeitsplätzen gegenüber Zugriffsversuchen aus dem Schülernetz (z.B. Klassenraum) ist nur gegeben, wenn die Benutzeranmeldung des Lehrers an einer Arbeitsstation erfolgt, welche tatsächlich zum IP-Netzwerk des einzurichtenden Lehrernetzes gehört und dieses fachgerecht gemäß der vorliegenden Anleitung – per VLAN-Technologie getrennt von anderen Schulnetzen – eingerichtet wurde.
3. Eine Absicherung des Lehrerarbeitsplatzes gegen nicht-netzwerk-basierte Abhör- bzw. Spionageversuche (z.B. Installation von Hardware-Keyloggern, Spionage-Software oder Spy-Cams) kann nur gewährleistet werden, wenn diese Arbeitsplätze durch physikalische Zutrittsbeschränkungen geschützt werden (s. Hinweis 1).
4. Gegen den unbedachten Umgang mit Lehrer-Passwörtern im Unterrichtsalltag, gibt es keine technischen Sicherungsmaßnahmen. Das „Über-die-Schulter-schauen-lassen bei Passwort-Eingabe" oder gar die Weitergabe des Passworts an Dritte sollten ebenso vermieden werden, wie der selbstklebende Notizzettel mit Kennwörtern, der am Bildschirm oder unter der Tastatur befestigt wurde.

Unter http://www.it.kultus-bw.de/site/pbs-bw-new/get/params_Dattachment/1916479/3VLANs.pdf findet sich ein Beispiel für die Trennung der verschiedenen Netzsegmente. Hierbei wird ein optionaler Server für das Lehrernetz ausgewiesen.

Das hier beschriebene Verfahren trennt den Verkehr zwischen den einzelnen Netzsegmenten (Lehrernetz und Pädagogisches Netz). Gleichzeitig ermöglicht es Nutzern beider Netze, auf Ressourcen auf dem Schulserver im Pädagogischen Netz zuzugreifen.

Um zu vermeiden, dass Unbefugte auf Schülerdaten zugreifen, müssen die Daten zusätzlich geschützt werden. Dies können Sie über verschiedene Wege realisieren:

1. Speichern der Daten auf einem verschlüsselten USB-Stick. Die Verschlüsselung ist wichtig, um die Daten zu schützen, falls der USB-Stick abhandenkommt.
2. Einrichtung eines Servers im Lehrernetz. Sofern dieses System über ein Rechte-Management verfügt und die Daten der einzelnen Benutzer voneinander getrennt sind, muss keine Verschlüsselung erfolgen.

3. Eigener Datenspeicher (NAS/Server/…), der nur im Lehrernetz erreicht werden kann. Hierfür bietet sich beispielsweise das kostenlose Betriebssystem FreeNAS[2] an, welches als vmware-Installation auf dem Virtualisierungsserver installiert werden kann. Jeder Benutzer muss in diesem Fall ein eigenes Verzeichnis pflegen und die Daten verschlüsseln.

Hierbei muss in beiden Fällen auf ein Rechtesystem geachtet werden, dass den Zugriff durch unbefugte Dritte (zum Beispiel pädagogische Mitarbeiter, die mit der Benotung nicht betraut sind) verhindert.

Konsultieren Sie in Fragen zur Umsetzung eines Datenspeichers bitte Ihren Dienstleister.

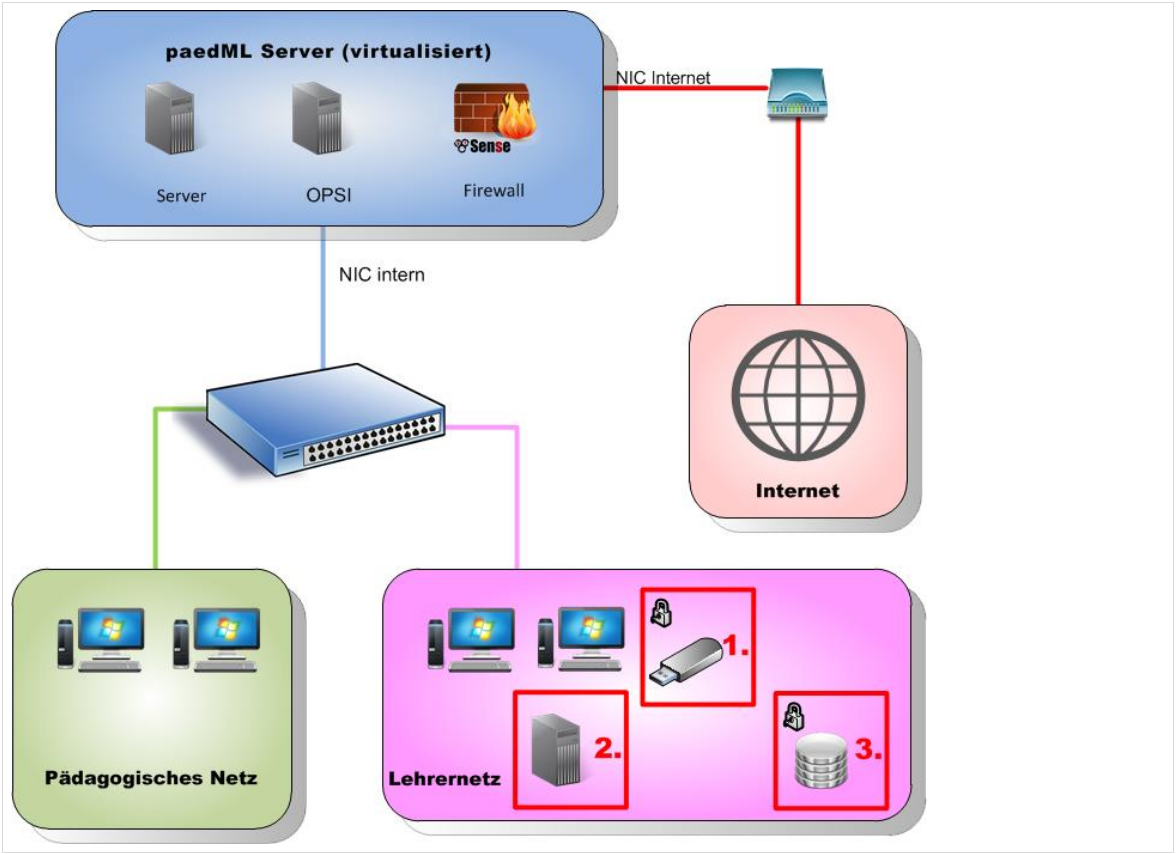

Abb. 1: Sicherung sensibler Daten durch Netztrennung und eigenen Container

[2] http://www.freenas.org/download/

Es wird dringend empfohlen, dass Sie vor der Umsetzung der „*Arbeitsumgebung Lehrkräfte*“[3] die folgenden Unterlagen konsultieren:

- http://www.it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Netztechnik+_+Netzbrief
- http://lehrerfortbildung-bw.de/sueb/recht/grund/verwalt/

2. Übersicht der Netze in der paedML Linux

Die paedML Linux wird im Auslieferungszustand mit dem „Pädagogischen Netz“ (der Unterrichtsumgebung) und dem „Gästenetz“ (dem Netzwerk, in das schulfremde Geräte aufgenommen werden können) ausgeliefert.

Neben einer Netzwerkkarte für das Pädagogische Netz und einer Netzwerkkarte für das (optionale) Gästenetz wird eine dritte Netzwerkkarte am Virtualisierungs-Server benötigt, über die eine Verbindung zum Internet hergestellt wird.

Die folgende Abbildung zeigt die Standard-Netzwerke der paedML Linux im Auslieferungszustand:

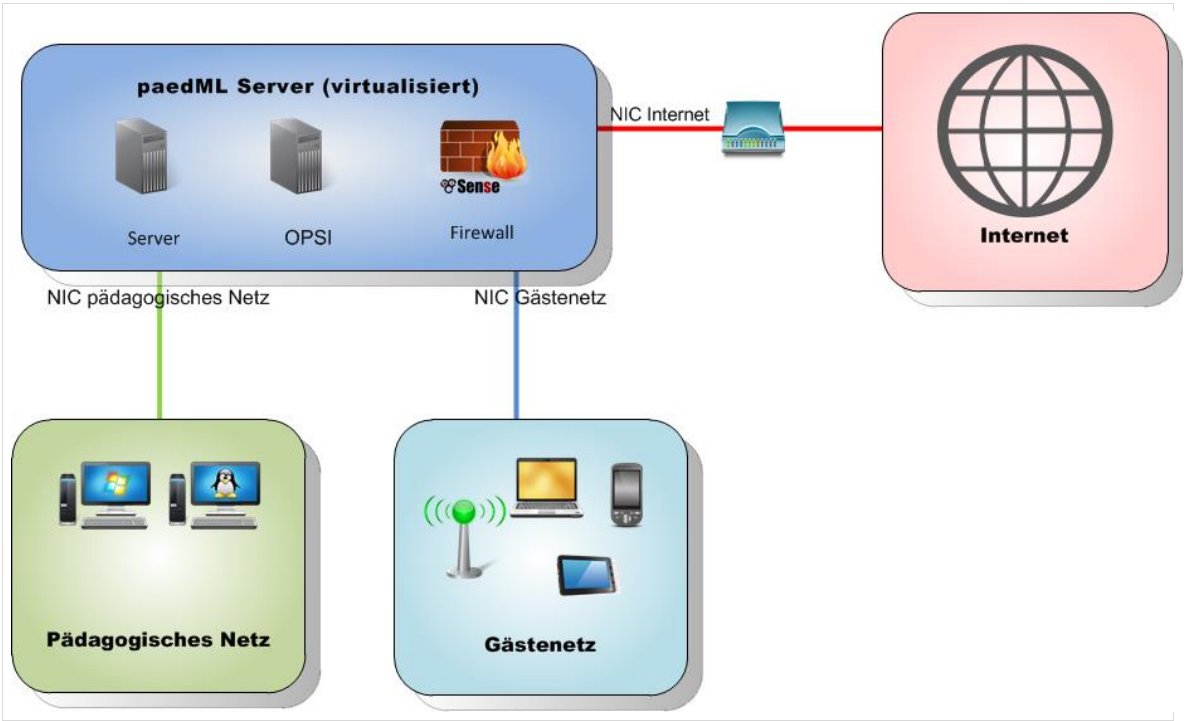

Abb. 2: Standard-Netze der paedML Linux

[3] Netzbrief vom September 2015 (http://www.it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Netztechnik+_+Netzbrief)

Im Folgenden werden die möglichen Netzwerkkonfigurationen der paedML beschrieben:

2.1 Auslieferungszustand

In der paedML Linux ist die Erweiterung der Netzsegmente vorbereitet, aber nicht eingerichtet[4]. Dies bedeutet, dass Sie die paedML ohne weitere Anpassungen verwenden können. Sie haben nur ein Netz, das „Pädagogische Netz“, in dem sich alle Clients und Server der Unterrichtsumgebung befinden. Auf das „Lehrernetz“ und ein großes Pädagogisches Netz muss bei dieser Konfiguration jedoch verzichtet werden.

2.2 Aufteilung des Schulnetzes in getrennte Netzsegmente

Um die erweiterte Netzwerkinfrastruktur einzurichten, wird an die Netzwerkkarte des pädagogischen Netzes ein Layer3-Switch angeschlossen, der entsprechend konfiguriert werden muss (vgl. Kapitel 3, ab Seite 16).

Über diesen Switch wird bei Konfigurationen mit Lehrernetz der Netzverkehr zwischen den verschiedenen Netzsegmenten getrennt.

Auch das „große“ Pädagogische Netz, sowie individuelle Netzwerkkonfigurationen werden über den Switch zur Verfügung gestellt.

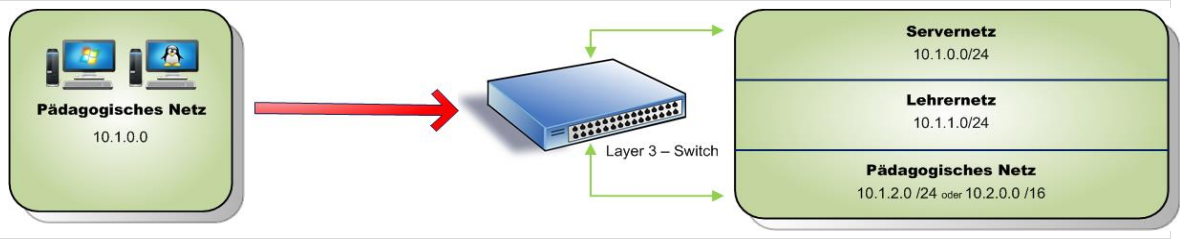

Abb. 3: Schematische Darstellung: Aus dem „alten“ pädagogischen Netz werden drei Netze

Das Gästenetz erhält keine Anpassungen.

2.2.1 IP-Segment „Servernetz“

Um den Datenverkehr des Lehrernetzes vom pädagogischen Netz abzuschirmen, muss zusätzlich eine Zwischenschicht (Servernetz) eingeführt werden. Auf dieses Netzsegment kann aus den andern Netzbereichen zugegriffen werden, ohne dass der jeweilige Netzwerkverkehr für das andere Netz sichtbar ist.

[4] Bestandskunden, die ihr System vor der Implementierung der Netzerweiterung (paedML Linux 6.0, Errata 2) installiert haben, bekommen die Netzsegmente automatisch über ein Update installiert, müssen die Netzsegmente aber noch einrichten (vgl. Kapitel 7, Seite 44).

Im bisherigen Netzsegment „Pädagogisches Netz“ (IP-Adressraum 10.1.0.0/ 24) laufen weiterhin die paedML Server. Hier können auch eigene Systeme für zentral erreichbare Dienste eingerichtet werden (z.B. zusätzliche Geräte für eigene Webserver, AdminVM, Drucker…).

Der IP-Bereich „Pädagogisches Netz“ wird bei der Einrichtung der hier beschriebenen Netzwerkerweiterungen zum „Servernetz“.

2.2.2 IP-Segment „Lehrernetz“

Im neu hinzugekommenen IP-Adressraum 10.1.1.0/24 ist das neue Lehrernetz beheimatet. Hier stehen Ihnen 219 IP-Adressen für Geräte des Lehrernetzes zur Verfügung.

2.2.3 IP-Segment „Pädagogisches Netz“

Wenn Sie Ihr Schulnetz um ein „Lehrernetz“ erweitern, wird zusätzlich ein neues Netzsegment „Pädagogisches Netz“ eingeführt, in dem der Unterricht stattfindet. Dieses „neue Pädagogische Netz“ enthält einen anderen IP-Adressraum (10.1.2.0/ 24, oder 10.2.0.0/ 16) als das „alte Pädagogische Netz“. Im pädagogischen Netz sind NUR Arbeitsplatz-Rechner und keine Server.

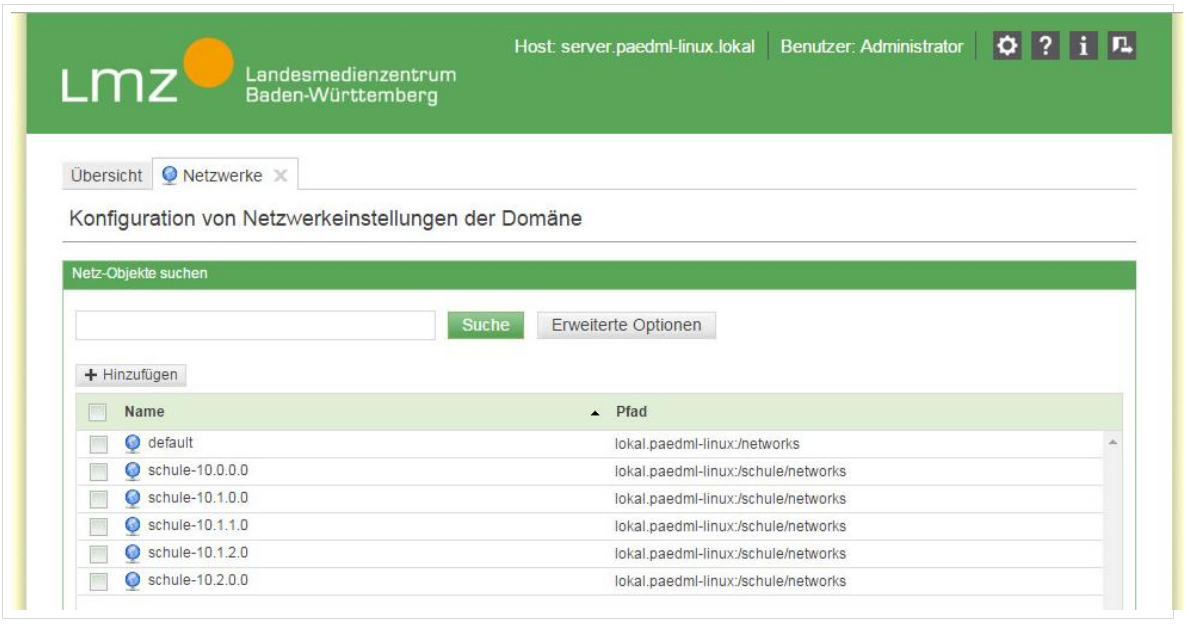

Abb. 4: Übersicht der paedML Netzwerkinfrastruktur mit neuen Netzsegmenten

2.3 Pädagogisches Netz – „kleines Netz“ oder „großes Netz“?

Mit der Einführung der hier beschriebenen Netzerweiterungen kann die Netzwerkkonfiguration der paedML Linux dergestalt angepasst werden, dass ein größerer IP-Adressbereich für das pädagogische Netz zur Verfügung gestellt wird.

Es gibt die Möglichkeit bei der Netzwerkerweiterung aus einem von zwei Pädagogischen Netzen, die sich in Umfang und Adressbereich unterscheiden, zu wählen.

	Pädagogisches Netz (klein)	Pädagogisches Netz (groß)
IP-Adressbereich	10.1.2.0/24	10.2.0.0/16
Anzahl der IP-Adressen[5]	254	65534

Tabelle 2 - Verschiedene IP-Adressbereiche

Das „große“ Pädagogische Netz bietet die Möglichkeit, dass Sie Netzadressen wählen können, die den Raumbezeichnungen Ihrer Schule entsprechen.

Sie können beispielsweise eigene IP-Adressbereiche für Räume vergeben (Raum 118 erhält den Adresspool 10.2.118.0, Raum 119 den Adresspool 10.2.119.0). Hierbei handelt es sich jedoch nur um eine Adresskosmetik und um keine Trennung der Netzsegmente, da sich die Adressen im gleichen Subnetz befinden.

Um die Netzwerke einzelner Räume voneinander zu isolieren, müssen die Hinweise in Kapitel 10 (ab Seite 46) umgesetzt werden.

Schulen die nicht mehr als 198 Client-IP-Adressen (inklusive Drucker und Peripherie-Geräte) benötigen, wird empfohlen das kleine Pädagogische Netz zu nutzen.

Beim Anlegen von Rechnern über die Netzwerkaufnahme via PXE-Boot muss unbedingt darauf geachtet werden, dass die Rechner im „großen“ Pädagogischen Netz mit der Subnetzmaske 255.255.0.0 angelegt werden, da sonst ein neues Netz angelegt wird, das in der paedML ohne Funktion ist!

Rechner, die falsch aufgenommen wurden, können nicht auf Funktionen (z.B. opsi, Schulkonsole,…) der paedML zugreifen.

[5] Nicht alle IP-Adressen können fest zugewiesen werden, da Adressen für die Rechneraufnahme via DHCP reserviert sind.

3. Vorbereitungen für die Switch-Konfiguration

Die Konfiguration des Layer3-Switches wird exemplarisch anhand des 10 Port Cisco „SG 300-10“-Switches beschrieben.

Cisco „SG 300“-Switches gibt es in verschiedenen Ausführungen, die sich beispielsweise in der Anzahl der Ports unterscheiden. Das größte Modell hat 50 Hardware-Ports.

Die „SG 300“-er Baureihe ist für kleine bis mittelgroße Netzwerke geeignet und kann bis zu 300 Endgeräte versorgen.

VLAN-fähige Layer3 Switche anderer Hersteller können entsprechend eingebunden werden. Bitte vergleichen Sie vor Beschaffung die jeweiligen Kenndaten, um Fehlanschaffungen zu vermeiden.

Die Konfiguration des Netzwerkes ist originäre Aufgabe des Dienstleisters. Erfahrene Netzwerkberater, die gewillt sind diese Aufgabe zu übernehmen, können sich in die Thematik einarbeiten – es kann jedoch nicht von Netzwerkberatern verlangt werden, sich in die Tiefen der VLAN-Konfiguration einzuarbeiten.

Die Konfiguration des Schulnetzes kann nur beratend durch die Mitarbeiter der paedML Hotline unterstützt werden, da sie die Begebenheiten vor Ort in der Regel nicht kennen.

3.1 Aufnahme des Switches in die paedML Linux

Um das Gerät in Ihrem paedML Linux-Netzwerk zu betreiben, müssen Sie, wie im Administrator-Handbuch[6] Kapitel „*Verwaltung von Geräten*“ beschrieben, das Gerät in die paedML Linux aufnehmen. Dies geschieht über das Schulkonsolen-Modul „Schul-Administration | Rechner (Schulen)“. Verbinden Sie hierfür einen Port des Geräts mit dem pädagogischen Netz. Nehmen Sie den Switch als „*Gerät mit IP-Adresse*“ in die paedML auf.

[6] http://support-netz.de/technische-unterstuetzung/kundenportal/linux/dokumentationen.html

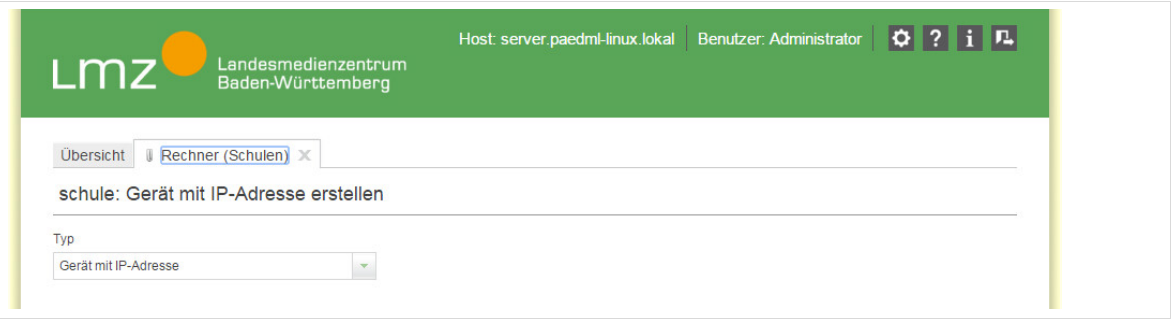

Abb. 5: Neuanlage eines Gerätes mit IP-Adresse

Vergeben Sie die IP-Adresse *10.1.0.10* / Subnetzmaske *255.255.255.0*.

Speichern Sie die Einstellungen ab.

3.2 Anschließen des Switches

Damit das Gerät konfiguriert werden kann, müssen Sie es direkt mit einem Rechner verbinden und über die statische IP-Adresse (*192.168.1.254* / Subnetzmaske *255.255.255.0*) des cisco-Routers zugreifen. Über diese IP-Adresse können Sie die Konfigurationsmaske des Switches aufrufen. Der Clientrechner muss dafür natürlich im gleichen Netz sein.

Beim ersten Login sind Benutzername und Kennwort auf den Wert `cisco` gesetzt. Sie müssen nach der Anmeldung das Kennwort ändern.

Nach dem Login steht Ihnen die Benutzeroberfläche zur Verfügung. Auf der linken Seite finden Sie die Menüstruktur, rechts den Inhalt des jeweils aktiven Menüpunktes. Oben rechts wird angezeigt, wenn Änderungen noch nicht in die Systemkonfiguration übernommen wurden. Das Gerät zeigt mit dem Hinweis „*Save*“ an, dass Daten gespeichert werden müssen.

Da Änderungen nicht automatisch gespeichert werden, ist es ratsam regelmäßig den Fortschritt der Konfiguration zwischen den einzelnen Arbeitsschritten zu speichern.

Hinweise zum Speichern der Konfiguration finden Sie in Kapitel 5 auf Seite 38.

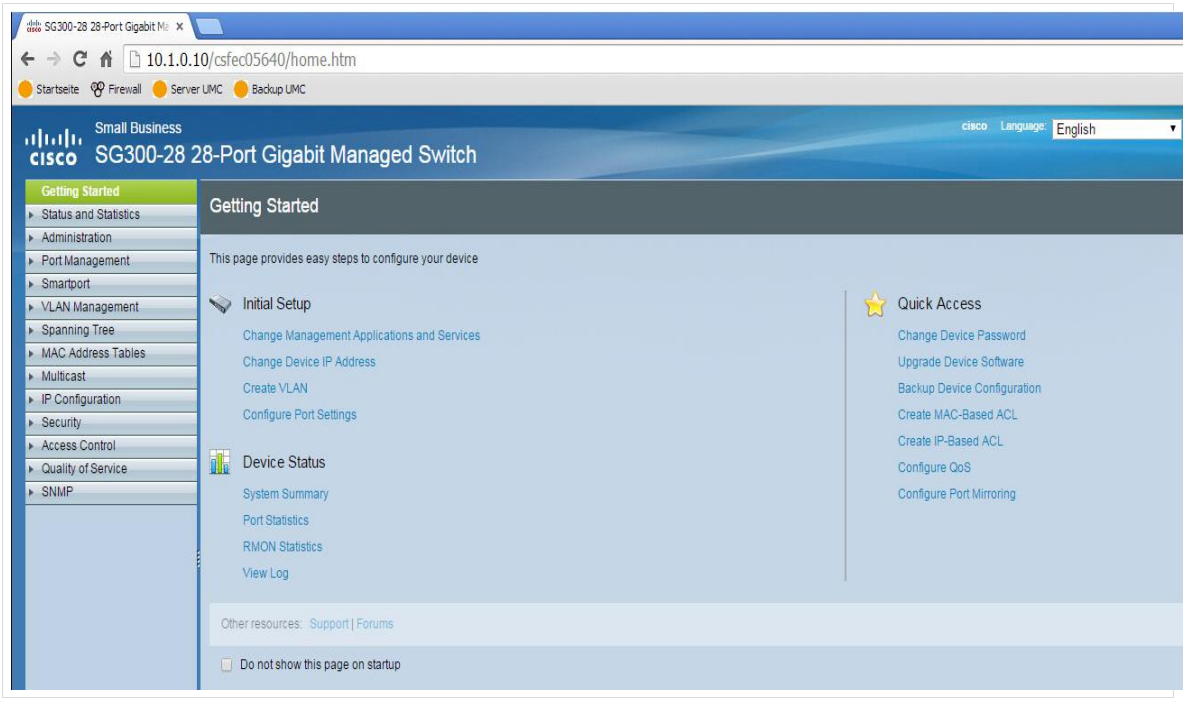

Abb. 6: Aufruf der Management-Oberfläche des Cisco-Switches

Während der Konfiguration wird die IP-Adresse des Gerätes umgestellt (vgl. Kapitel 4.3.1, Seite 23). Nach diesem Schritt ist der Switch über die Adresse *192.168.1.250* zu erreichen.

Wenn der Switch vollständig eingerichtet wurde, können Sie das Gerät mit dem Schulnetz verbinden und über die IP-Adresse 10.1.0.10 den Switch zugreifen.

Wir empfehlen dringend die Konfiguration komplett durchzuführen und das Gerät erst danach mit dem Schulnetz zu verbinden.

4. Konfiguration

Übersicht

Im Folgenden werden die Einstellungen – wie bereits beschrieben – an einem Cisco-Gerät vorgenommen. Sie können jedoch auch andere Hardware einsetzen. Die folgenden Arbeitsschritte sind notwendig, um eine sichere Trennung der schulischen Netzwerke zu erreichen:

1. Einrichtung der Netzsegmente (Definition der VLANS)
2. Zuweisung der Netzsegmente an Hardware-Ports (bei Cisco-Geräten wird hierbei auch definiert, wie der Netzverkehr innerhalb und zwischen den Netzen stattfindet).
3. Konfiguration der VLANS
   3.1. Vergabe definierter IP-Adressräume der Netze „SERVERNETZ“, „LEHRERNETZ“ und „PÄDAGOGIK“

3.2. Einrichten von Routen zwischen den Netzen (auf das „SERVERNETZ“ soll von den anderen beiden Netzen zugegriffen werden können (Datenablage, Imaging,…))
3.3. Einrichten von DHCP-Relaying (notwendig für Imaging)
3.4. Optional: Einrichten von „Wake On Lan“-Funktionalität.

4. Um „LEHRERNETZ“ und „PÄDAGOGIK“ voneinander zu trennen, werden Regeln eingerichtet (Access Control Lists) und den Netzen zugewiesen.
5. Abschließend muss noch beachtet werden, dass das Spanning-Tree-Protokoll zu Problemen bei der Rechneraufnahme führt und hierfür Einstellungen getätigt werden müssen.

4.1 Einrichtung der Netzsegmente

4.1.1 Aktivieren der Layer3-Switch-Funktionalität

Dieser Schritt muss zwingend als erster Schritt ausgeführt werden.

Bei unseren Tests im Labor waren alle Einstellungen des Gerätes zurückgesetzt, die vor diesem Arbeitsschritt konfiguriert wurden!

Nach Anmeldung am Gerät muss zunächst einmal der System-Modus für den Layer3-Switch aktiviert werden. Dies geschieht über den Menüpunkt "*Administration* | *System Settings*". Dort muss das Optionsfeld "*System Mode*" auf „*L3*“ eingestellt sein. Die Konfiguration wird über den Button "*Apply*" gespeichert.

Anschließend wird das Gerät neu gestartet. Der Neustart dauert einige Minuten! Hierbei werden alle Einstellungen zurückgesetzt. Auch das Kennwort muss erneut geändert werden.

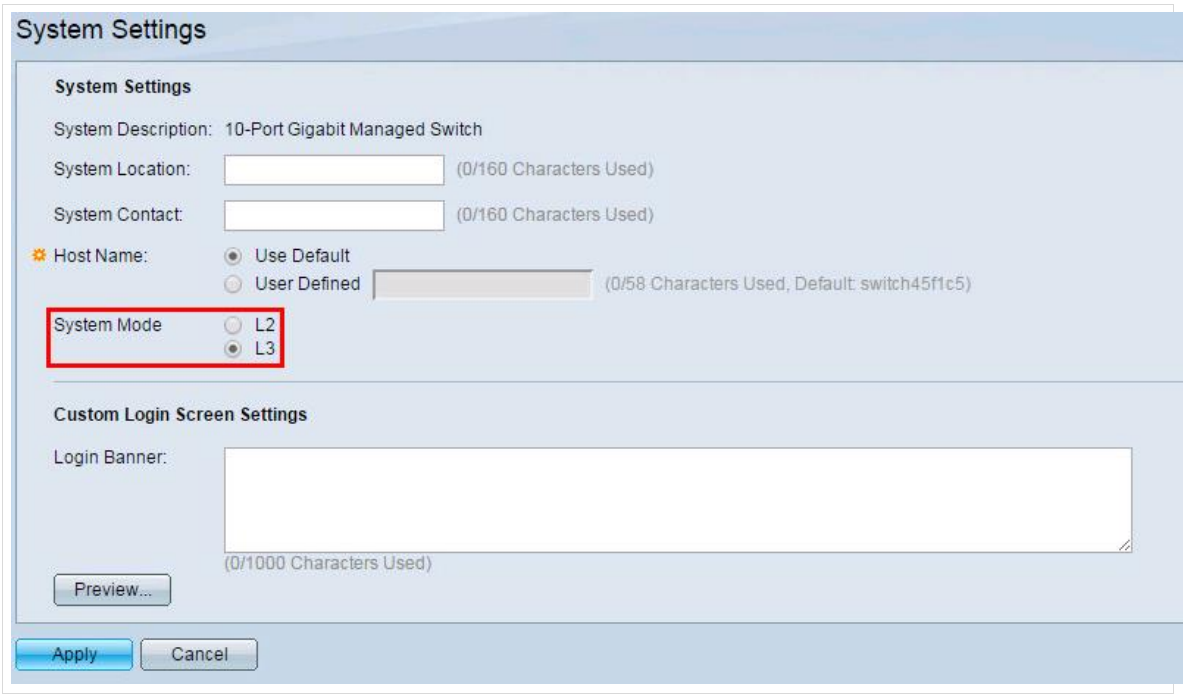

Abb. 7: Aktivieren der Layer3-Funktionalität.

4.1.2 Anlegen der VLANs

Über virtuelle LANs (VLANs) wird das pädagogische Netz um Netzsegmente erweitert. Die folgende Tabelle gibt eine Übersicht über die IP-Adressräume und die VLAN-ID.

Netzwerkname	IP-Adresse	VLAN-ID
SERVERNETZ	10.1.0.0/24	10
LEHRERNETZ	10.1.1.0/24	20
PAEDAGOGIK[7]	10.1.2.0/24	30
PAEDAGOGIK-GROSS[8]	10.2..00/16	40

Tabelle 3 - Zuweisung von paedML-Netzen an VLANs

Die Konfiguration der VLANs geschieht über den Menüpunkt "*VLAN Management* | *Create VLAN*".

Auf dem Gerät ist ein Management Netz angelegt (*VLAN ID 1*). Hier darf nichts geändert werden.

Über den Button "*Add...*" können die VLANs erstellt werden.

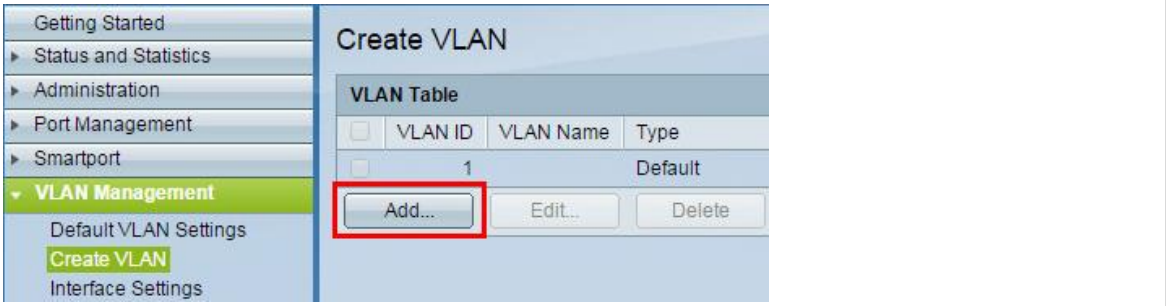

Abb. 8: Hinzufügen von VLANs

Die VLAN-IDs „*10*“, „*20*“, „*30*“ oder „*40*“, müssen nacheinander über den folgenden Dialog erstellt werden.

Im Feld "*VLAN ID*" muss die VLAN-ID eingetragen werden, im Feld "*VLAN Name*" der entsprechende Name des VLANs. Über den Button "*Apply*" wird die Konfiguration hinzugefügt.

[7] „Kleines“ Pädagogisches Netz

[8] „Großes“ Pädagogisches Netz

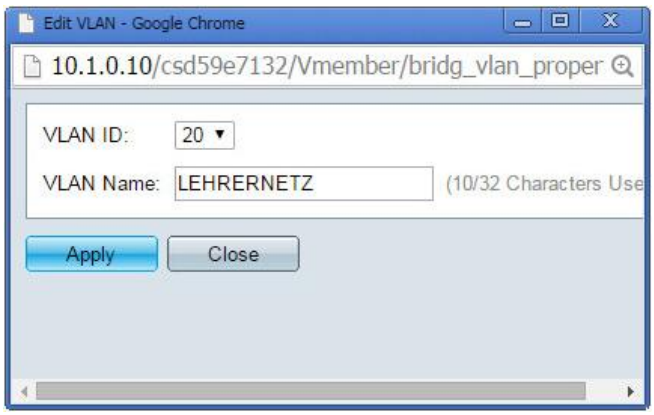

Abb. 9: Exemplarische Einrichtung des VLANs „LEHRERNETZ“

Wenn alle VLANs angelegt wurden, sehen Sie diese in der Übersicht („*VLAN Management* | *Create VLAN*“).

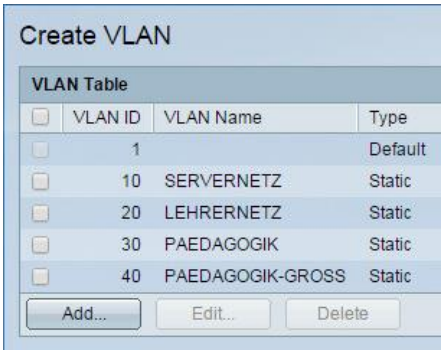

Abb. 10: Übersicht über die neu angelegten VLANs

4.2 Zuweisung der Hardware-Ports an VLANs auf dem Switch

Die neu angelegten VLANs sind nach der Einrichtung an keinen Anschluss (Port) am Switch zugeordnet. Im nächsten Schritt müssen daher die eingerichteten VLANs an einen (oder mehrere) Port(s) des Switches zugewiesen werden.

Überlegen Sie sich, wie Sie die Ports des Switches so belegen, dass beim Patchen nicht versehentlich falsche Netzsegmente mit den zugewiesenen Ports verbunden werden.

Dies kann über Aufkleber auf dem Gerät oder über eine Farbcodierung von Port und Kabel geschehen (z.B. grün = Pädagogisches Netz, blau = Servernetz, rot = Lehrernetz).

Über den Menüpunkt „*VLAN Management* | *Port to VLAN*“ findet die Zuweisung der Ports an die VLANs statt.

Über das Dropdown-Menü „*VLAN-ID equals to* `WERT`“ müssen Sie zunächst auswählen, welchen Port Sie an welches VLAN zuweisen wollen. Klicken Sie auf die Schaltfläche „*Go*“, um zu den Einstellungen des ausgewählten VLANs zu gelangen.

Nun wählen Sie aus, an welchen Hardware-Ports des Switches das VLAN verfügbar sein soll. Dies geschieht über das Aktivieren der Radio-Buttons in der Matrix.

In der oberen Zeile können Sie ein „*Interface*“ bestimmen, das Sie mit den darunter stehenden Werten konfigurieren können.

Wählen Sie die folgenden Werte aus, um die Ports an ein VLAN zuzuweisen, oder für ein VLAN zu deaktivieren:

- *Excluded* – Dieser Wert verhindert, dass das VLAN auf anderen Ports als den ausgewählten verfügbar ist.
- *Tagged* – Dieser Wert fügt den IP-Paketen einen VLAN-Tag hinzu**. Das Feld sollte nur dann aktiviert werden, wenn das nächste Gerät den VLAN-Tag bearbeiten kann** (zum Beispiel bei kaskadierten Switches).
- *Untagged* – Dies ist der Standard-Wert, der verwendet werden sollte, wenn es sich bei den angeschlossenen Geräten um „normale Endgeräte“ handelt, die VLAN-Tags nicht verarbeiten können.

Im folgenden Screenshot wird das Servernetz (VLAN-ID 10) an die Hardware-Ports eins bis drei des Switches zugewiesen:

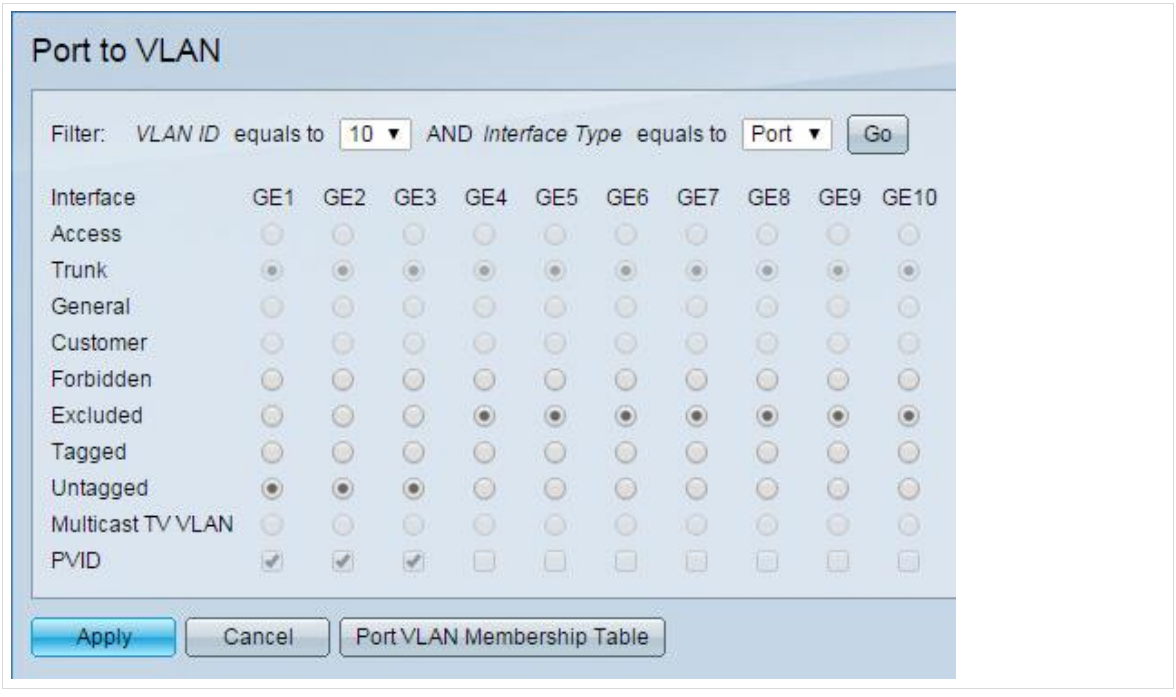

Abb. 11: Zuweisung der Hardware-Ports an das Servernetz

Über den Menüpunkt „*VLAN Management* | *PortVLAN Membership*“ erhalten Sie eine Übersicht, welche VLANs an welchem Hardwareport („*GE*“) anliegen. In der Kopfzeile sehen Sie eine Agenda, in der die einzelnen Werte der Spalte „*Administrative VLANs*“ aufgeschlüsselt sind.

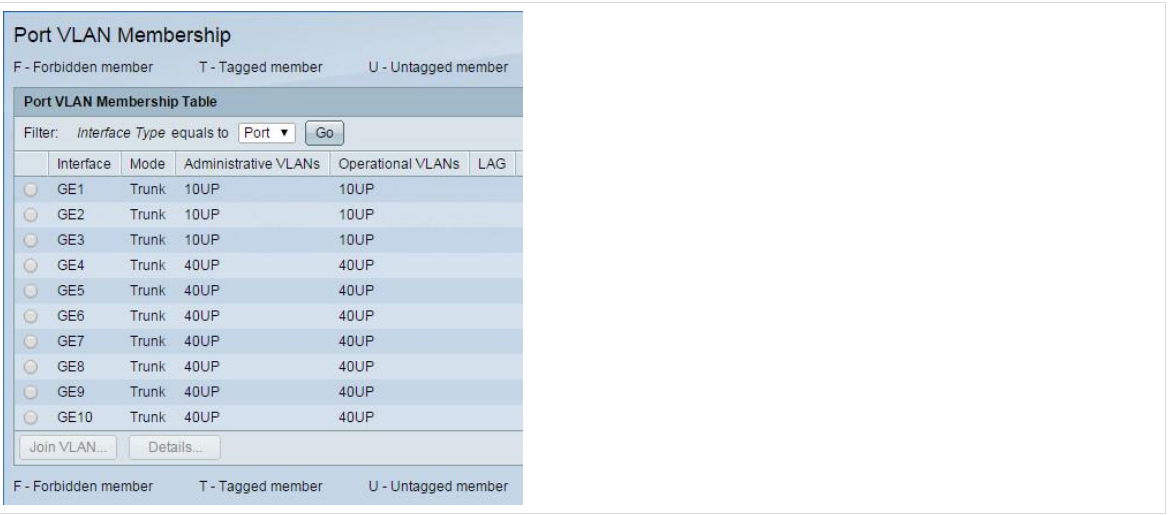

Abb. 12: Übersicht über die Port-VLAN-Zuordnung (großes Pädagogisches Netz, ohne Lehrernetz)

4.3 Konfiguration der VLANs

Die VLANs sind jetzt angelegt und an Ports des Routers zugewiesen, aber noch keinem Netzsegment zugeordnet. Dies geschieht im folgenden Abschnitt.

4.3.1 Zuweisung von IP-Adressen an die VLAN-Ports

Die folgende Tabelle zeigt welche IP-Adresse an welches VLAN zugewiesen wird. Unter dieser IP-Adresse, ist der Switch aus dem jeweiligen Netzsegment erreichbar. Die Adresse ist der Gateway des jeweiligen Netzsegmentes.

(Netz)	Interface	IP Address Type	IP Address	Mask
Default-Netz	VLAN 1	Static	192.168.1.250	255.255.255.0
(SERVERNETZ)	VLAN 10	Static	10.1.0.10	255.255.255.0
(LEHRERNETZ)	VLAN 20	Static	10.1.1.1	255.255.255.0
(PÄDAGOGIK)	VLAN 30	Static	10.1.2.1	255.255.255.0
(PÄDAGOGIK-GROSS)	VLAN 40	Static	10.2.0.1	255.255.0.0

Tabelle 4 - Adresszuweisung an VLAN-IDs

Die Zuweisung der IP-Adressen geschieht über den Menüpunkt "*IP Configuration* | *IPv4 Management and Interfaces* | *IPv4 Interface*". Fügen Sie über den Knopf „*Add…*“ die fehlenden IP-Adressen hinzu (1). Es öffnet sich ein neues Fenster, in dem **die folgenden Schritte für jedes VLAN ausgeführt werden müssen**.

Wählen Sie die im Dropdown-Menü „*VLAN*“ die VLAN-ID des jeweiligen Netzes aus (2).

Aktivieren Sie den „*IP Adress Typ(e)*“-Wert „*Static IP Adress*“ (3).

Tragen Sie den Wert für die IP-Adresse und die Subnetzmaske aus der vorigen Tabelle in die entsprechenden Felder ein (4).

Übernehmen Sie die Werte mit „*Apply*“ (5).

Als erste IP-Adresse muss die Adresse des VLANs 1 auf *192.168.1.250* (Empfehlung) geändert werden.

Sobald eine IP eines anderen Netzsegmentes vergeben wird, setzt der Switch dieses Netz als „Default-“ bzw. Management-Netz. Um einen weiteren Zugriff von dem Konfigurationsrechner (192.168.1.x) zu ermöglichen, ist dieser erste Schritt erforderlich.

Nach Änderung dieses Wertes müssen Sie als IP-Adresse die 192.168.1.250 in den Browser eingeben, um erneut auf den Switch zuzugreifen.

Wiederholen Sie den Vorgang für jedes VLAN (vgl. Tabelle) und schließen Sie den Dialog „*Add IP Interface*“ im Anschluss.

Der Knopf „*Apply*“ (6) in der Hauptmaske übernimmt die Änderungen (die damit aber nicht in die Konfiguration geschrieben werden („*Save*“-Knopf ganz oben rechts).

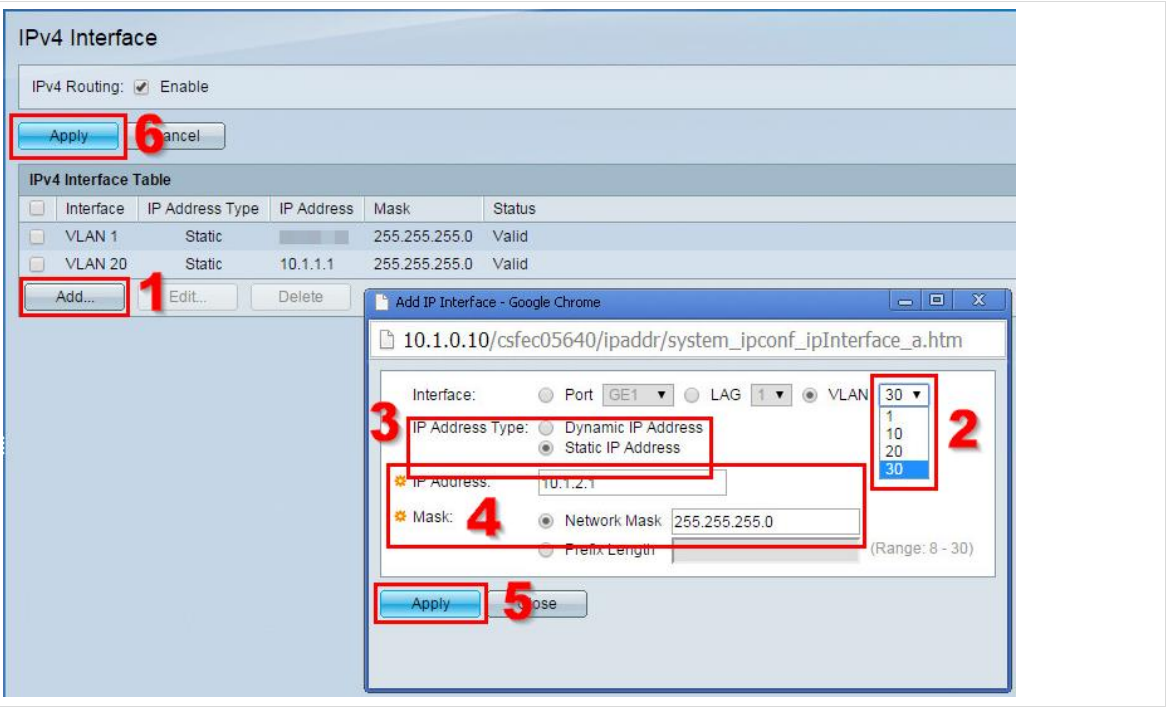

Abb. 13: Zuweisung von IP-Adressen an die VLANs

Wenn alle IP-Adressen richtig zugewiesen wurden, erhalten Sie die folgende Tabelle

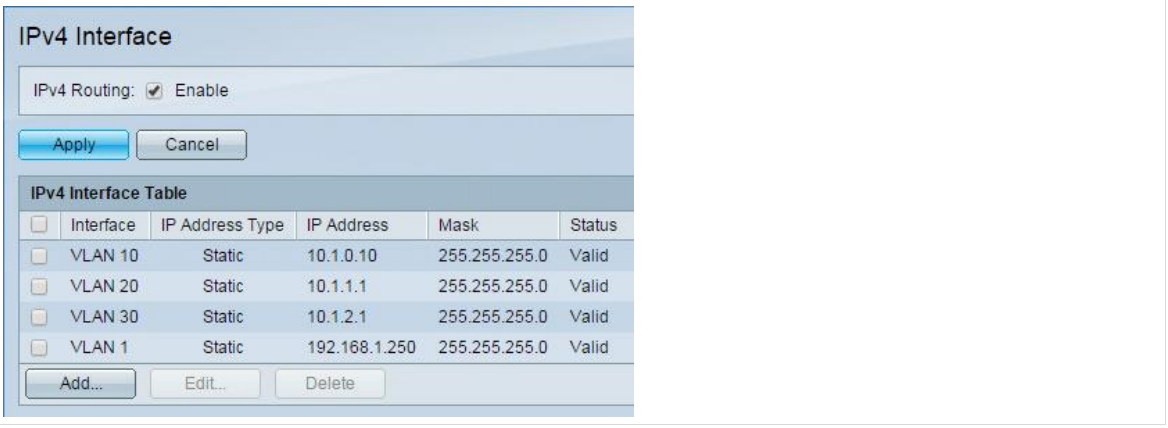

Abb. 14: Zuweisen der IP-Adressen an die VLANs

4.3.2 Konfiguration des Routings

Über den Menüpunkt "*IP Configuration* | *IPv4 Management and Interfaces* | *IPv4 Routes*" werden die IPv4-Routen definiert.

Überprüfen Sie hier, ob die Routen automatisch angelegt wurden.

In diesem Menü können bei Bedarf weitere Routen (für selbst angelegte Netzsegmente) definiert werden („*Add*"-Button).

ACHTUNG! Routen werden nur dann angezeigt, wenn ein Gerät an einen dem Netz zugewiesenen Port angeschlossen ist.

Es wird vermutlich so sein, dass Sie alles richtig konfiguriert haben, aber nicht alle Routen in der Übersicht angezeigt werden.

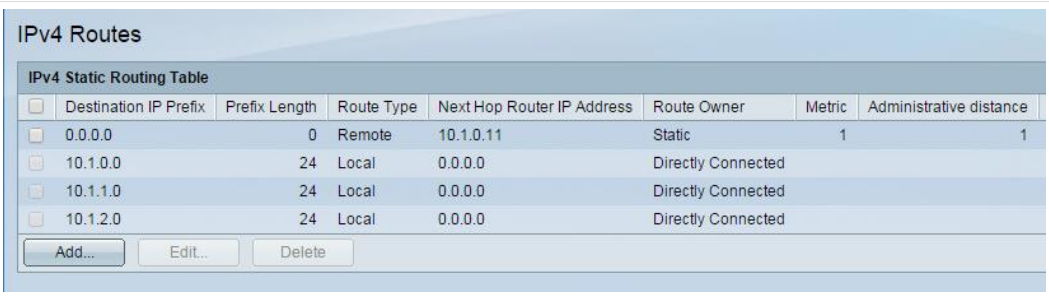

Abb. 15: Übersicht über die IPv4 Routen (ohne „großes" Pädagogisches Netz)

4.3.3 Aktivieren von DHCP-Relaying

Wenn ein Rechner im Schulnetz gestartet wird, bekommt er über den paedML Server eine IP-Adresse zugewiesen. Damit die DHCP-Anfrage vom Server (und nicht vom Layer3-Switch) beantwortet wird, muss sie vom Switch weiter geleitet werden. Dies geschieht über das sogenannte *DHCP-Relaying*.

IP-Adressen sind jeweils nur aus dem am Port des Switches angelegten Subnetz heraus verfügbar.

Sie aktivieren DHCP-Relaying über den Menüpunkt "*IP Configuration* | *DHCP Snooping/Relay* | *Properties*".

Im Bereich "*DHCP Relay Server Table*" muss über den Button "*Add...*" der DHCP-Server "*10.1.0.1*" (IP-Adresse des paedML Servers) hinterlegt werden (1). Einen Screenshot hierzu sehen Sie in der übernächsten Abbildung.

Anschließend müssen Sei den Haken bei „*DHCP Relay* | *Enable*“ setzen (2).

Speichern Sie die Einstellungen mit „*Apply*“ (3).

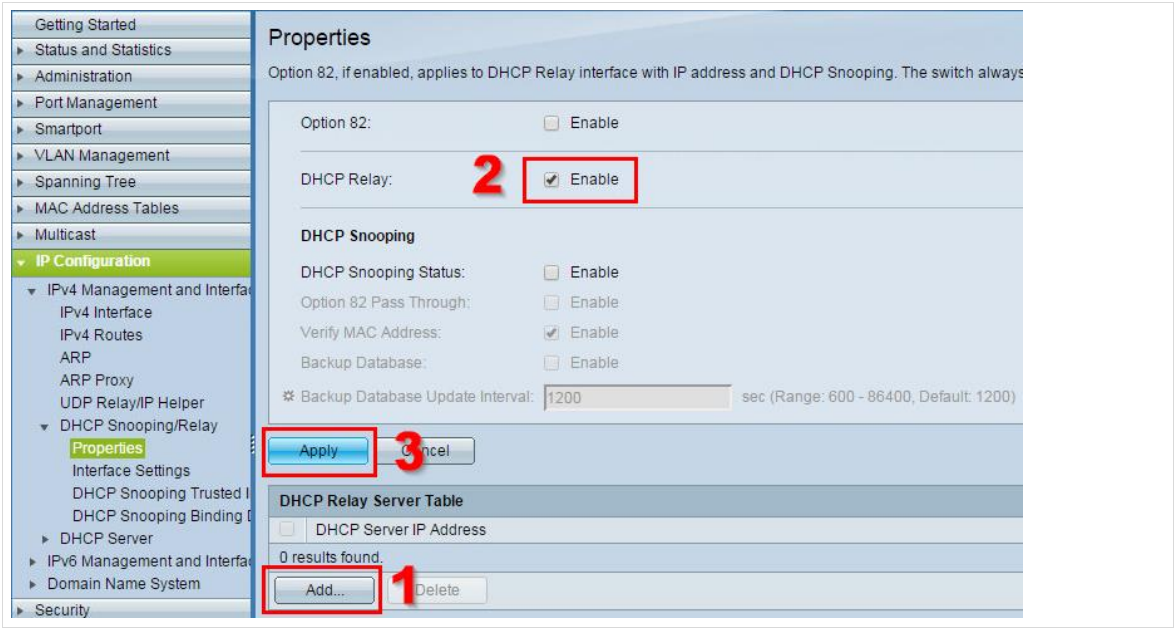

Abb. 16: Einstellungen für das DHCP-Relaying

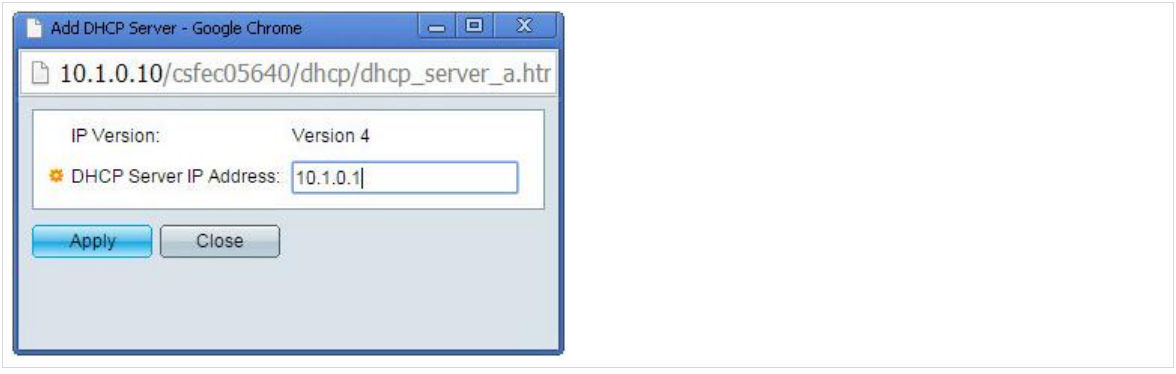

Abb. 17: Eintragen des DHCP-Servers nach Betätigung der „Add…“-Schaltfläche

Nach der erfolgten Einrichtung werden alle DHCP-Anfragen an den paedML Server weitergeleitet.

Über den Menüpunkt "*IP Configuration* | *DHCP Snooping/Relay* | *Interface Settings*" werden anschließend die IP-Adressen der VLANs hinterlegt.

Über „*Add*“ können Sie festlegen, über welche Interfaces DHCP-Anfragen weiter geleitet werden.

Die Weiterleitung von Anfragen aus dem Servernetz ist nicht nötig, da sich der paedML-Server in diesem Netz befindet.

Wählen Sie im folgenden Fenster das „*Interface“* (*VLAN-ID*) das Anfragen stellen können soll und aktivieren Sie „*DHCP-Relay*“. „*DHCP-Snooping*“ bleibt deaktiviert. Speichern Sie die Einstellungen mit „*Apply*“.

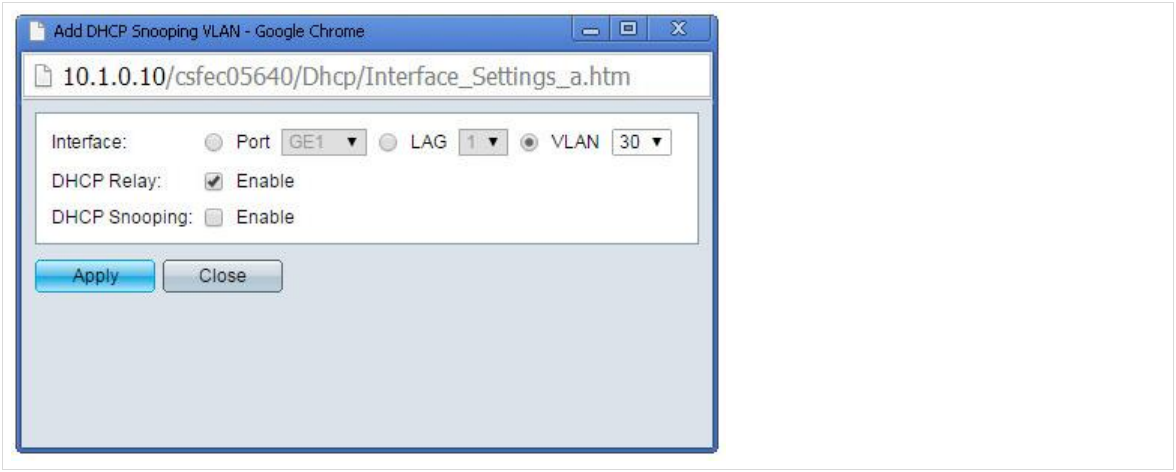

Abb. 18: Aktivieren von DHCP-Relaying für ein VLAN

Die folgende Tabelle zeigt wie die „*Interface Settings*“ gesetzt sein sollten:

Interface	Interface IP-Address	DHCP Relay	DHCP Snooping
VLAN 20	10.1.1.1	Enabled	Disabled
VLAN 30	10.1.2.1	Enabled	Disabled
VLAN 40	10.2.0.1	Enabled	Disabled

Tabelle 5 - Zuordung des DHCP-Relayings an die VLANs

4.3.4 Aktivieren der Wake-On-Lan-Funktion

Wenn Sie Hardware haben, die Wake-On-Lan unterstützt und wenn Sie diese Funktion nutzen wollen, so muss im nächsten Schritt die Weiterleitung der „Magic Packets“ aktiviert werden.

Dies geschieht über den Menüpunkt „*IP Configuration* | *IPv4 Management an Interfaces* | *UDP Relay / IP Helper*“. Hier muss das folgende UDP-Relay hinterlegt werden, welches die Weiterleitung ermöglicht:

Source IP Interface	UDP Destination Port	Destination IP Address
10.1.0.10	9[9]	255.255.255.255

Tabelle 6 - UDP-Relay für Wake on Lan

Über den Button "*Add...*" können Regeln hinzugefügt werden.

Im Dropdown-Menü für "*Source IP Interface*" muss das Netzwerk ausgewählt werden, von welchem die neue Regel gültig sein soll. Hier muss also die Schnittstelle des Servernetzes („*10.1.0.10*“) aktiviert werden.

Unter "*UDP Destination Port*" wird im Feld "*Port*" ein eigener Port „*9*“ eingetragen. Im Feld "*Destination IP Address*" muss die IP-Adresse eingetragen werden, auf welches Netzwerk die neue Regel angewandt werden soll. Da die Funktion in allen Netzen verfügbar sein soll, wird hier „*255.255.255.255*“ eingetragen.

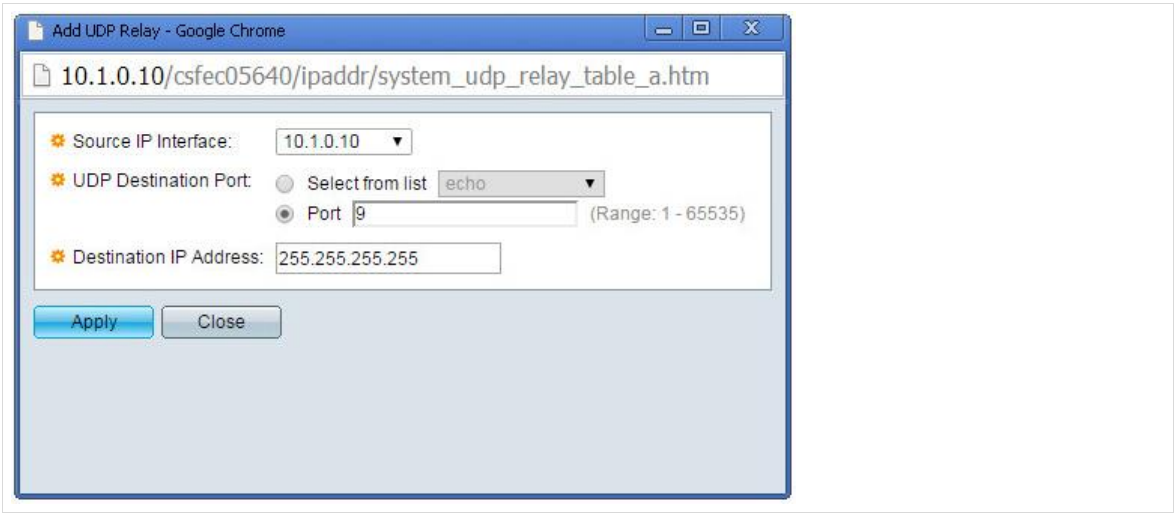

Abb. 19: Konfiguration des UDP-Relays

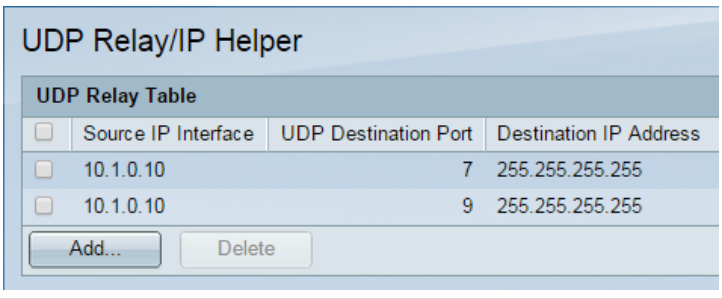

Abb. 20: Eingetragenes UDP-Relaying

[9] In der Regel „lauschen“ Wake-On-Lan-fähige Netzwerkkarten auf UDP-Port 9. Es gibt aber auch Geräte, die mit Port 7 arbeiten. Weitere Informationen zu Wake-On-Lan finden Sie unter http://www.dd-wrt.com/wiki/index.php/WOL .

4.4 Trennung der VLANs

Mit Hilfe von „*Access Control Lists*“ (*ACLs*), also Listen, die die Zugriffskontrolle zwischen den Netzsegmenten regulieren, geschieht die logische Trennung der Netzsegmente und somit die Absicherung. Jedem Netzsegment kann eine ACL zugewiesen werden. ACLs wiederum bekommen eine oder mehrere Zugriffsregeln (*Acces Control Entries* (*ACE*)) zugewiesen.

In der hier beschriebenen Umsetzung wird der Zugriff der VLANs „LEHRERNETZ“ und „PAEDAGOGIK“ in das Servernetz erlaubt. Der Zugriff zwischen dem Pädagogischen Netz und dem Lehrernetz wird unterbunden.

4.4.1 Erstellen von ACLs

Im ersten Schritt müssen die neuen ACLs „*LEHRERNETZ*“ und „*PAEDAGOGIK*“ angelegt werden.

Öffnen Sie hierfür das Menü "*Access Control* | *IPv4-Based ACL*". Drücken Sie auf den „*Add…*“-Knopf. Es öffnet sich ein neuer Dialog. Tragen Sie die Namen der Regeln in das Feld „*ACL Name:*“ ein.

Übernehmen Sie den Eintrag mit „*Apply*“. Wiederholen Sie den Vorgang für die ACL “*PAEDAGOGIK*“ und schließen Sie den Dialog mit „*Close*“.

Abb. 21: Anlegen der ACL „LEHRERNETZ“

Anschließend sehen Sie in der Übersicht die zwei neu angelegten Regeln.

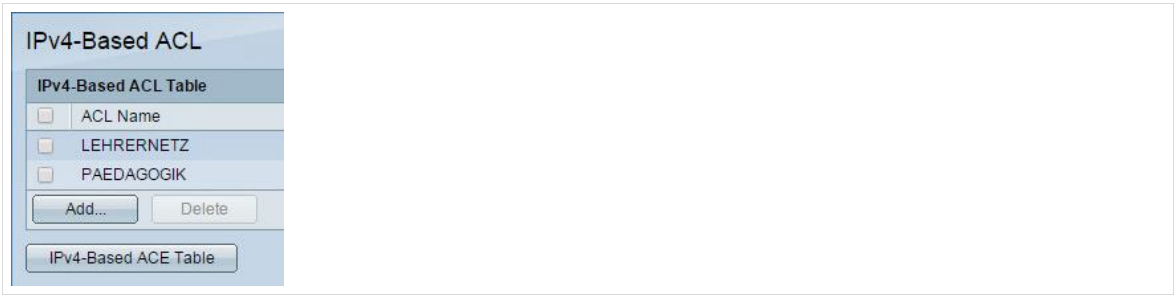

Abb. 22: Neu angelegte ACLs in der Übersicht

4.4.2 Erstellen von ACEs

Auf der Seite "*Access Control* | *IPv4-Based ACE*" werden Zugriffsregeln (Access Control Entries (ACE)) definiert und an ACLs zugewiesen.

Um eine Zugriffsregel (ACE) zu einer Zugriffsliste (ACL) zuzuweisen wählen Sie im Dropdown-Menü „*ACL Name equals to*“ den Namen der ACL und klicken Sie auf „*Go*“. Anschließend werden alle der ACL zugewiesenen ACEs angezeigt – sofern es welche gibt. Mit dem „*Add*“-Button legen Sie eine neue Regel an. Bestehende Regeln können nach Auswahl mit der Checkbox vor der Zeile über den Knopf „*Edit…*“ geändert werden.

Abb. 23: Bearbeiten von ACEs

Je Regel müssen die Einträge für „*Priority*“, “*Action*“, „*Protocol*“, „*Destination IP Adress Value*“ und „*Destination IP Wildcard Mask*“ überprüft und gegebenenfalls angepasst werden.

Wenn Sie eine neue Regel definiert haben, scrollen Sie in dem Fenster ganz nach unten und drücken Sie auf „*Apply“*, um die Regel zu übernehmen. Abschließend drücken Sie auf „*Close*“, um das Fenster zu schließen.

Die Regeln für „*LEHRERNETZ*“ und „*PAEDAGOGIK*“ sind fast identisch – sie unterscheiden sich lediglich in der Priorität (Feld „*Priority*“). Regeln mit höherer Priorität werden vor niedrig priorisierten Regeln abgearbeitet. Die folgende Tabelle gibt einen Überblick über die Werte der ACEs:

Wert / ACL	LEHRERNETZ (1)	LEHRERNETZ (2)	PAEDAGOGIK (1)	PAEDAGOGIK (2)
Priority	10	20	30	40
Action	Permit	Deny	Permit	Deny
Protocol	Any (IP)	Any (IP)	Any (IP)	Any (IP)
Source-IP-Address	Any	Any	Any	Any
Destination IP Address	User Defined	User Defined	User Defined	User Defined
Destination IP Address Value	10.1.0.0	10.0.0.0	10.1.0.0	10.0.0.0
Destination IP Wildcard Mask	0.0.0.255	0.255.255.255	0.0.0.255	0.255.255.255

Tabelle 7 - Übersicht der ACEs

- Die ersten Regelsätze (*ACL Name „LEHRERNETZ (1)“ und „PAEDAGOGIK (1)“*) ermöglichen den Zugriff auf das *SERVERNETZ´*.
- Die zweiten Regelsätze (*ACL Name „LEHRERNETZ (2)“ und „PAEDAGOGIK (2)“*) unterbinden den Zugriff aus dem eigenen Netzsegment in andere Netzsegmente.#

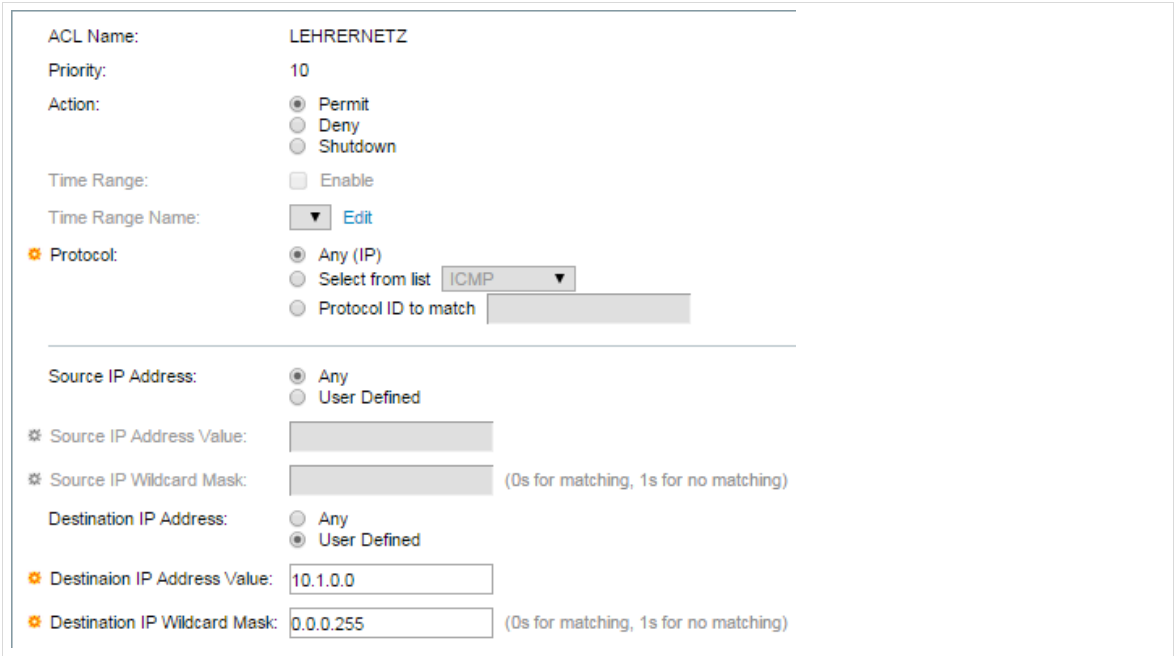

Abb. 24: Anlegen der ersten Zugriffs-Regel – hier: Zugriff von Lehrernetz auf Servernetz

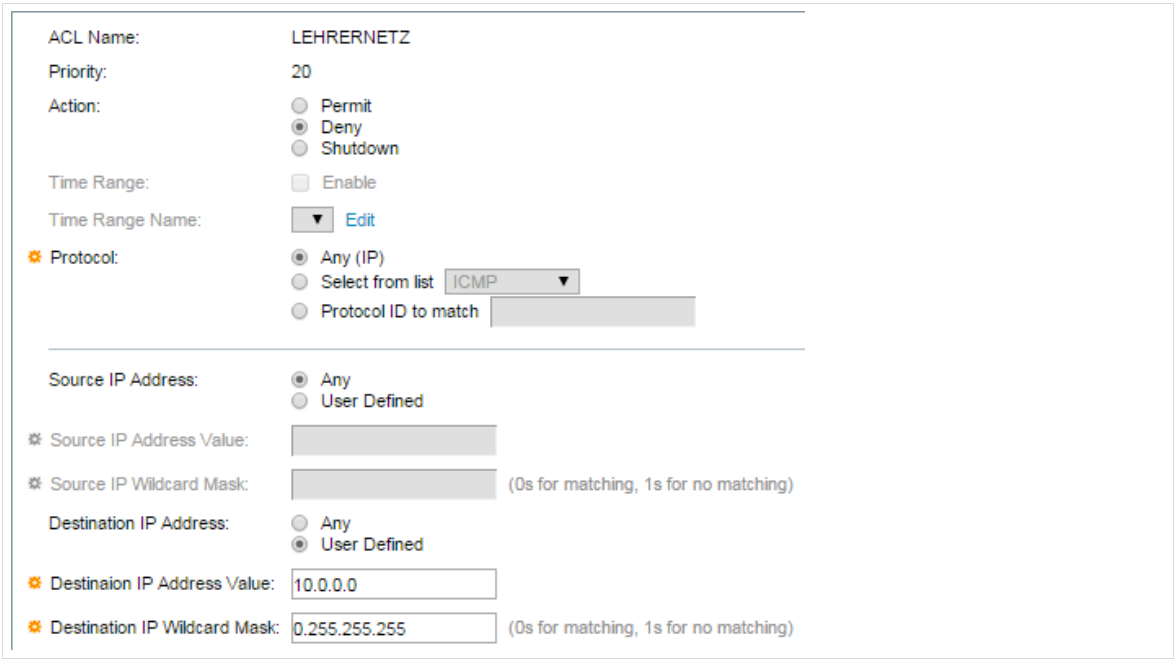

Abb. 25: Anlegen der zweiten Zugriffs-Regel – hier: Sperre von Zugriff auf andere Netze aus Lehrernetz

Die gleichen (sich lediglich im Feld „Priority unterscheidenden) Regeln müssen Sie anschließend für die ACL „PAEDAGOGIK“ anlegen.

Wenn die ACEs angelegt wurden, erscheinen Sie in der Übersicht.

Abb. 26: Übersicht über die Regeln des Lehrernetzes

Abb. 27: Übersicht über die Regeln des PÄDAGOGISCHEN NETZES

4.4.3 Zuweisen von ACLs an Hardwareports auf dem Router

Nachdem die Regeln definiert wurden, müssen Sie auf die Hardware-Ports gelegt werden, an denen das jeweilige Netzsegment anliegen soll.

In der Beispiels-Konfiguration sind dies die Ports fünf bis acht (LEHRERNETZ) und Port neun bis zwölf (PAEDAGOGISCHES NETZ).

Im Menü „*Access Control* | *ACL Binding*“ geschieht die Zuordnung an die Hardwareports. Wählen Sie einen Port aus, den Sie konfigurieren wollen und drücken Sie auf „*Edit…*“

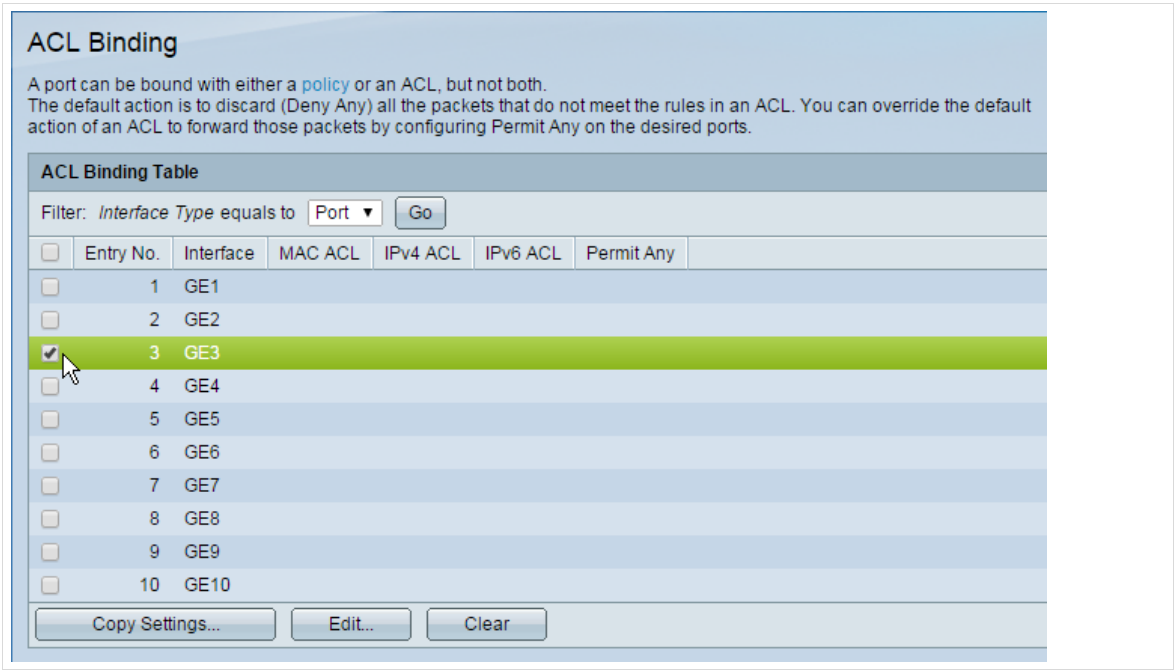

Abb. 28: Auswahl des zu konfigurierenden Ports

In der folgenden Maske muss das „*Interface*“ (hier der *Port GE9*) ausgewählt und die vorher definierte ACL zugewiesen werden.

Der Wert „*Permit Any:*“ muss auf „*Enable*“ gestellt sein.

Speichern Sie die Einstellungen mit „*Apply*“ ab und wiederholen Sie den Vorgang für jeden weiteren Port.

Schließen Sie die Maske anschließend mit „*Close*“.

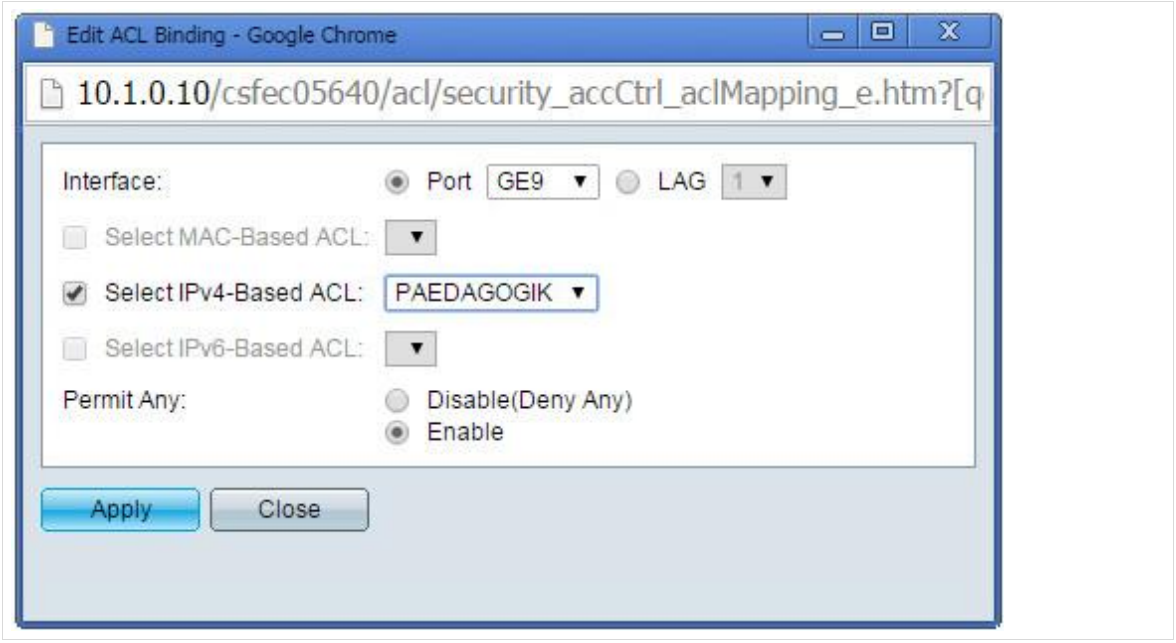

Abb. 29: Zuweisen der ACL an Ports

In der ACL-Binding-Übersicht werden nach erfolgter Zuordnung alle zugewiesenen ACLs angezeigt.

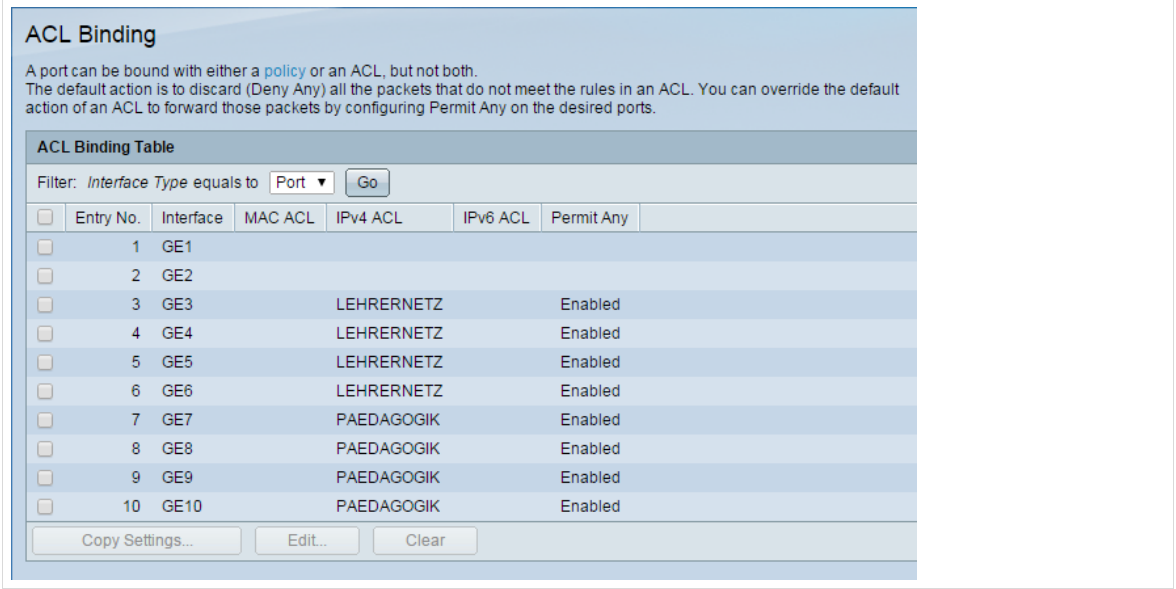

Abb. 30: Übersicht zum ACL-Binding

ACLs können in dieser Maske auch wieder von einem Port entfernt werden. Hierfür müssen Sie die entsprechenden Einträge markieren und auf „Clear“ drücken.

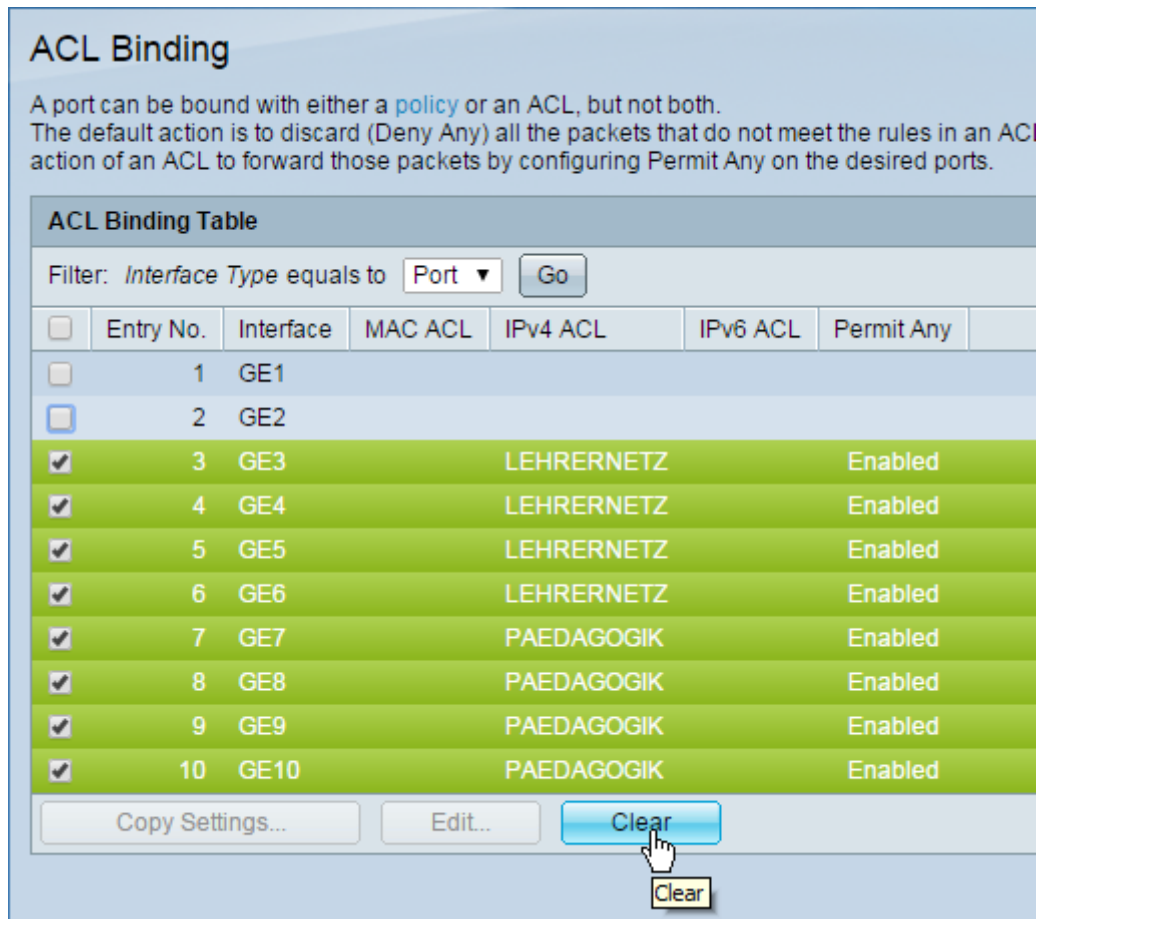

Abb. 31: Entfernen von zugeordneten ACLs

4.5 Anpassung Spanning-Tree-Protokoll

Das Spanning-Tree-Protokoll verhindert, dass fehlerhafte Netzsegmente das gesamte Netzwerk lahmlegen[10]. Daher sollte diese Option im Switch aktiviert sein.

Derzeit gibt es bei den Cisco-Geräten Fallstricke bei der Clientaufnahme, die Sie entweder mit einem temporären Workaround oder durch Anpassung über die Switch-Kommandozeile beheben müssen.

Workaround – nicht empfohlen
Für die Rechneraufnahme über den PXE-Boot, können Sie temporär unter „*Spanning Tree* | *STP Status & Global Settings*“ den Haken bei „*Spanning Tree State: Enable*“ entfernen. Anschließend übernehmen Sie die Änderung mit „*Apply*“.

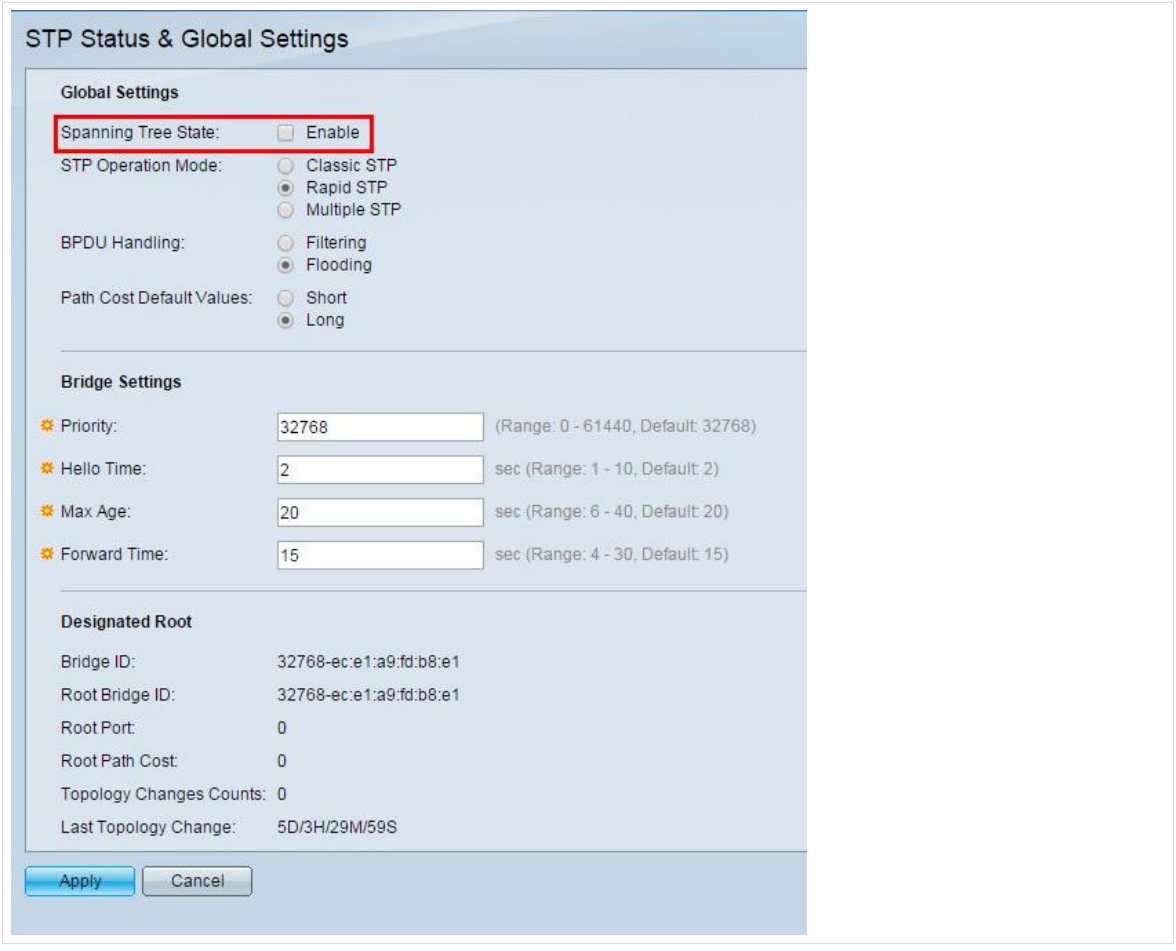

Abb. 32: Deaktivieren Sie Spanning-Tree temporär für die Rechneraufnahme.

[10] Mehr Informationen finden Sie bspw. unter http://www.admin-magazin.de/Das-Heft/2014/03/Wie-organisiert-Spanning-Tree-ein-Ethernet-Netzwerk

Spanning Tree sollten Sie nach erfolgter Rechneraufnahme unbedingt wieder aktivieren!

Alternativen zur Rechneraufnahme über den PXE-Boot (direkt über die Schulkonsole oder über eine Rechnerliste) sind im Administratorhandbuch beschrieben.

Anpassung der Switch-Konfiguration
Um die Rechneraufnahme über PXE-Boot bei aktiviertem Spanning-Tree-Protokoll dauerhaft zu gewährleisten, müssen Sie eine SSH-Verbindung mit dem Switch aufbauen.

Unter „*Security* | *TCP/UDP Services*“ aktivieren Sie zunächst die SSH-Verbindung.

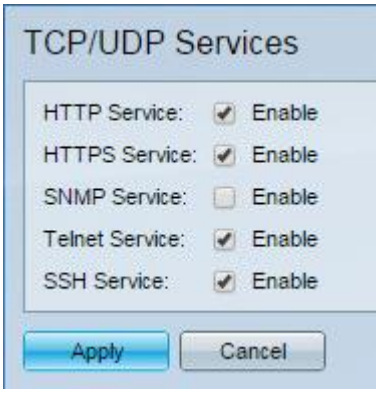

Abb. 33: Der SSH-Service muss für den Zugriff aktiviert sein.

Verbinden Sie sich mit dem Programm *putty* mit dem Cisco-Switch.

Melden Sie sich mit Ihren Zugangsdaten an.

Auf jedem Port, an dem Server oder Clients angeschlossen sind, müssen die folgenden Befehle ausgeführt werden. (**Passen Sie die Befehle an Ihr Netz an. Hier hängt der Server an Port 3, an Port 4 und 8 sind Clients angeschlossen.**)

```
configure
int gi3
spanning-tree portfast
int gi4
spanning-tree portfast
int gi8
spanning-tree portfast
exit
```

Schließen Sie anschließend die Verbindung mit dem Switch.

5. Speichern der Switch-Konfiguration

Alle Änderungen, die in einem Menü vorgenommen werden, sind temporär. Sobald der Switch neu gestartet wird, wird die alte Konfiguration verworfen.

Dies ist vor allem nützlich, wenn sich Anwender durch eine Fehlkonfiguration aussperren. In diesem Fall muss das Gerät einfach für ein paar Sekunden vom Strom genommen werden. Beim Neustart lädt es die letzte Konfiguration.

Es ist ratsam, Zwischenschritte zu speichern!

Nach Abschluss der Konfiguration des Switches müssen Sie diese speichern. Dies geschieht über den blinkenden "*Save...*"-Knopf oben rechts in der Oberfläche.

Alternativ können Sie das Menü "*Administration* | *File Management* | *Copy/Save Configuration*" aufrufen.

Um die aktuelle Konfiguration („Running Configuration“) dauerhaft zu speichern markieren Sie die folgenden Auswahlpunkte:

- *Source File Name: Running configuration*
- *Destination File Name: Startup configuration*

Die Konfiguration wird über den Button "*Apply*" gesichert. Nach Abschluss des Speichervorgangs ist sichergestellt, dass die aktuelle Konfiguration bei einem Neustart des Switches geladen und angewandt wird.

Abb. 34: Schreiben der aktuellen Konfiguration in die Start-Konfiguration.

6. Sichern der Konfiguration

Sie können die Konfiguration optional auch herunterladen und außerhalb des Switches sichern. Dazu rufen Sie das Menü "*Administration* | *File Management* | *Download/Backup Configuration*" auf.

Sie können die Daten mit dem Webbrowser, von dem aus die Benutzeroberfläche des Cisco-Routers bedient wird, lokal speichern.

Wählen Sie hierfür den Eintrag „*Transfer Method via HTTP/HTTPS*“ aus.

Als "*Save Action*" wird "*Backup*" ausgewählt.

Als Wert für "*Source File Type*" müssen Sie – je nach Konfiguration, die gesichert werden soll – "*Running configuration file*" oder "*Startup configuration file*" auswählen.

Stellen Sie den Wert für "*Sensitive Data*" auf "*Plaintext*", um die Datei später auch lesen zu können.

Anschließend wird der Download über den Button „*Apply*“ angestoßen.

Abb. 35: Sichern der Konfigurationsdatei

Der nächste Dialog zeigt an, ob Fehler beim Transfer der Datei aufgetreten sind.

Abb. 36: Status des Transfervorgangs.

Die Konfigurationsdatei wird anschließend auf den Client übertragen. Im vorliegenden Beispiel wurde die Startkonfiguration in die Datei „*startup-config.txt*“ gespeichert.

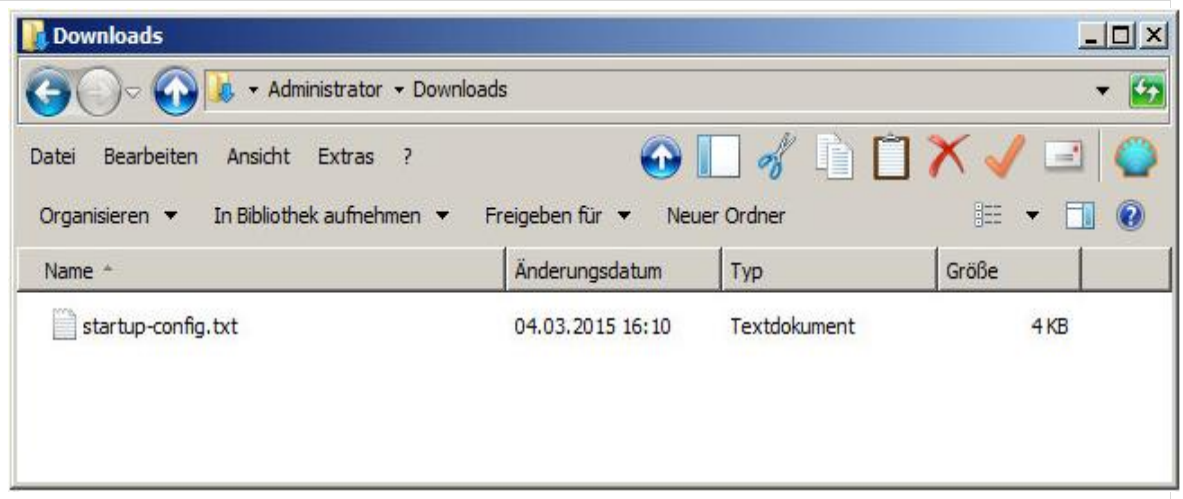

Abb. 37: Heruntergeladene Konfigurationsdatei.

7. Konfiguration einspielen

Um eine vorhandene Konfigurationsdatei in den Switch einzuspielen, öffnen Sie das Menü „*Administration* | *File Management* | *Download/Backup Configuration/Log*“.

Aus Sicht des Switches handelt es sich beim Dateitransfer um einen „*Download*“. Der Wert für „*Save Action*“ muss daher auf „*Download*“ gestellt sein.

In der Zeile „*Source File Name*“ müssen Sie die Datei auswählen, die übertragen werden soll. Drücken Sie hierfür auf „*Datei auswählen*“.

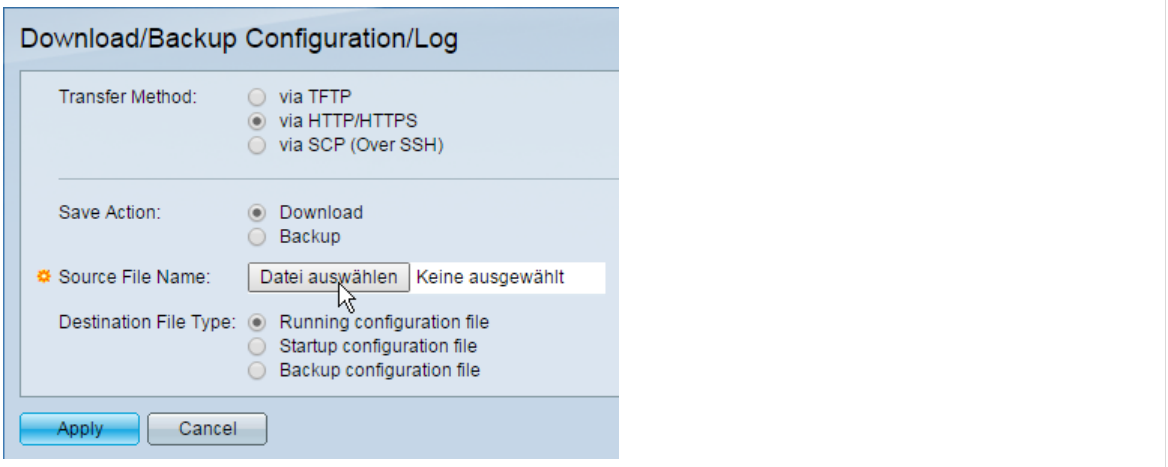

Abb. 38: Übertragung einer Konfigurationsdatei an den Switch

Es öffnet sich ein Windows-Dialog, in dem die zu übertragene Konfiguration ausgewählt werden muss.

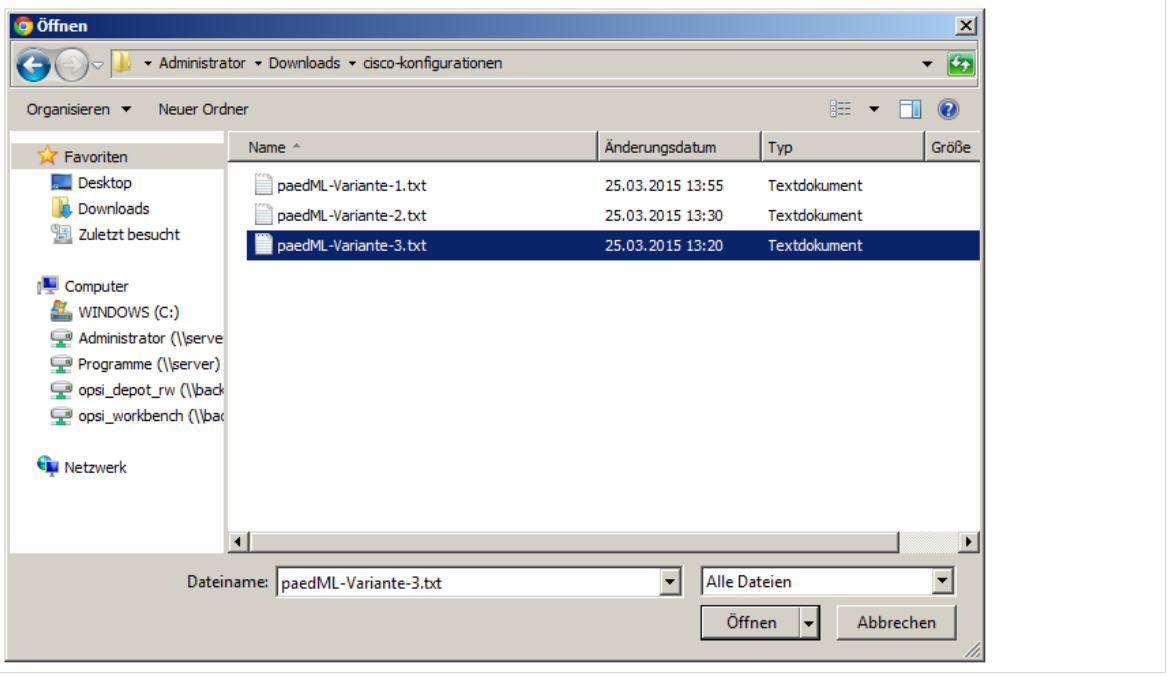

Abb. 39: Auswahl der zu übertragenen Konfigurationsdatei.

Im Anschluss können Sie die Datei mit „*Apply*“ hochladen.

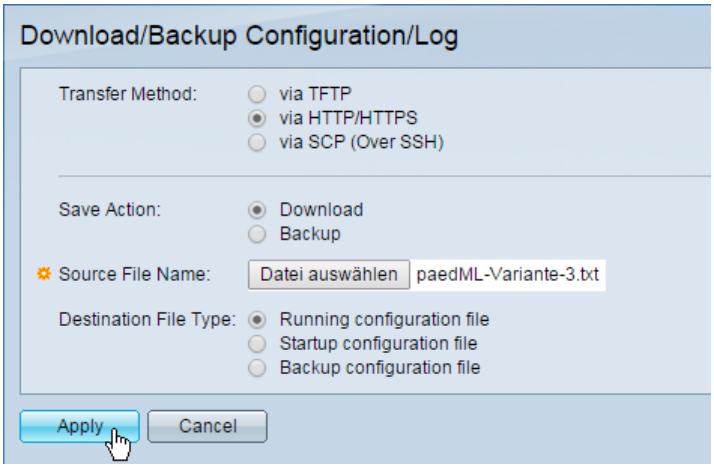

Abb. 40: Hochladen der Konfigurationsdatei.

Es erscheint ein Dialogfenster, in dem Sie darauf hingewiesen werden, dass während des Einspielens der Konfiguration keine anderen Menüs des Cisco-Switches aufgerufen werden sollten, da sonst das Einspielen der Konfiguration abbricht. Diesen Dialog müssen Sie mit „*OK*“ bestätigen.

Warten Sie bis der Prozess mit einer Meldung wie der folgenden abgeschlossen ist.

Der Eintrag „*Status“* zeigt an, ob die Konfiguration hochgeladen wurde. Im Fehlerfall wird eine Fehlermeldung („*Error Message*“) angezeigt.

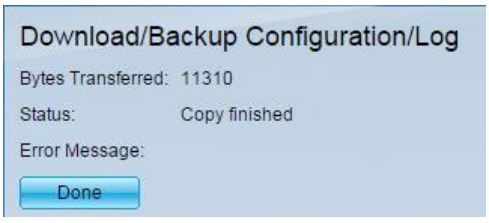

Abb. 41: Bestätigung des Dateiuploads.

8. Rechneraufnahme

Die Aufnahme von Rechnern und anderen Geräten (Drucker, Netzwerkperipherie) ist ausführlich im Administratorhandbuch der paedML Linux im Kapitel „*Verwaltung von Geräten*“ beschrieben.

Beachten Sie bei der Aufnahme von Geräten mit den hier beschriebenen Netzwerkerweiterungen, dass Sie die Geräte mit einer anderen IP-Adresse in die paedML aufnehmen müssen als bei einer Installation in der Standard-Konfiguration (mit einem Pädagogischen Netz im IP-Adressbereich *10.1.0.0 / 24* (alt)).

Die IP-Adresse ist abhängig vom Netzsegment, in dem das Gerät betrieben werden soll. Dieser IP-Adressbereich wird über das VLAN, in dem das Gerät angeschlossen ist, bestimmt.

Außerdem muss sichergestellt sein, dass ein Gerät, das bspw. in das Lehrernetz aufgenommen werden soll, auch an den entsprechenden Ports des in Kapitel 3 konfigurierten Switches betrieben wird.

Sie können je Netzsegment eine Adresse durch die paedML vergeben lassen, in dem Sie die „*Adresse für die automatische Aufnahme*“, die der Adresse des Netzes entspricht, vergeben. Das Gerät bekommt dauerhaft diese Adresse zugewiesen.

Sie können aber auch händisch eine statische Adresse vergeben. Dies ist zum Beispiel sinnvoll, wenn Sie ein Netzwerk so einrichten wollen, dass Sie bestimmte Räume mit einheitlichen IP-Adressen einrichten wollen (z.B. in einem großen Schülernetz: *Raum 118: 10.2.118.0, Raum 119: 10.2.119.0*).

Wenn Sie Geräte im großen pädagogischen Netz (*10.2.0.0 / 16*) beziehungsweise Netzen mit einer anderen Subnetzmaske als *255.255.255.0* anlegen möchten, müssen Sie das Feld *„Subnetzmaske“* stets mit der richtigen Subnetzmaske ausfüllen - der Standardwert ist *255.255.255.0.*

Achten Sie darauf KEINE IP-Adresse aus dem DHCP-„Aufnahme“-Pool[11] zu vergeben.

Im Fall der Erweiterung des Schulnetzes um selbst definierte Netzsegmente (vgl. Seite 46 ff.) müssen IP-Adressen bei der Rechneraufnahme entsprechend der selbst eingerichteten Netzsegmente vergeben werden!

[11] Der DHCP-„Aufnahme“-Pool ist der Adressbereich, aus dem unbekannte Geräte, mit einer IP-Adresse versorgt werden. Dies wird für die Rechneraufnahme in der paedML Linux genutzt.

Netzsegment	Adresse für automatische Aufnahme	Statisch zu vergebene IP-Adressen	Subnetzmaske	DHCP-„Aufnahme“-Pool
Servernetz	10.1.0.0	10.1.0.32 bis 10.1.0.229 (198 Adressen)	255.255.255.0	10.1.0.230 bis 10.1.0.254
Lehrernetz	10.1.1.0	10.1.1.10 bis 10.1.1.229 (219 Adressen)	255.255.255.0	10.1.1.230 bis 10.1.1.254
entweder				
Pädagogisches Netz (klein)	10.1.2.0	10.1.2.1 bis 10.1.2.229 (229 Adressen)	255.255.255.0	10.1.2.230 bis 10.1.2.254
oder				
Pädagogisches Netz (groß)	10.2.0.0	10.2.1.1 bis 10.2.251.254 (63754 Adressen)	**255.255.0.0**[12]	10.2.252.0 bis 10.2.255.254

Tabelle 8 - IP-Adressen für die Rechneraufnahme

[12] Achten Sie unbedingt darauf die richtige Subnetzmaske zu vergeben!

9. Manuelle Anpassungen für Bestandskunden

Mit dem Errata-Update 2 wurde dieser Arbeitsschritt bereits durchgeführt.

Alle Kunden, die mit einem Datenträger installiert haben, der vor Sommer 2015 (Errata 2) ausgeliefert wurde, müssen nachträglich konfigurative Anpassungen in den Netzwerkeinstellungen der paedML vornehmen.

Wenn Sie die IP-Adressbereiche 10.1.1.0 (Lehrernetz) und/oder 10.1.2.0/24 (kleines Pädagogisches Netz) und/oder 10.2.0.0/16 (großes Pädagogisches Netz) nutzen wollen, müssen Sie die folgenden Arbeitsschritte ausführen.

Ab Kapitel 10 „Netzerweiterung um eigene Netze“ (S. 46 ff) wird beschrieben, welche Schritte zur Konfiguration ausgeführt werden müssen:

- Anlegen neuer Netzsegmente – Sofern Sie keine eigenen Netze definieren wollen (vgl. Einführung von Kapitel 10 und Kapitel 10.1.1 bis 10.1.3, ab Seite 46), müssen hier keine Änderungen vorgenommen werden. Beim Update zur paedML Linux Errata 2 werden die in der bisherigen Anleitung besprochenen Netze automatisch angelegt.
- Konfiguration DHCP-Server (vgl. Kapitel 10.1.4, ab Seite 51).
- Konfiguration DNS-Server (vgl. Kapitel 10.1.5, ab Seite 54).
- Setzen von statischen Routen (vgl. Kapitel 10.1.6, Kapitel 10.1.7 und Kapitel 10.1.8, ab Seite 54)
- Anpassungen an der Firewall (vgl. Kapitel 10.2,ab Seite 56)

Stellen Sie sicher, dass diese Konfigurationsschritte in Ihrem System vorgenommen werden. Erst danach können Sie die neuen Netze nutzen.

10. Netzerweiterung um eigene Netze

Weitere Netzbereiche

Falls die hier beschriebenen Anpassungen für Ihre Anforderungen an das Schulnetz nicht ausreichen, können Sie das Schulnetz um weitere IP-Bereiche erweitern. Über die Anlage weiterer VLANs können Sie weitere Netzsegmente erstellen und voneinander trennen. So können zum Beispiel Fachschaften, verschiedene Schulgebäude oder auch einzelne Klassenzimmer mit eigenen Netzsegmenten versorgt werden.

Im ersten Schritt sollte überprüft werden, welche Netze im Server eingerichtet sind. Öffnen Sie hierfür das Schulkonsolenmenü „*Domäne* | *Netzwerke*“. Darin werden alle Im System angelegten Netzsegmente angezeigt.

Bereits angelegte Netzsegmente müssen nicht neu angelegt werden. Es wird jedoch empfohlen die Konfigurationsschritte der folgenden Kapitel wenigstens zu überprüfen und ggf. durchzuführen.

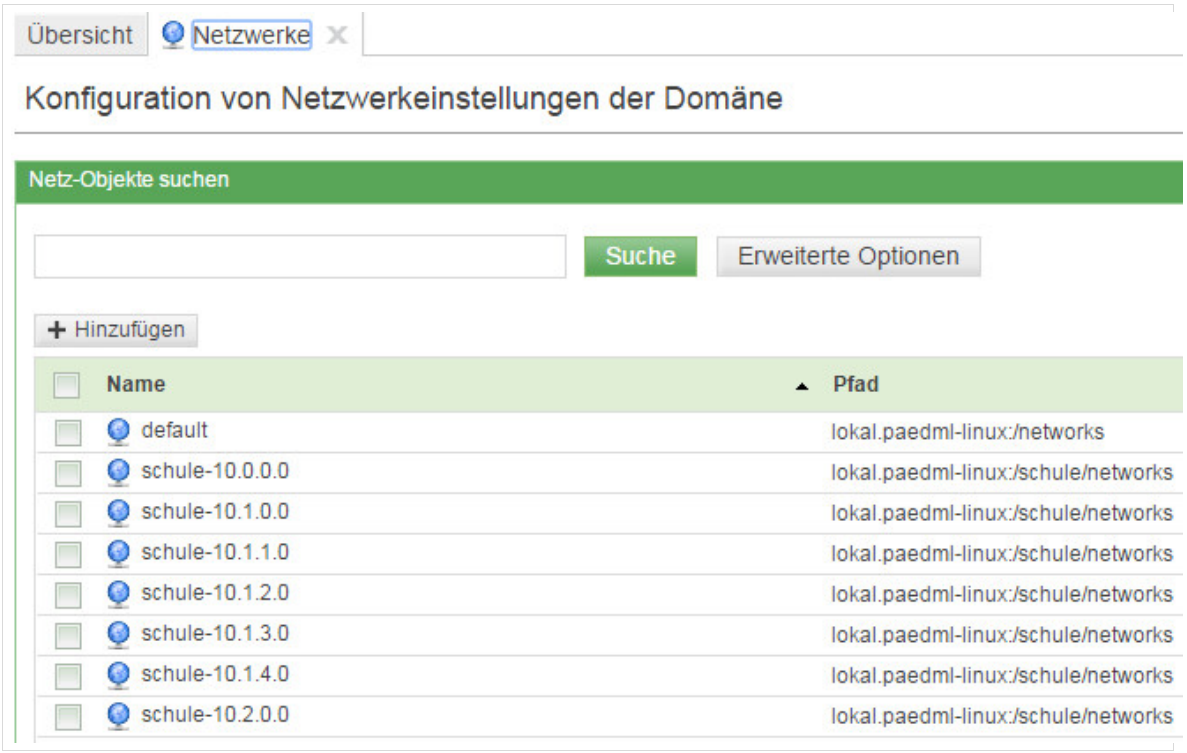

Abb. 42: Hier wurden schon fleißig Netze angelegt.

10.1 Erweiterung des Schulnetzwerkes durch Netze/IP-Bereiche

Im Auslieferungszustand sind in der *paedML Linux* folgende Netze/IP-Adressen definiert:

Netz	Subnetz	IP-Adressen	Verwendung
PAEDAGOGIK	10.1.0.0/24	10.1.0.1 – 10.1.0.20	Für paedML-System reservierte IP-Adressen
		10.1.0.1	server.paedml-linux.lokal („*Server*“)
		10.1.0.2	backup.paedml-linux.lokal („*OPSI-Server*“)
		10.1.0.10	Router[13] (L3-Switch z.B. Cisco SG 300-10)
		10.1.0.11	firewall.paedml-linux.lokal („*Firewall*“)
		10.1.0.13	adminvm.paedml-linux.lokal („*AdminVM*“)
		10.1.0.21-10.1.0.31	Reservierter Bereich zur Nutzung durch den Betreiber. (z.B. Intranet-Server etc.)
		10.1.0.32 – 10.1.0.229	Client-Rechner (max. 198)
		10.1.0.230 – 10.1.0.254	DCHP-Pool für nicht registrierte Geräte (z.B: bei Rechneraufnahme, max. 25)
GAESTENETZ	172.16.0.0/12	172.16.1.1	firewall.paedml-linux.lokal („*Firewall*“)
		172.16.2.1-172.31.255.254	Netzbereich für Gast-Geräte
INTERNET			IP per DHCP oder statische IP-Adresse

Tabelle 9 Netzübersicht im Auslieferungszustand.

Wie aus „Tabelle 9 Netzübersicht im Auslieferungszustand“ ersichtlich, stehen im Auslieferungszustand für Clients im pädagogischen Netz insgesamt 198 IP-Adressen zur Verfügung (10.1.0.32 - 10.1.0.229).

Sollte dieser Adressraum nicht ausreichen, können Sie weitere IP-Segmente definieren. Hierfür werden die IP-Adressbereiche *10.1.3.0 / 24* bis *10.1.255.0 / 24* empfohlen.

[13] Optionales Gerät zur Anbindung weiterer Netze (z.B. Lehrernetz oder Netzwerweiterungen).

10.1.1 Grundkonzept anhand eines Beispiels

- Für Clients soll ein eigenes Subnetz, mit der Bezeichnung „*PAEDAGOGIK2*“ eingerichtet werden.
- Das Netz „*PAEDAGOGIK2*“ bekommt einen gesonderten IP-Bereich (z.B. *10.1.3.0/24*).
- Das Netz „*PAEDAGOGIK2*“ muss mit Hilfe eines Routers an das Netz „*PAEDAGOGIK*“ angebunden werden. Für den Router ist im Netz „*PAEDAGOGIK*“ die IP *10.1.0.10* bereits vorgesehen, im Netz „*PAEDAGOGIK2*“ wird dem Router die IP *10.1.3.1* vergeben.

Hinweise

- Damit die Clients in zusätzlichen Netzen per *Wake-on-LAN* aufgeweckt werden können, muss das dafür notwendige sogenannte *Magic-Packet* über Router-Grenzen hinweg transportiert werden (vgl. Kapitel 4.3.4, Seite 27).
- Die *paedML Linux* kann über das hier beschriebene Verfahren um beliebig viele Netze erweitert werden. So lässt sich beispielsweise erreichen, dass sich verschiedene Klassenzimmer, Gebäudeteile,… in jeweils eigenen Subnetzen befinden.

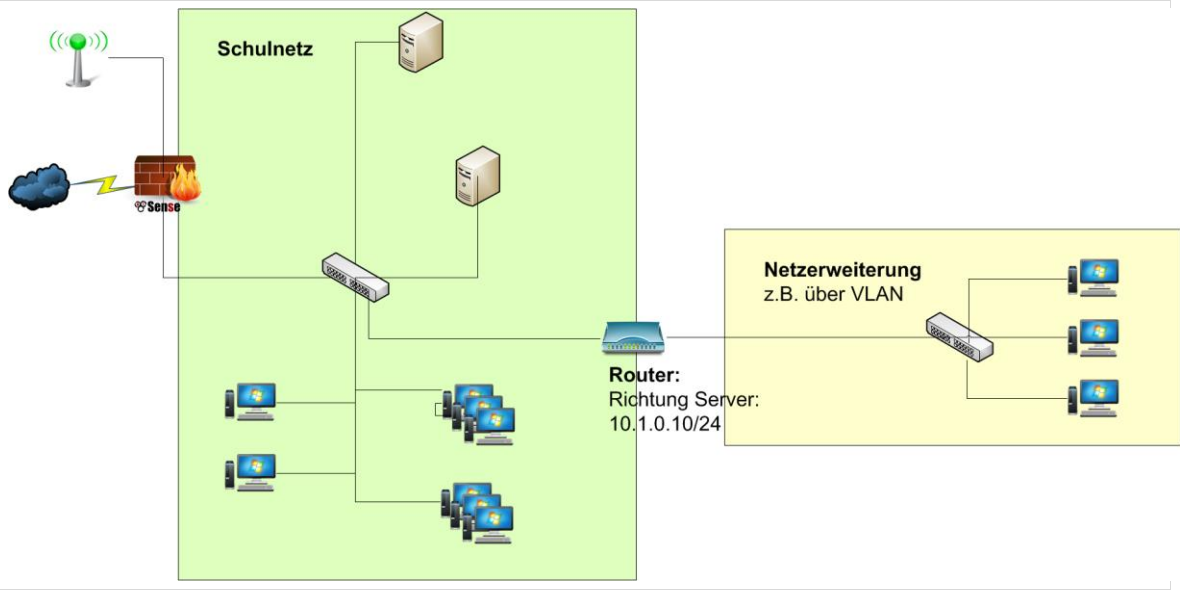

Abb. 43: Erweiterung der paedML Linux um zusätzliche Netze (Die Abbildung ist kein Beispiel für ein sicheres Lehrernetz!)

10.1.2 Erstellen der Importdatei

Das Hinzufügen von Netzwerken geschieht über die Kommandozeile des Servers. Zunächst muss eine Textdatei mit den zu importierenden Netzen erstellt werden. Die Textdatei kann entweder direkt auf dem Server erstellt oder auf den Server kopiert werden. Die Textdatei enthält je eine Zeile für jedes neue Netzwerk, jede Zeile muss nach dem folgenden Muster aufgebaut sein:

`<schulnr>`*TAB*`<netzwerk>`*TAB*`<ipbereich>`*TAB*`<router_ip>`*TAB*`<dns_ip>`*TAB*`<wins_ip>`

Jedes Netz muss in einer neuen Zeile definiert werden. Zum Trennen dürfen ausschließlich Tabulatoren verwendet werden!

Die einzelnen Felder der Importdatei müssen durch jeweils **genau ein Tabulatorzeichen** voneinander getrennt sein!

Bedeutung der einzelnen Felder:

Feld	Beschreibung	Mögliche Werte
<schulnr>	**Muss immer „schule“ lauten**	schule
<netzwerk>	Netzwerk und Subnetzmaske	10.1.2.0/24 – 10.1.255.0/24
<ipbereich>	Bereich, aus dem IP-Adressen vergeben werden.	10.1.X.10 – 10.1.X.229[14]
<router_ip>	IP-Adresse des Routers im neuen Netz	10.1.2.1
<dns_ip>	IP-Adresse des DNS-Servers. **Muss immer „10.1.0.1“ sein**	10.1.0.1
<wins_ip>	IP-Adresse de WINS/Netbios-Servers. **Muss immer „10.1.0.1“ sein.**	10.1.0.1

Es können beliebig viele Netze importiert werden.

Beim IP-Bereich (zum Beispiel 10.1.123.10 – 10.1.123.229) handelt es sich um den dynamischen IP-Adressbereich, der Geräten bei der Geräteaufnahme in die paedML fest vergeben wird.

Die ersten zehn IP-Adressen des jeweiligen Netzsegmentes werden hierbei nicht vergeben. Die erste IP-Adresse (10.1.123.1) ist für den Router reserviert. Die folgenden Adressen (10.1.123.2 – 10.1.123.9) können fix an Geräte wie APs oder Drucker vergeben werden.

Der hintere IP-Adressbereich (in diesem Beispiel ab 10.1.123.240) ist der DHCP-Adresspool für die Rechneraufnahme in diesem Netz.

Im Folgenden werden beispielhaft zwei neue Netze (10.1.3.0/24 und 10.1.4.0/24) angelegt.

```
schule 10.1.3.0/24  10.1.3.10-10.1.3.229 10.1.3.1  10.1.0.1  10.1.0.1
schule 10.1.4.0/24  10.1.4.10-10.1.4.229 10.1.4.1  10.1.0.1  10.1.0.1
```

[14] X steht hierbei für das dritte Oktett der IP-Adresse. Dieser Wert kann zwischen 3 und 255 gewählt werden.

Wird für das Feld „*Netzwerk*“ keine Netzmaske angegeben, so wird automatisch die Netzmaske *255.255.255.0* verwendet. Sollte der IP-Adressbereich nicht explizit angegeben worden sein, wird der Bereich *X.Y.Z.20-X.Y.Z.250* verwendet.

```
 GNU nano 2.2.4                Datei: Extranetze.txt                      Verändert

schule  10.1.3.0/24     10.1.3.10-10.1.3.229    10.1.3.1        10.1.0.1        10.1.0.1
schule  10.1.4.0/24     10.1.4.10-10.1.4.229    10.1.4.1        10.1.0.1        10.1.0.1
```

Abb. 44: Beispieldatei zum Anlegen neuer Netze. Felder werden durch TAB getrennt.

10.1.3 Anlegen der Netze auf dem Server

Speichern Sie die Textdatei auf dem Server z.B. unter `/root/Extranetze.txt` und importieren Sie die Netze durch Aufruf des Skriptes `import_networks`:

```
# /usr/share/ucs-school-import/scripts/import_networks Extranetze.txt
```

Daraufhin wird der neue Netzbereich angelegt, Sie sollten in etwa folgende Ausgabe auf der Konsole erhalten:

```
root@server:~# /usr/share/ucs-school-import/scripts/import_networks Extranetze.txt
Stopping univention-s4-connector daemon.
done.
infile is  : Extranetze.txt
Stopping univention-directory-notifier
Stopping univention-directory-notifier daemon: .
ok: down: univention-directory-notifier: 0s
done.

univention-directory-notifier stopped
verify ou for school nr schule
do not need to copy dhcp subnet 10.1.0.0/24: cn=10.1.0.0,cn=schule,cn=dhcp,ou=schule,dc=paedml-linux
,dc=lokal (target already exists)
Skipping non-local subnet 10.1.1.0/24
Skipping non-local subnet 10.0.0.0/24
Skipping non-local subnet 10.1.2.0/24
Skipping non-local subnet 10.2.0.0/16
do not need to copy dhcp subnet 10.1.0.0/24: cn=10.1.0.0,cn=schule,cn=dhcp,ou=schule,dc=paedml-linux
,dc=lokal (target already exists)
Skipping non-local subnet 10.1.1.0/24
Skipping non-local subnet 10.0.0.0/24
Skipping non-local subnet 10.1.2.0/24
Skipping non-local subnet 10.2.0.0/16
generate network 10.1.3.0/24
iprange: 10.1.3.10-10.1.3.239
defaultrouter: 10.1.3.1
nameserver: 10.1.0.1
netbiosserver: 10.1.0.1
creating object zoneName=3.1.10.in-addr.arpa,cn=dns,dc=paedml-linux,dc=lokal
creating object cn=10.1.3.0,cn=schule,cn=dhcp,ou=schule,dc=paedml-linux,dc=lokal
creating object cn=schule-10.1.3.0,cn=networks,ou=schule,dc=paedml-linux,dc=lokal
setting default router
creating object None
connecting dhcp subnet (cn=10.1.3.0,cn=schule,cn=dhcp,ou=schule,dc=paedml-linux,dc=lokal) with polic
y (cn=schule-10.1.3.0,cn=routing,cn=dhcp,cn=policies,ou=schule,dc=paedml-linux,dc=lokal)
setting netbios server
creating object None
```

Abb. 45: Konsolenausgabe beim Anlegen des zusätzlichen Netzes.

Eine nicht korrekt formatierte Importdatei führt zu einer Fehlermeldung („*IndexError: list index out of range*“):

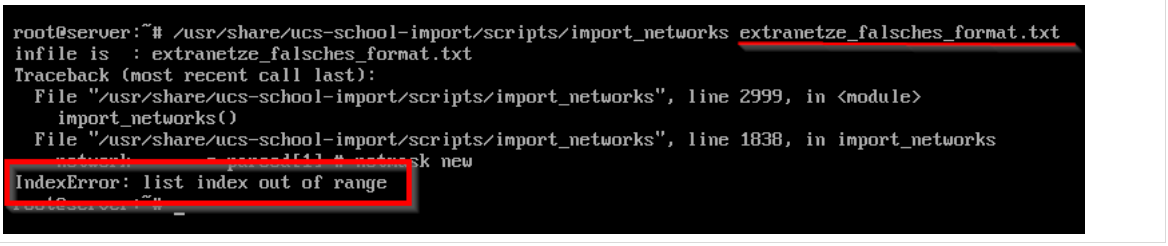

Abb. 46: Fehlermeldung bei nicht korrekt formatierter Importdatei

Überprüfen Sie in diesem Fall, ob die Importdatei korrekt formatiert ist:

- Alle Felder müssen durch einfachen Tabstopp getrennt werden.
- Einzelne Felder können in manchen Fällen ausgelassen werden, das darauf folgende Tabstoppzeichen darf jedoch nicht ausgelassen werden, dann folgen also zwei Tabstoppzeichen aufeinander.
- Die Datei darf keine Kommentarzeilen enthalten

10.1.4 Konfiguration des DHCP-Servers

Damit die Client-Registrierung funktioniert, muss manuell ein Bereich für die dynamische IP-Adressvergabe am DHCP-Subnetz hinterlegt werden. Das Vorgehen ist wie folgt:

Loggen Sie sich per Browser auf der Schulkonsole als Benutzer „*Administrator*“ ein.

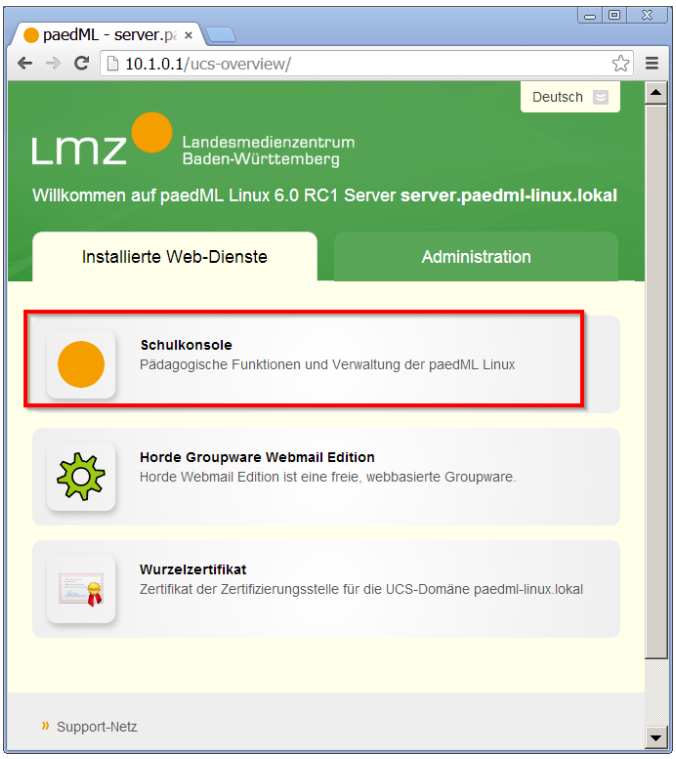

Abb. 47: Anmelden auf der Schulkonsole als Benutzer „Administrator“

Navigieren Sie über *„Domäne | DHCP“* zu der Konfigurationsseite für die DHCP-Einstellungen.

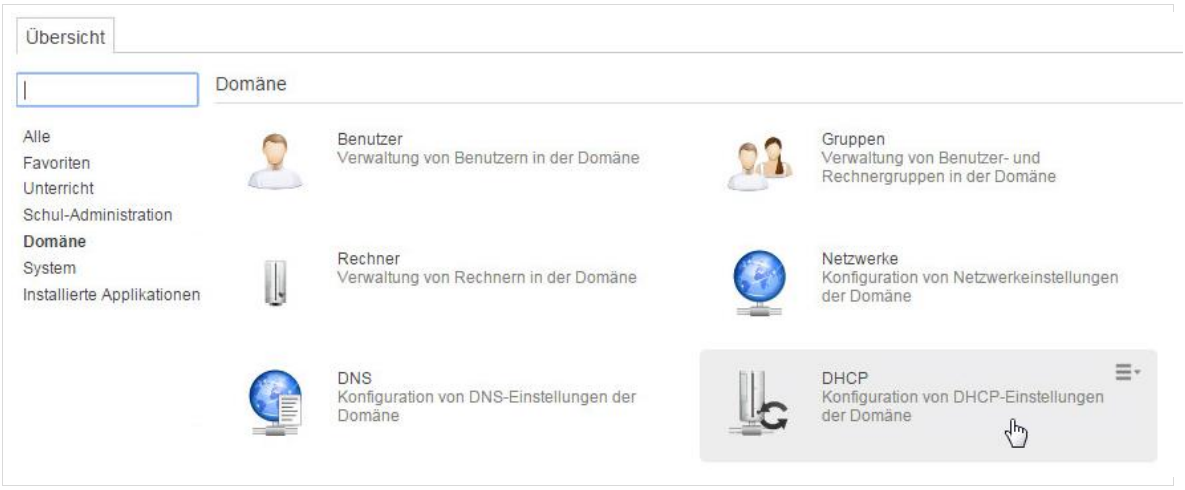

Abb. 48: Navigation zu den DHCP-Einstellungen

Wählen Sie die Domäne „*schule*“ aus:

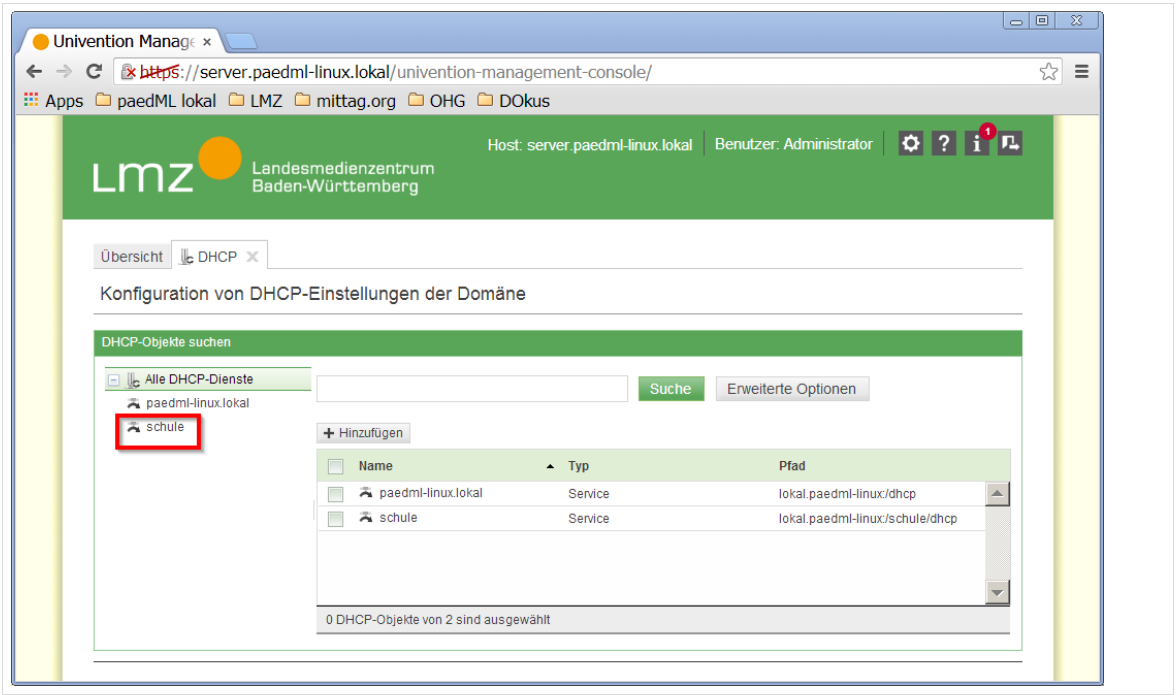

Abb.49: Auswahl der Domäne „schule“

Wählen Sie dann aus der Liste dasjenige Subnetz aus, dessen DHCP-Einstellungen geändert werden sollen; in diesem Falle eines der soeben neu erstellten Netze:

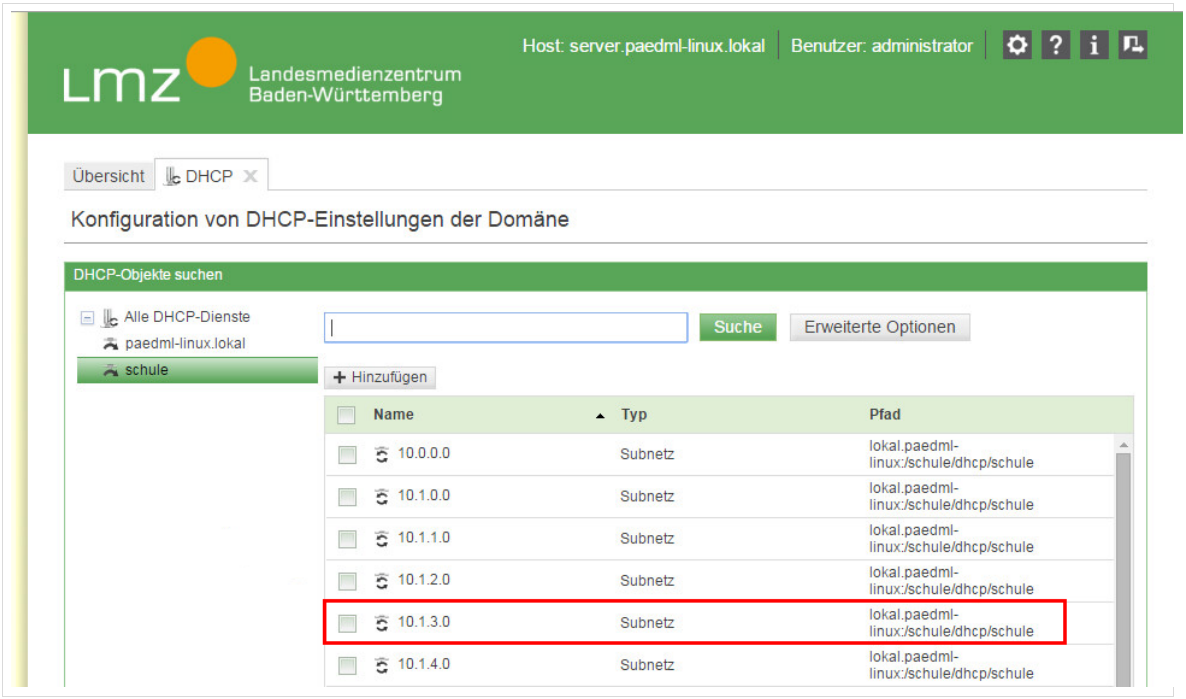

Abb. 50: Auswahl des zu bearbeitenden Subnetzes

Tragen Sie im Karteireiter „*Allgemein*“ unter „*Dynamische Adresszuweisung*“ den Bereich ein, aus dem die Clients bei der Rechneraufnahme per DHCP mit Adressen versorgt werden sollen. Klicken Sie zum Abschluss auf „*Änderungen speichern*“.

Schließen Sie den Reiter „*DHCP“* nicht, da er im nächsten Abschnitt benötigt wird.

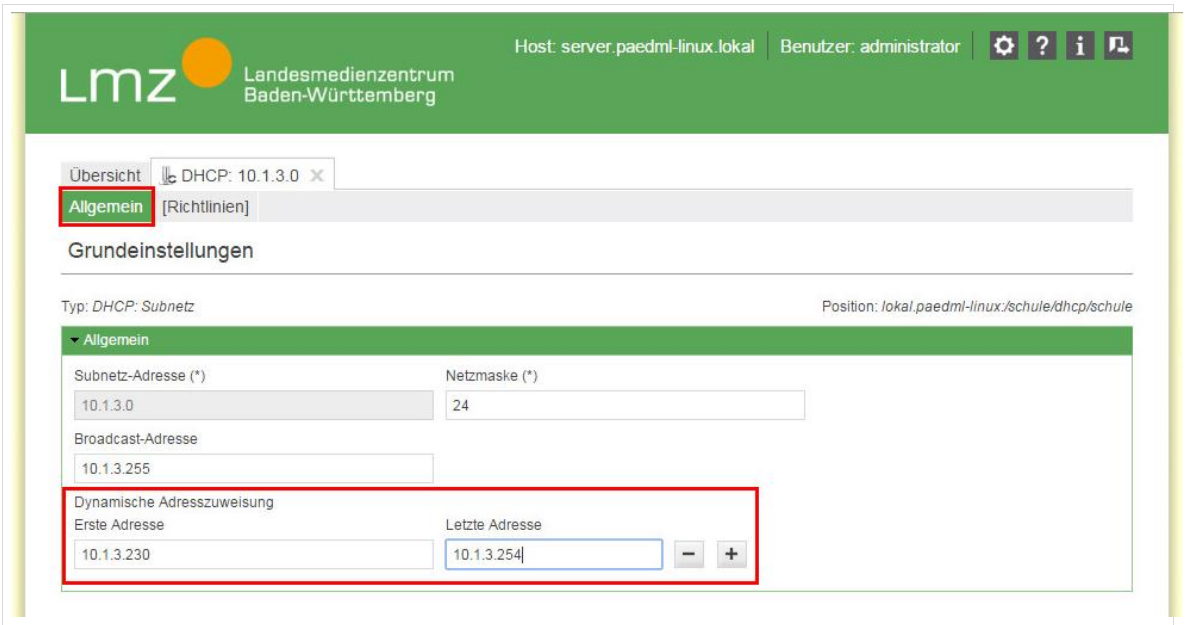

Abb. 51: Eintragen des IP-Bereichs

10.1.5 Kontrollieren des eingestellten DNS-Servers

Sie sollten sich nun noch immer im Reiter DHCP befinden. Wählen Sie erneut das Subnetz, das Sie soeben konfiguriert haben. Navigieren Sie auf den Karteireiter „[*Richtlinien*]“ und klicken Sie auf „*Richtlinie DHCP DNS“*. Überprüfen Sie, ob für die Domäne „*paedml-linux.lokal*“ der DNS-Server „*10.1.0.1*“ eingetragen ist.

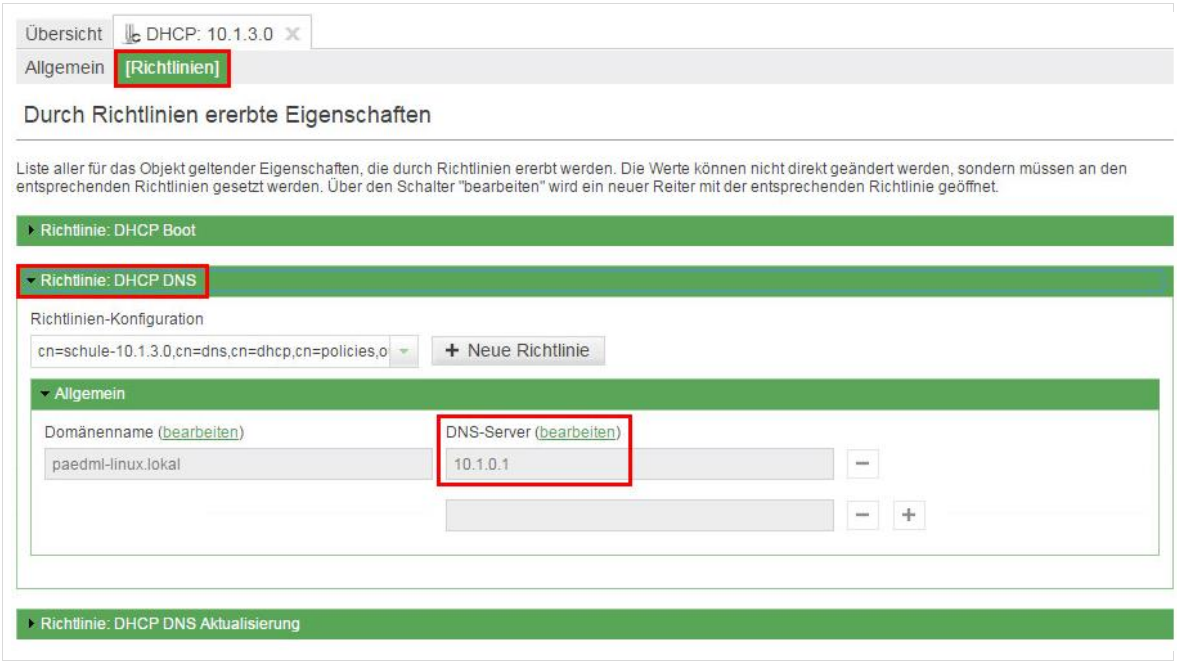

Abb. 52: Überprüfen der DNS-Einstellungen

Sollte hier kein DNS-Server eingetragen sein, so klicken Sie auf „*bearbeiten*“, tragen Sie im folgenden Fenster „*10.1.0.1*“ als IP-Adresse für den DNS-Server ein und klicken Sie dort auf „*Änderungen speichern*“:

Damit ist der DHCP-Dienst für das neue Netzwerk konfiguriert.

Wiederholen Sie die Arbeitsschritte aus Kapitel 10.1.4 und 10.1.5 für alle neu angelegten Netzsegmente!

10.1.6 Setzen der statischen Routen auf der VM „Server“

Auf den Maschinen „*Server*“, „*OPSI-Server“ und „Admin-VM“* müssen Routen zu den neuen Netzen definiert werden.

Für jedes neu definierte Netz muss eine statische Route über das Gateway 10.1.0.10 definiert werden. Das ist die IP des Routers im Netz „PAEDAGOGIK“ (bzw. „SERVERNETZ“, sofern Sie ein „LEHRERNETZ“ definiert haben), der in die neuen Netze routet.

Beispiel: Oben wurde das Netz *10.1.3.0/24* angelegt. Der Router hat im Netz „*PAEDAGOGIK*“ die IP *10.1.0.10*. Loggen Sie sich auf der VM „*Server*“ als Benutzer „*root*“ ein und führen Sie den folgenden Befehl (angepasst auf den IP-Bereich des neuen Netzes!) aus.

```
# ucr set "interfaces/eth0/route/10.1.3.0=net 10.1.3.0/24 gw 10.1.0.10"
```

Nach Ausführen des Befehls werden einige Dienste neu gestartet, Sie sollten folgende Konsolenausgabe erhalten:

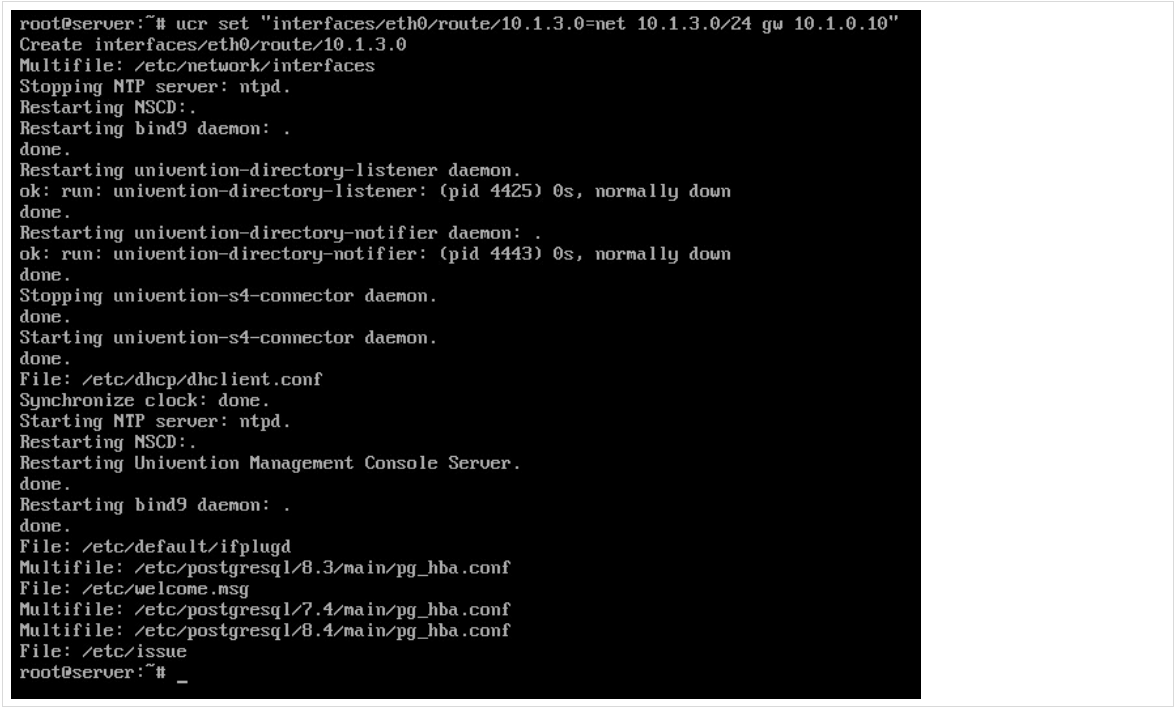

Abb. 53: Konsolenausgabe nach dem Setzen der statischen Route

10.1.7 Setzen der statischen Route auf der VM „*OPSI-Server*“

Wiederholen Sie das soeben beschriebene Setzen von Routen auf der VM „*OPSI-Server*“.

10.1.8 Setzen der statischen Route auf der VM *„Admin VM“*

Melden Sie sich an der virtuellen Maschine *„Admin VM*“ an. Führen Sie die Eingabeaufforderung von Windows als Administrator aus, indem Sie auf *„cmd.exe“* oder *„cmd64.exe“* mit der rechten Maustaste klicken. Danach wählen Sie *„Als Administrator ausführen“.*

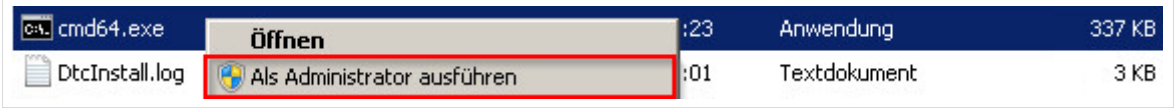

Abb. 54: Eingabeaufforderung als Administrator ausführen

In der Eingabeaufforderung müssen Sie nun die statische Route für alle von Ihnen eingerichteten Netze setzen. Beispielhaft wird dies für das *„große pädagogische Netz“* durchgeführt. Für andere Netze sind die Werte entsprechend anzupassen (siehe Kapitel 2.2):

```
route -p -4 add 10.2.0.0 mask 255.255.0.0 10.1.0.10
```

Die Option `-p` definiert, dass die Route dauerhaft gesetzt wird. `10.2.0.0` ist die Adresse des *„großen pädagogischen Netzes“.* Unter `mask` wird die Subnetzmaske angegeben und `10.1.0.10` ist in diesem Beispiel die Adresse des Routers.

10.2 Anpassungen an der Firewall

Auf der Firewall müssen folgende Anpassungen vorgenommen (bzw. überprüft) werden:

- Der Router, der das paedML-Netz „*PAEDAGOGIK*“ (bzw. „*SERVERNETZ*“) und die neu eingerichteten Netze verbindet, muss als Gateway definiert werden.

Im Auslieferungszustand ist der Gateway schon definiert.

Überprüfen Sie dennoch, ob der Gateway korrekt angelegt ist.

- Es muss je Netz eine statische Route eingerichtet werden, die den Netzwerkverkehr in das neu angelegte Netz leitet. Der Netzwerkverkehr wird über das Gateway geleitet.

Loggen Sie sich im Browser auf der VM „*Firewall*“ unter http://firewall.paedml-linux.lokal mit Benutzernamen „*Administrator*“ und dem dazugehörigen Passwort ein:

Abb. 55: Anmeldemaske der Firewall

10.2.1 Gateway eintragen

Sie befinden sich zunächst auf der Übersichtsseite der Firewall („*Dashboard*“).

Navigieren Sie über „*System* | *Routing*“ zu den Routing-Einstellungen der Firewall:

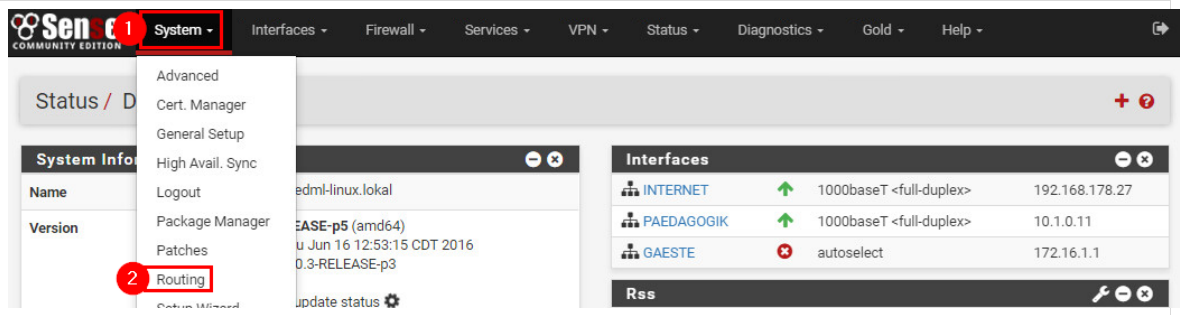

Abb. 56: Navigation zu den Routing-Einstellungen der Firewall

Anlegen eines neuen Gateways

Sie befinden sich im Reiter „*Gateways*“. Hier sollte der Eintrag „*Router*“ mit den Einstellungen aus dem Screenshot vorhanden sein. In diesem Fall ist der Gateway definiert.

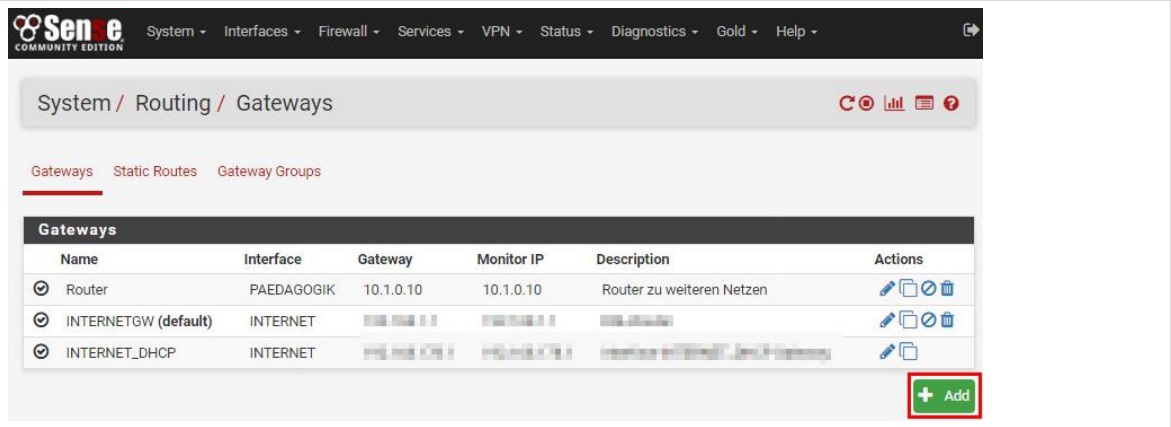

Abb. 57: Anlegen eines neuen Gateways

Sollte der Eintrag nicht vorhanden sein, so klicken Sie bitte auf das „+“-Icon, um einen neuen Gateway anzulegen.

Füllen Sie die in der folgenden Tabelle genannten Felder aus und speichern Sie mit „*Save*“.

Feld	Inhalt
Interface	Wählen Sie das Netz „PAEDAGOGIK“ aus
Name	Vergeben Sie einen Namen für das Gateway (Achtung: Keine Sonderzeichen verwenden!)
Gateway	Die IP des Gateways im Netz „PAEDAGOGIK“, im Standardfall also 10.1.0.10
Default Gateway	Haken nicht setzen
Description	Kurze Beschreibung, (Freitextfeld)

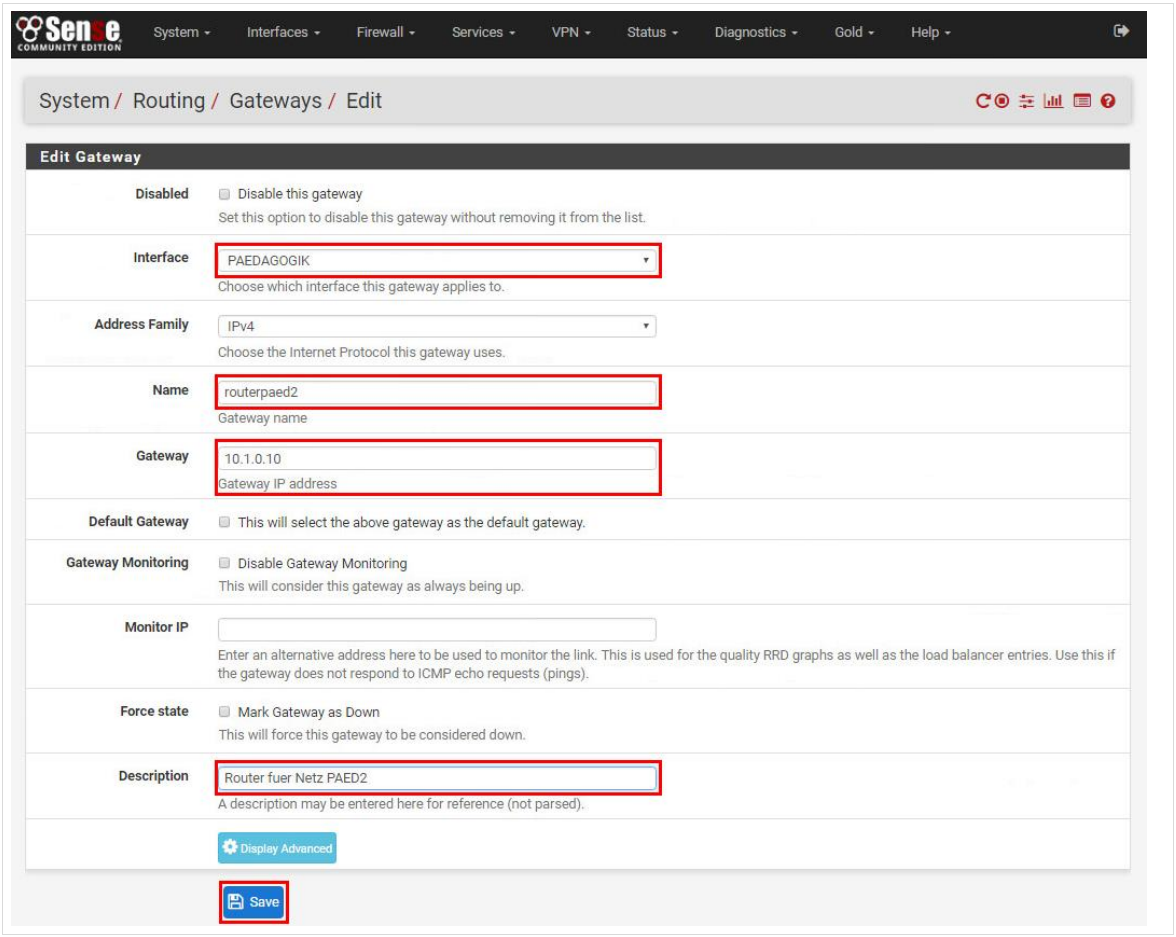

Abb. 58: Die Einstellungen für das neue Gateway

Überprüfen Sie die Einstellungen und übernehmen Sie die Änderungen endgültig mit Klick auf „*Apply changes*“:

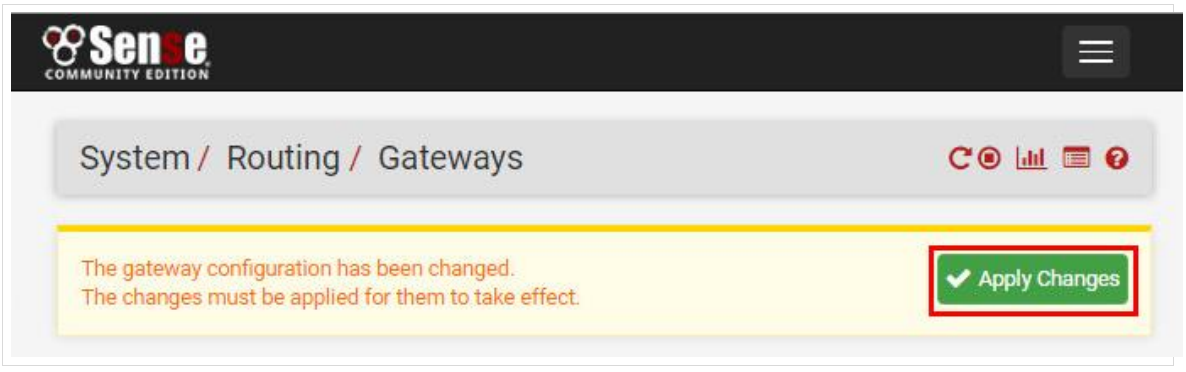

Abb. 59: Übernehmen der Änderungen

Die Meldung „*The changes have been applied successfully*“ zeigt an, dass der Gateway erfolgreich angelegt wurde.

10.2.2 Einrichten einer statischen Route

Diesen Vorgang müssen Sie für ALLE NEU angelegten NETZE WIEDERHOLEN!

Navigieren Sie zunächst durch Klick auf den Karteireiter „*Static Routes*“ zum Einstellungsbereich für die statischen Routen. Kunden, die mit dem Errata2-Update oder später installiert haben, sollten hier bereits Routen für das „*LEHRERNETZ*“, das Netz „*PAEADGOGIK*“ (kleines Pädagogisches Netz 10.1.2.0/24) und das Netz „*PAEDAGOGIK-GROSS*“ (10.2.0.0/16) vorfinden.

Wenn Sie diese Routen nicht haben, müssen sie ebenfalls eingerichtet werden.

Klicken Sie auf das „+“-Icon, um eine neue statische Route anzulegen:

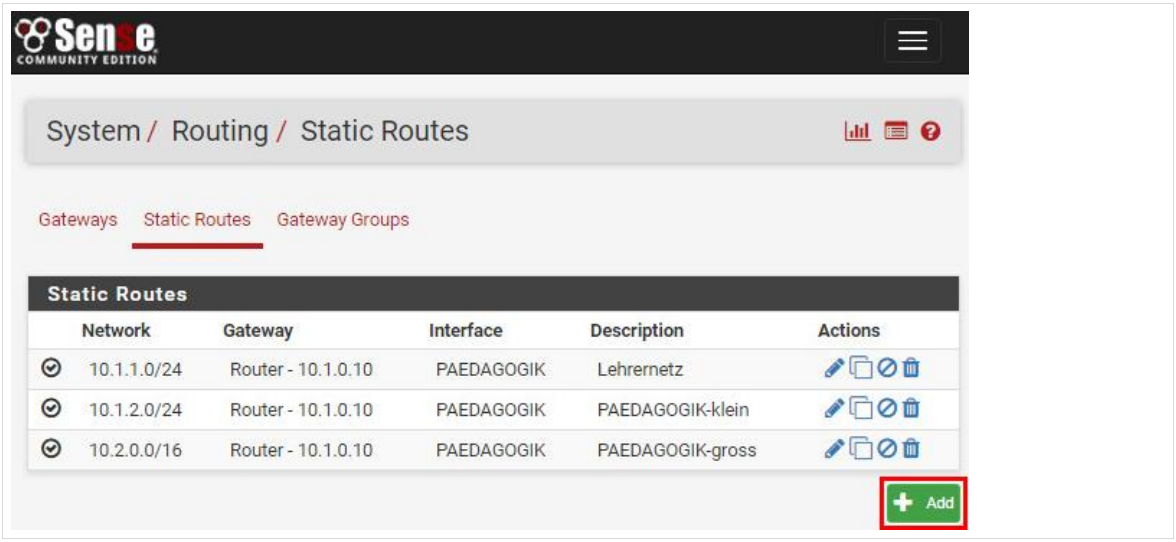

Abb. 60: Anlegen einer neuen statischen Route.

Füllen Sie dann die folgenden Felder aus und speichern Sie mit „*Save*“.

Feld	Inhalt
Destination Network	Das neue angelegte Netzwerk, in das die Route verweisen soll. In unserem Beispiel also *10.1.3.0/24*
Gateway	10.1.0.10
Disabled	Nicht anwählen. (Hiermit kann die Route deaktiviert werden, ohne den Eintrag wieder löschen zu müssen)
Description	Eine kurze Beschreibung der Route (Freitextfeld)

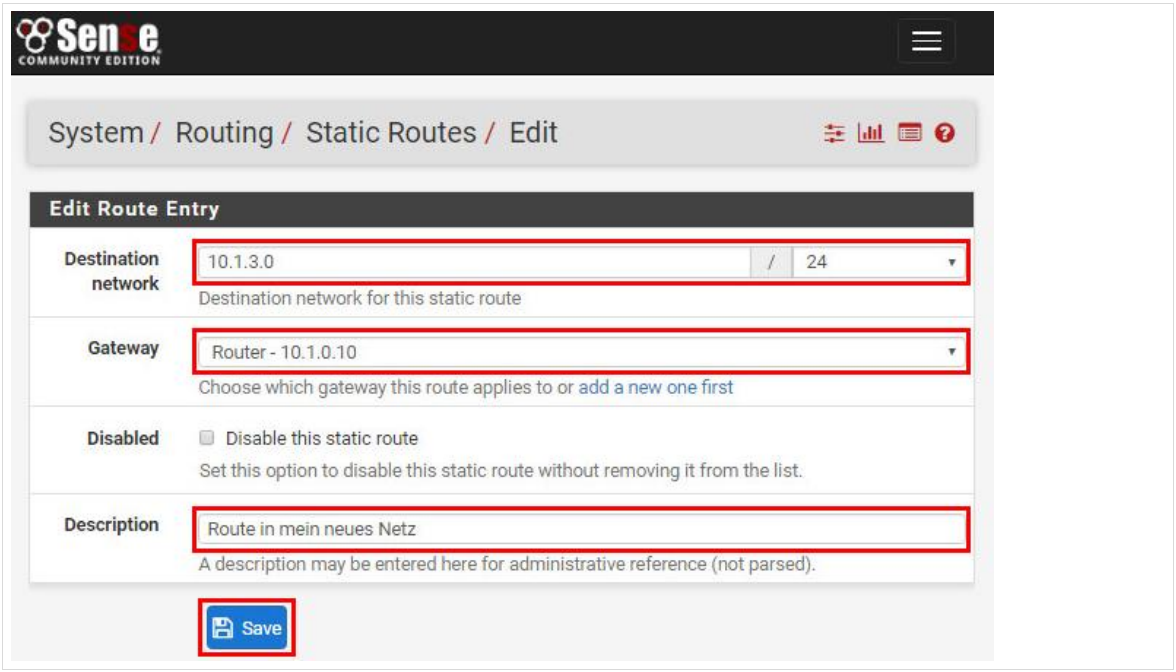

Abb. 61: Einstellungen für eine statische Route.

Überprüfen Sie die Einstellungen und übernehmen Sie die Änderungen endgültig durch Klick auf „*Apply changes*“.

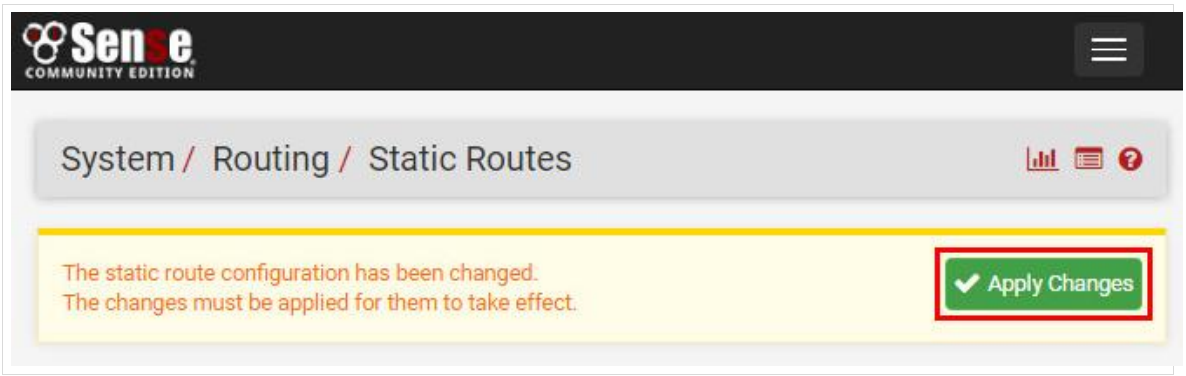

Abb. 62: Endgültiges Übernehmen der Änderungen.

Die Meldung „*The changes have been applied successfully*“ zeigt an, dass die statische Route erfolgreich angelegt wurde. Klicken Sie auf „*Close*“

Auf der Übersichtsseite „*Routes*“ erscheint nun die soeben angelegte statische Route:

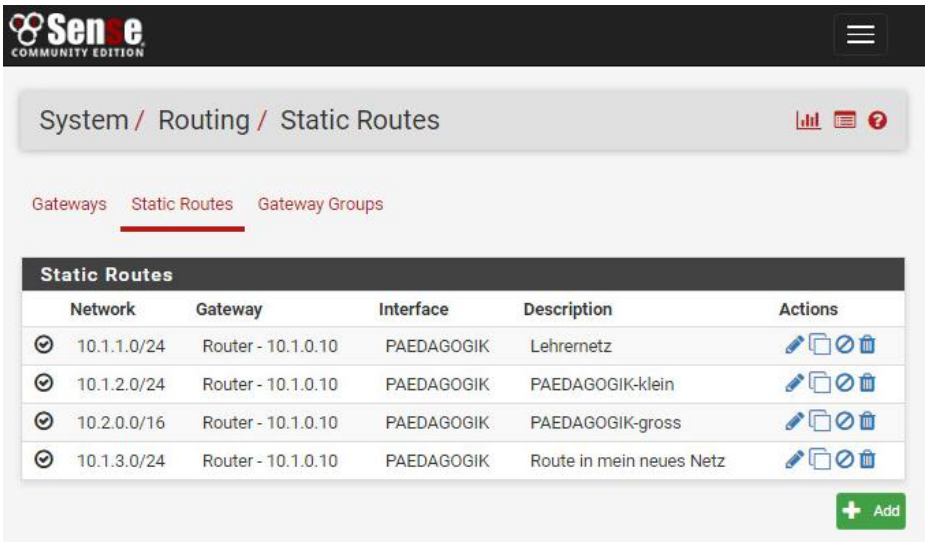

Abb. 63: Übersicht über alle statischen Routen

Melden Sie sich über „*System* | *Logout*“ wieder von der Firewall ab:

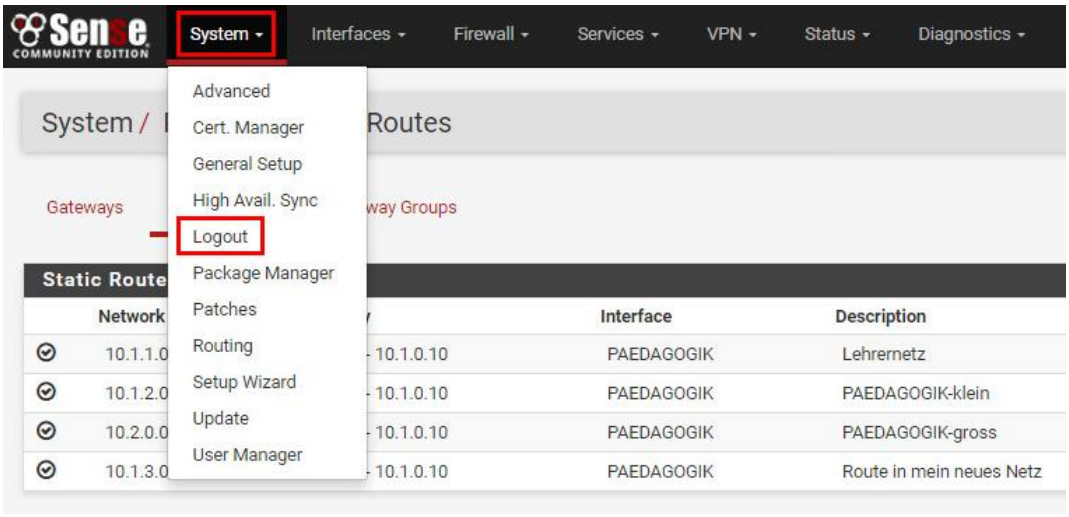

Abb. 64: Abmelden von der WebGUI der Firewall

10.2.3 Konfiguration des Routers

Damit die Einrichtung eigener Netze funktioniert benötigen Sie einen Router zwischen den Netzen. Die Einrichtung geschieht analog zu den Kapiteln 3 und 4 (Seite 16 ff.).

Aufgrund der Vielzahl von erhältlichen Routermodellen können die vorzunehmenden Einstellungen am Router an dieser Stelle nicht ausführlich beschrieben werden.

Prinzipiell sind auf dem Router folgende Einstellungen vorzunehmen:

WAN-Seite des Routers (Netz „*SERVERNETZ*“)

- Statische IP: 10.1.0.10
- Netzmaske: 255.255.255.0,
- Standardgateway: 10.1.0.11

Beispiel für LAN-Seite des Routers (das neu angelegte Netz)

- Statische IP: z.B. 10.1.5.1
- Netzmaske: z.B. 255.255.255.0
- DHCP: DHCP-Server des Routers ausschalten!

  Der Router darf nicht selbstständig IP-Adressen per DHCP vergeben sondern muss DHCP-Anfragen an das Netz „*PAEDAGOGIK*“ bzw. den Server (10.1.0.1) weiterreichen. Typische Bezeichnungen hierfür sind etwa „*DHCP Relaying*“ oder „*DHCP Forwarding*“.

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111

70190 Stuttgart