VLAN Installation und Routing mit pfSense, Mikrotik, DD-WRT oder Cisco RV Routern

aqui (Level 5) - Jetzt verbinden

01.03.2009, aktualisiert 01.05.2019, 273186 Aufrufe, 70 Kommentare, 9 Danke

Das folgende Tutorial beschreibt in einzelnen und einfach nachvollziehbaren Schritten, wie man die o.a. Firewall oder Router in eine bestehende, oder auch neu zu installiernde VLAN-Switch Infrastruktur, integriert bzw. an VLAN fähige Switches anschliesst um zwischen VLANs routen zu können, wenn kein Layer 3 (Routing) Switch verfügbar ist.
Damit ist eine sichere Kommunikation und Firewall Funktionalität zwischen (V)LANs (z.B. einem Gäste Netz abgetrennt vom Firmennetz) einfach und schnell realisierbar.
Die Verwendung von pfSense ist dabei nicht zwingend ! Das Tutorial zeigt eine allgemeine Lösung am Beispiel einfacher und preiswerter VLAN fähiger Router oder Firewalls.
Die VLAN Grundprozeduren zur Konfiguration gelten generell auch für andere Netzwerk Komponenten (Switches, Router, Firewalls, Server etc.) die allgemein VLANs nach dem IEEE 802.1q Standard supporten.

Inhaltsverzeichnis

Allgemeines zum Thema VLAN:

Das folgende Tutorial behandelt das Einrichten und Routen von VLANs auf Switches und Routern/Firewalls, also dem Segmentieren von Netzen was generell Skalierbarkeit und Performance in LAN Netzen sicherstellt.
Es wird vorausgesetzt das ein wenig Basiswissen zum Thema VLANs und VLAN-Tagging nach dem IEEE 802.1q Standard und VLANs im Allgemeinen vorhanden ist !
Als Basis Lektüre zum weiteren Verständnis und speziell zu diesem Thema VLAN sind folgende Informationen hilfreich und sinnvoll zu lesen:

Netzmafia:
http://www.netzmafia.de/skripten/netze/netz7.html#7.12
Edi's VLAN Tutorial:
http://www.schulnetz.info/2011/04/
bzw.
http://de.wikipedia.org/wiki/Virtual_Local_Area_Network
Als Video bei YouTube:
https://www.youtube.com/watch?v=TuGoZ9TgTOA
https://www.youtube.com/watch?v=Dah0wXQz0Q4
und
http://www.heise.de/netze/VLAN-Virtuelles-LAN--/artikel/77832
und auch VLANs auf Servern und Endgeräten:
https://www.administrator.de/VLAN_Routing_%C3%BCber_802.1q_Trunk_auf_MS_ ...

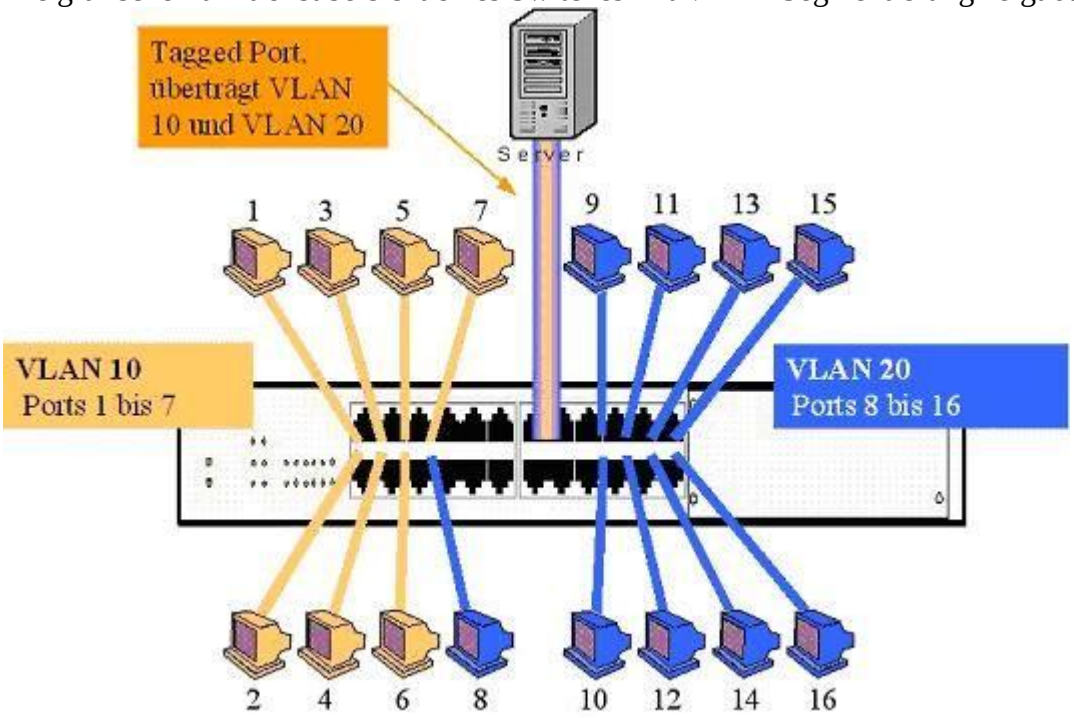
Das Tutorial lehnt sich bei einigen der hier vorgestellten Hardwarelösungen an bereits bei *Administrator.de* bestehende Tutorials an wie z.B. das Einrichten einer pfSense Firewall:
Preiswerte, VPN fähige Firewall im Eigenbau oder als Fertiggerät
oder auch das Tutorial zum Captive Portals bzw. Gäste Hotspots mit dieser Firewall:
WLAN oder LAN Gastnetz einrichten mit einem Captive Portal (Hotspot Funktion)
Oder bezieht sich auf Router Reviews wie z.B. das zum beliebten Mikrotik RB750(G)
Mikrotik RB750 - Quick Review

Diese Anleitung zur Einrichtung von VLAN Support ist keineswegs fest auf auf die o.a. pfSense Firewall bezogen, sondern kann ebenfalls problemlos für eine allgemeine Integration von VLAN (Tagging) fähigen Endgeräten in eine bestehende VLAN Umgebung verwendet werden, um so die Kommunikation zwischen VLAN Segmenten sicherzustellen.
Zwei weitere Punkte befassen sich mit der Einrichtung von VLANs bzw. VLAN Routing auf einem Router mit der populären DD-WRT Firmware auf *WRT54GL* oder *Buffalo WZR HP-G300NH* usw. Hardware und auf dem sehr preiswerten Mikrotik_Routern z.B. dem hEX oder preiswerteren hAPlite mit WLAN Port.
Die Linkliste am Schluß verweist zusätzlich auf die VLAN Konfiguration von Netzwerk Karten in Windows und Linux Rechnern unter anderem auch dem populären Raspberry Pi.

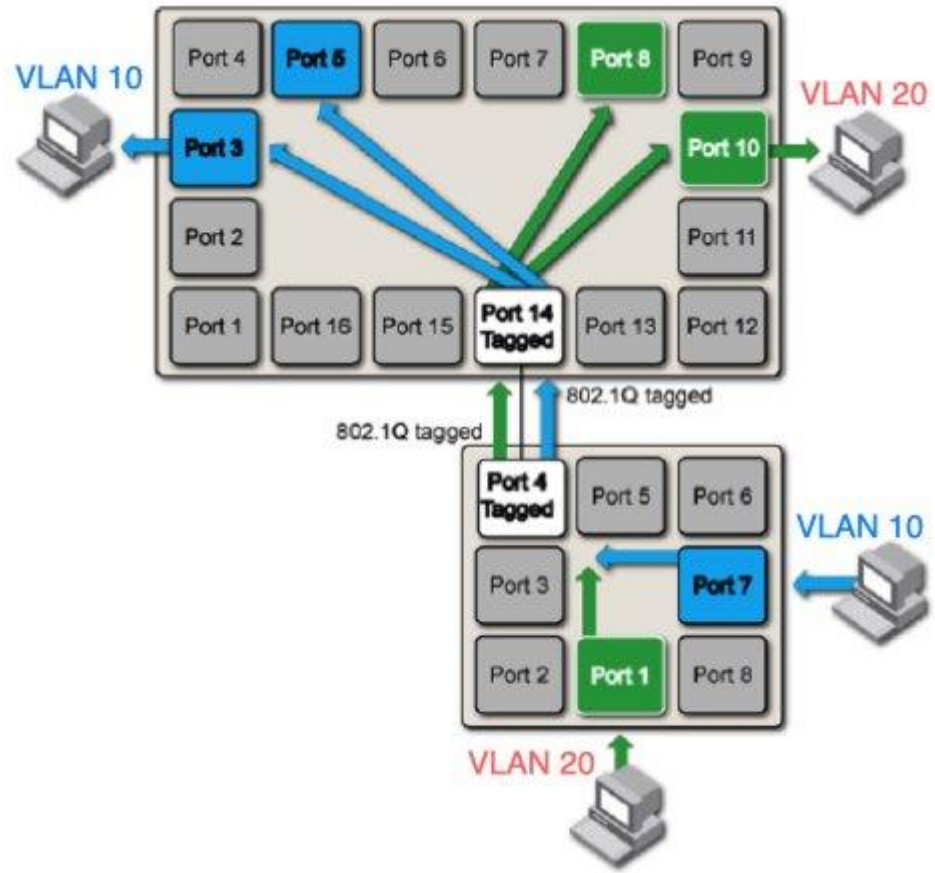
Alles in allem also eine Universalanleitung um eine Kommunikation zwischen VLANs bzw. VLAN Switches zu ermöglichen wenn diese LAN

Switches keine interne Layer 3 (Routing) Fähigkeit besitzen !
Nur zum Verständniss: Niemals darf man VLAN mit VPN verwechseln !
VLAN Technik bietet keine Verschlüsselung. Sie sorgt lediglich für einen Trennung, sprich das sich 2 und mehr Netzwerk Segmente (Subnetze) innerhalb eines VLAN Switches nicht "sehen", hat also mit "VPN" rein gar nichts zu tun.

Generell sind VLANs damit also völlig getrennte LAN Segmente (Layer 2 Broadcast Domains) auf einer Physik, sprich einem LAN Switch die per se erstmal **nicht** miteinander kommunizieren können. Sie verhalten sich wie physisch völlig getrennte LAN Netzwerke.
Kommunikation kann nur ein Router zwischen den VLANs herstellen.
Die grafische Funktionsübersicht eines Switches mit VLAN Segmentierung zeigt das folgende Bild:



Das folgende Prinzipschaubild zeigt 2 Switches (16 Port und 8 Port) die mit einem Tagged Uplink verbunden sind der die VLAN Information zwischen den Switches weitergibt:



Endgeräte Ports wie die der obigen PCs sind immer untagged, denn deren Ports werden im Switch fest dem jeweiligen VLAN zugeordnet. So erhält man z.B. 2 physisch völlig getrennte Netzwerke in einer gemeinsamen Switch Hardware. Der Sinn einer Segmentierung mit VLANs !
Ein Tagged Link kann statt eines Switches aber auch einen Router oder sog. MSSID WLAN Accesspoints (unten dazu mehr) anbinden wenn diese Endgeräte die in den Datenpaketen enthaltene VLAN Information benötigen. Dazu später mehr...

Dieses Tutorial geht nicht im Detail auf die Installation von pfSense und seine Router- bzw. Firewall und VPN Funktionen ein. Auch nicht auf das Flashen von DD-WRT Firmware auf den dafür passenden Routerplattformen.
Die vollständige Installationsprozedur für alle diese Hardwarelösungen beschreiben die u.g. Tutorials hier im Forum oder weitere Threads unten in

den **Weiterführenden Links**.

Die mit ca. 35 €uro preiswerteste Möglichkeit einfach und effektiv zwischen VLANs zu routen und Firewalling zu nutzen bietet ein Mikrotik Router RB 750 oder RB 750G (Gigabit) oder der aktuelle Nachfolger *hexLite* wie hier im Forum vorgestellt:
https://www.administrator.de/index.php?content=124700
Für größere Installationen in Bezug auf Ports und Performance ist aber eher ein Mikrotik 2011 empfehlenswert:
http://varia-store.com/Hardware/MikroTik-Routers/MikroTik-RouterBoard/R ...
bzw. ohne grafische Statusanzeige auf dem Front Panel bzw. wer darauf verzichten möchte:
http://varia-store.com/Wireless-Systeme/Fuer-den-Innenbereich/Mikrotik- ...
Diese Hardware ist auch Grundlage des Tutorials zum Routing zwischen 2 und mehr LAN IP Netzen:
https://www.administrator.de/index.php?content=56073#toc16

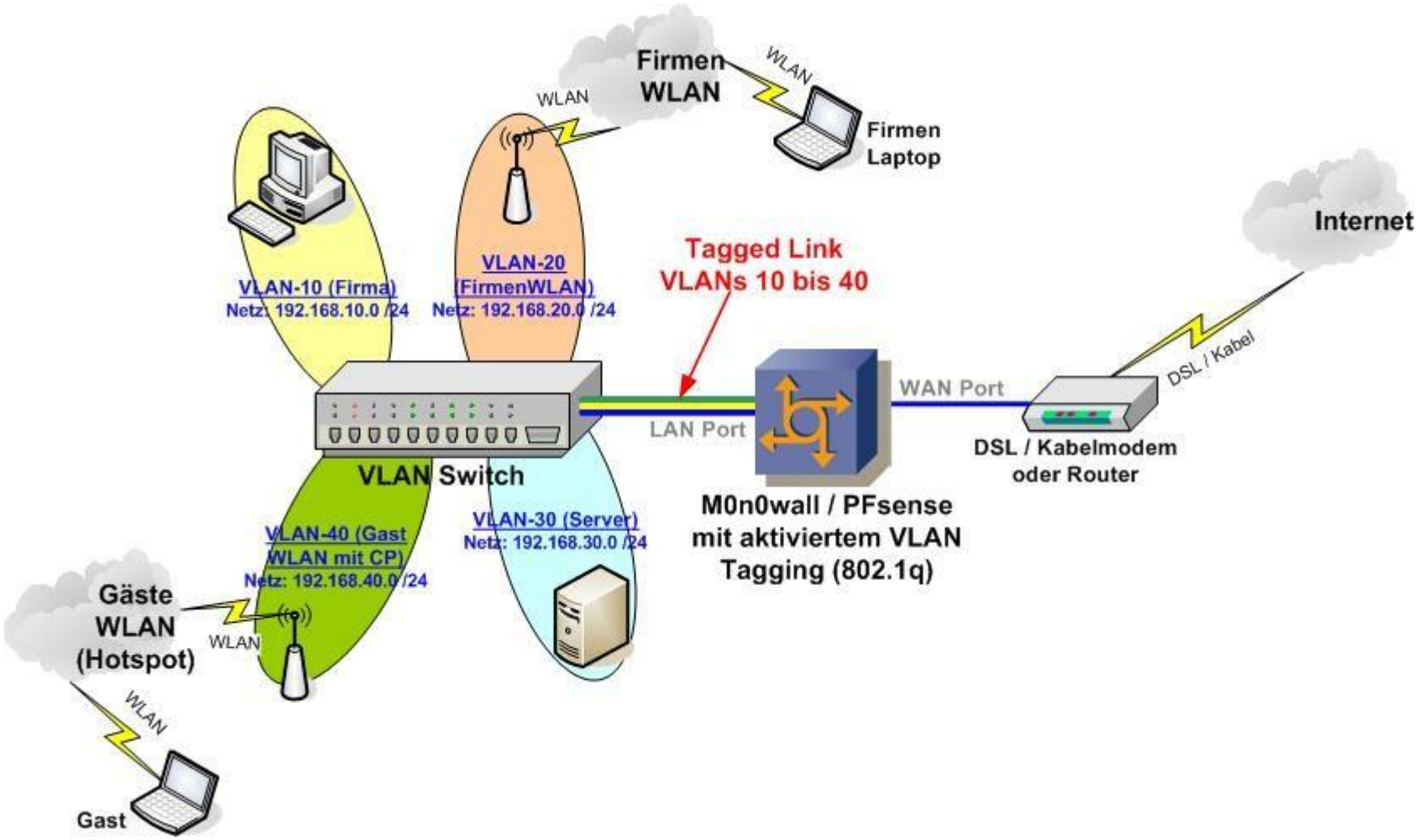
Wer mehr Sicherheit bei der VLAN Segmentierung fordert dem empfiehlt sich natürlich immer der Einsatz einer kleinen VLAN fähigen Firewall:
https://www.administrator.de/contentid/149915
Diese Hardware ist auch wiederum Grundlage des Captive Portal / Hotspot Tutorials für Gastnetze hier bei Administrator.de. Das u.a. Kapitel ***Praxisbeispiel*** beschreibt die Integration von Gstnetzen in eine VLAN Infrastruktur im Detail::
https://www.administrator.de/WLAN_oder_LAN_Gastzugang_einrichten_mit_ein ...
Infos zu DD-WRT Firmware findet man detailiert auf deren Webseite bzw. Wiki und in Teilen hier:
https://www.administrator.de/index.php?content=123285#toc2
Los gehts...

VLAN Netzdesign und Switches

VLAN fähige Switches sind heute mittlerweile gang und gäbe und das auch im billigen Consumer Bereich. Alle Hersteller in diesem Comodity Bereich haben sich auf den Produktnamen ***Websmart Switches*** geeinigt, welche sich über ein einfaches Webinterface konfigurieren lassen.
Populäre einfache Vertreter sind z.B.:
NetGear_GS105E_und_108E
D-Link_DGS-1210-16 bzw. die baugleiche 24 und 48 Port Variante
Trendnet_TEG-160WS

Cisco_SLM2024
Cisco_SG-200 (Sogar mit 8 Port Model und PoE)
HP-1700_Switch
Alle anderen Consumer Marken wie Allnet, Longshine & Co. sind ebenfalls mit entsprechenden Modellen vertreten.
Bei Premium Marken wie Cisco, Extreme, Brocade, Juniper ist die VLAN Funktionalität selbstverständlich.

Es wird für die folgenden Beispiele vorausgesetzt das bereits ein VLAN Switch vorhanden ist, der die entsprechenden VLAN IDs eingerichtet hat (IDs 10, 20 30 usw.) und ein Switchport, der sog. Uplink oder "Trunk" Port ist, wo alle VLANs **tagged** übertragen werden.
Pakete erthalten an diesem Port vom Switch einen VLAN Tag mit der Angabe des VLANs. Über diese VLAN ID Ziffer kann ein empfangener Switch oder Endgerät dieses Paket sofort wieder dem richtigen VLAN zuordnen.
In den beiden Switch Beispielkonfigurationen von Cisco und HP unten ist dies immer der Switchport **1** !
Generell kann die VLAN Zuordnung zu jedem vorhandenen Hardware Interface der pfSense Firewall, Router oder Server gemacht werden.
Als Beispiel für dieses Tutorial dient hier das VLAN Trunking auf dem Standard LAN Interface vr0 der pfSense (ALIX Hardware)



Analog kann dies natürlich auch auf dem WAN Interface vr1 oder dem dritten physischen "OPT" Interface vr2 (sofern vorhanden) passieren, sollte man z.B. mehrere unabhängige Gast VLANs, Firmen VLANs oder generell mehrere unabhängige IP Segmente (Netze) einrichten wollen.
Auch eine VLAN Struktur an mehreren Interfaces parallel ist machbar, wenn auch weniger sinnvoll.

Wichtig ist hierfür immer das sog. *Parent Interface* (Basis Interface) an der pfSense, zu dem die VLANs bzw. deren ID Taggings korrespondieren. Will man also wie hier im Beispiel das LAN Interface (vr0) als sog. "Parent" Interface für die VLANs verwenden, dann wird das Default VLAN 1 hier untagged übertragen und alle weiteren VLANs auf diesem Interface mit einem 802.1q Tag versehen, denn entsprechende VLAN fähige Switches dann wieder verstehen.
Wenn Router/Firewall und VLAN-Switch auf dem Tisch liegen kanns losgehen...

VLAN Setup auf dem Netzwerk Switch

Es gibt eine Vielzahl solcher Switches am Markt, da die Netz Segmentierung mit VLANs heutzutage auch in kleineren Netzen mittlerweile zum Standard gehört.
Zum erfolgreichen Anschluss der VLAN Router oder Firewall Konfiguration an eine bestehende Switch Infrastruktur mit VLAN Nutzung gehört natürlich zuallererst auch die Betrachtung der Switch Konfiguration bzw. der Anschluss des so eingerichteten Router Ports an einen VLAN fähigen Switch. Dies geschieht immer über einen sog. **Tagged** Uplink !
Die Einrichtung wird deshalb hier beispielhaft an zwei VLAN fähigen Switches wie dem Cisco Catalyst 29xx und einem billigen HP ProCurve Switch beschrieben und zusätzlich an 2 sog. "Web Smart" Switches von D-Link und Trendnet.
Bei anderen VLAN oder Web Smart Switch Herstellern im Consumer Bereich ist das Verfahren analog ! Ggf. sogar per simplen Mausklick über das Web Management des Switches zu machen wie bei Linksys, D-Link oder NetGear u.a.

Die beschriebenen Switches haben im Beispieldesign folgende Portzuordnung:

Switch Port 1: Uplink Anschluss der o.a. konfigurierten pFsense/M0n0wall, Tagged Links für alle VLANs 10 bis 40 und VLAN 1 (Default VLAN)
Switch Port 10-11: Endgeräte (untagged) VLAN 10
Switch Port 12-13: Endgeräte (untagged) VLAN 20
Switch Port 14-15: Endgeräte (untagged) VLAN 30
Switch Port 16-17: Endgeräte (untagged) VLAN 40

Beispiel Konfiguration Cisco Catalyst IOS Switch


```
Cisco_Switch#

clock timezone MET 1
clock summer-time MEST recurring last Sun Mar 2:00 last Sun Oct 3:00
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 description Tagged Link zur Firewall
 switchport mode trunk
 switchport trunk encapsulation dot1q
(switchport trunk allow vlan all)   -->> (neuere IOS Versionen)
!
interface FastEthernet0/10
 description Enduser Ports in VLAN 10
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet0/11
 description Enduser Ports in VLAN 10
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet0/12
 description Enduser Ports in VLAN 20
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/13
 description Enduser Ports in VLAN 20
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/14
 description Enduser Ports in VLAN 30
 switchport access vlan 30
```

```
 spanning-tree portfast
!
interface FastEthernet0/15
 description Enduser Ports in VLAN 30
 switchport access vlan 30
 spanning-tree portfast
!
interface FastEthernet0/16
 description Enduser Ports in VLAN 40
 switchport access vlan 40
 spanning-tree portfast
!
interface FastEthernet0/17
 description Enduser Ports in VLAN 40
 switchport access vlan 40
 spanning-tree portfast
!
!
interface Vlan1
 ip address 172.16.1.254 255.255.255.0
 no ip route-cache
!
no ip http server
ip http secure-server
!
end
```

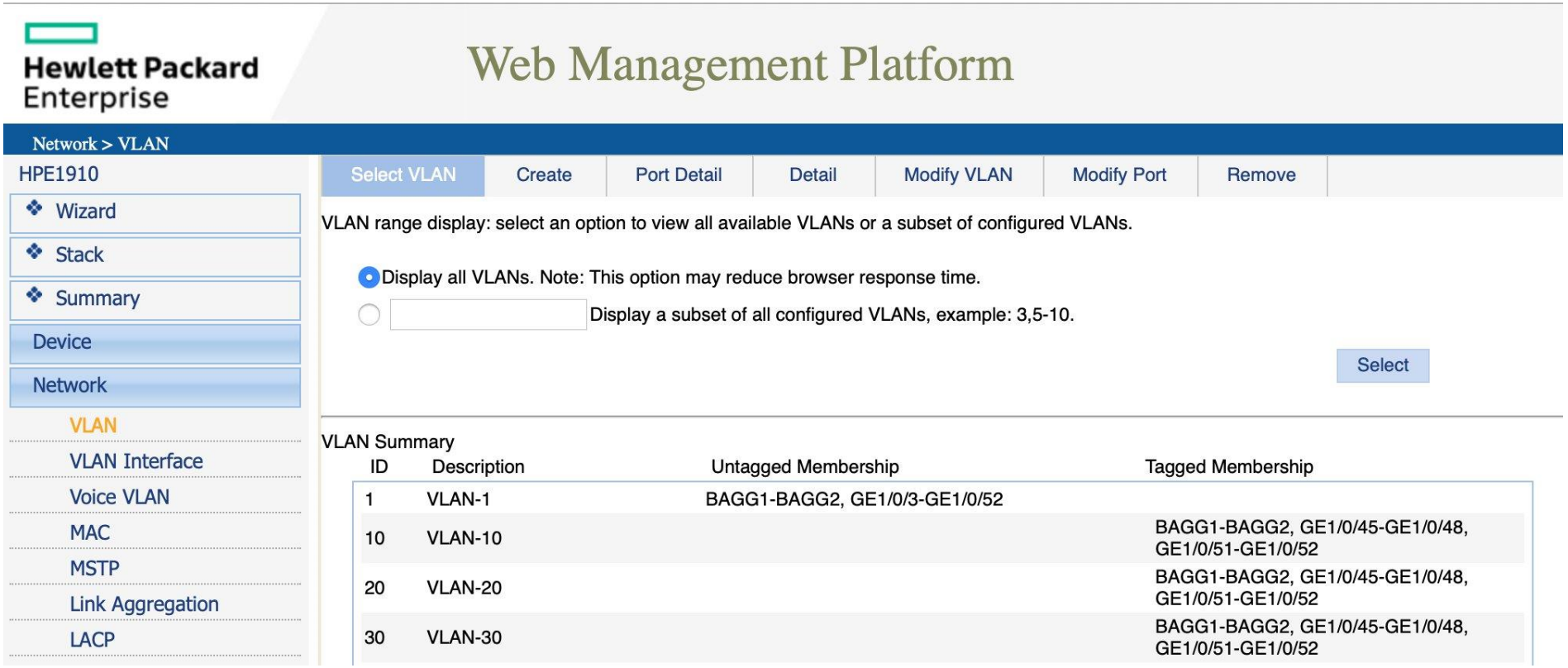
Beispiel Konfiguration HP ProCurve Switch (CLI)


```
HP_Switch#

time timezone 60
time daylight-time-rule Middle-Europe-and-Portugal
spanning-tree protocol-version rstp
spanning-tree force-version rstp-operation
exit
interface 1
```

```
   name "VLAN Tagged Link zur Firewall"
exit
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-9
   ip address 172.16.1.254 255.255.255.0
   exit
vlan 10
   name "Firma"
   untagged 10-11
   tagged 1
   exit
vlan 20
   name "Firmen WLAN"
   untagged 12-13
   tagged 1
   exit
vlan 30
   name "Server"
untagged 14-15
   tagged 1
   exit
vlan 40
   name "Gaeste Netzwerk"
untagged 16-17
   tagged 1
   exit
```

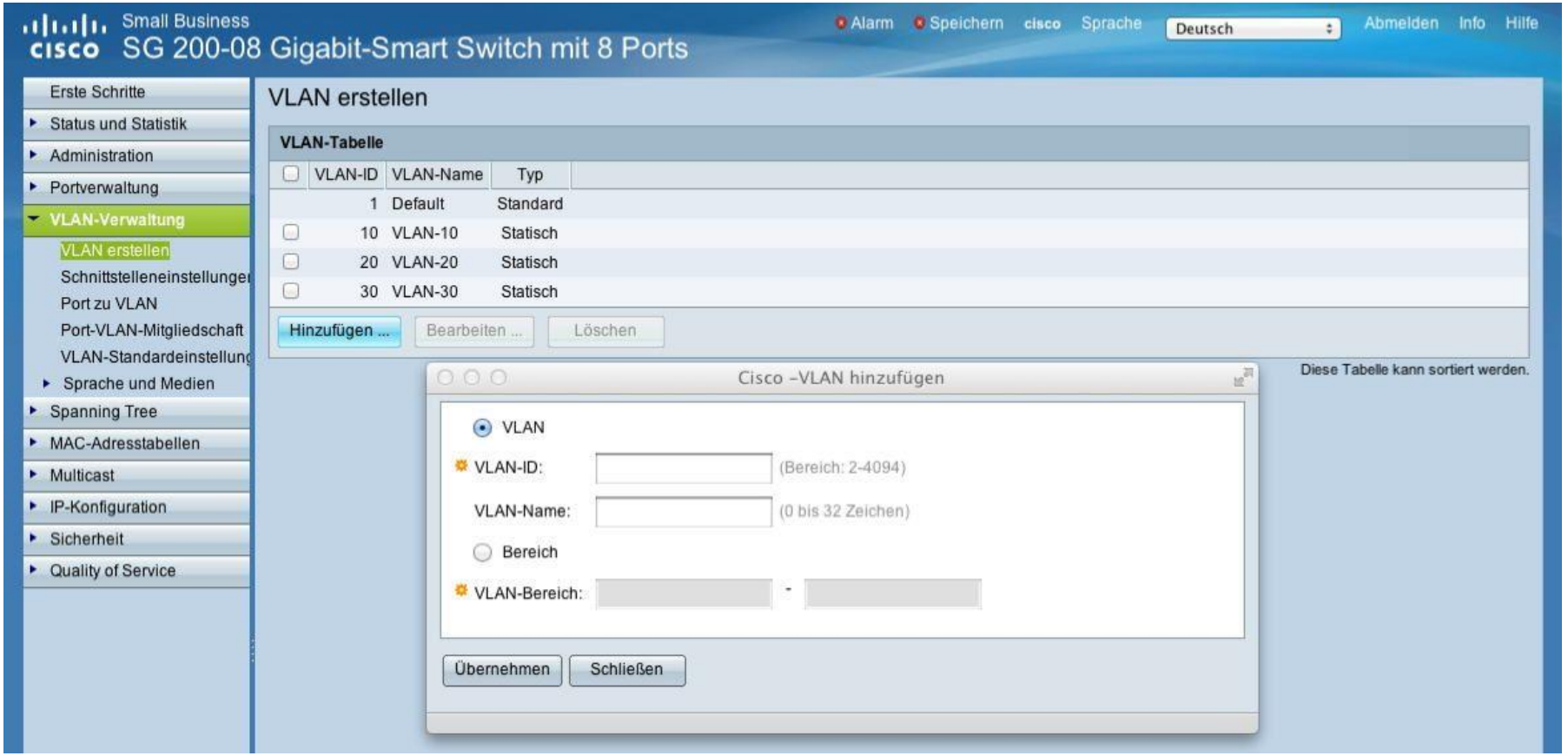
Beispiel Konfiguration HP WebSmart Switch V1910

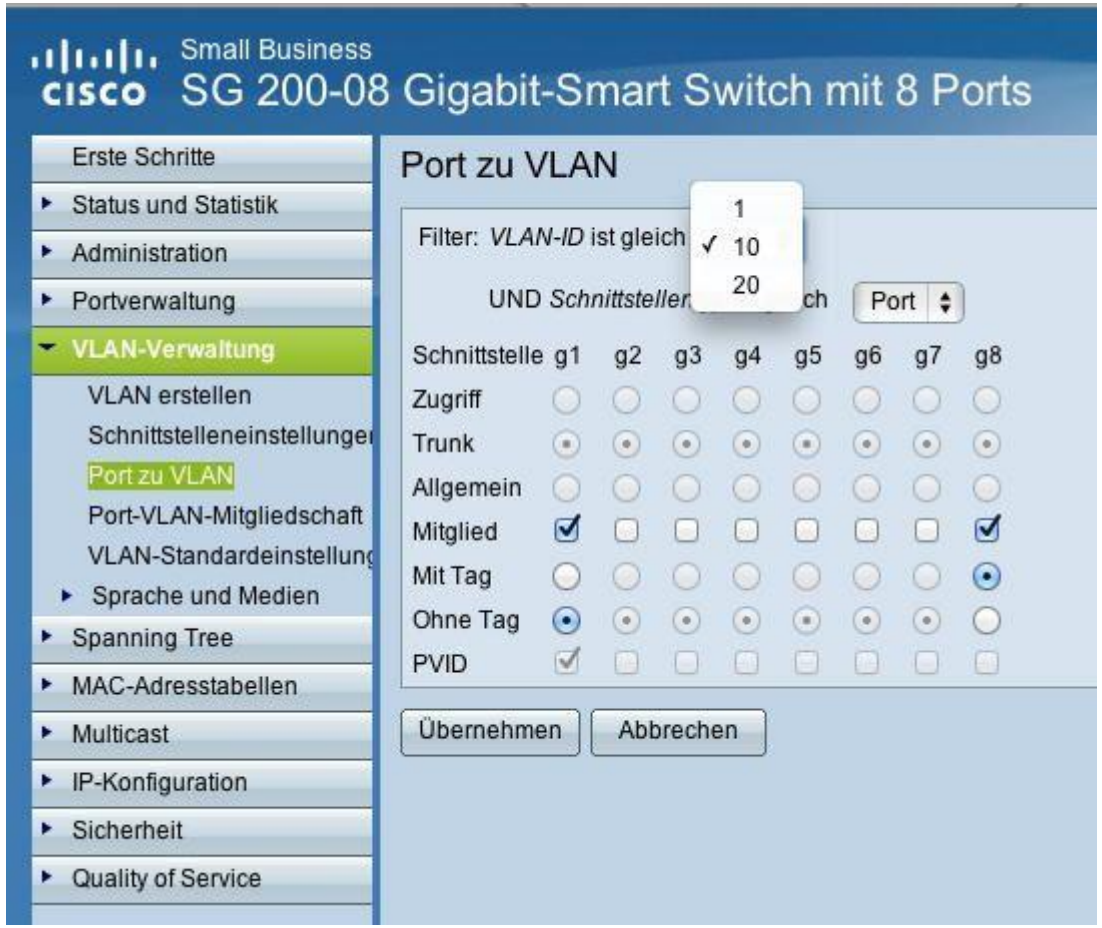


Siehe zum HP V1910 auch hier.

Beispiel Konfiguration Cisco Switch SG-200er Serie

Den Reigen der Beispielkonfigurationen für die zahllosen SOHO (Small Office, Home Office) Web Smart Switches eröffnet ein Cisco aus der SF bzw. SG-200er Serie.
Die Konfiguration ist in der Grundstruktur immer gleich wie die folgenden Screenshots aus einer Auswahl verbreiteter Web Smart VLAN Switches zeigen.
Sie besteht immer aus den zwei Schritten: VLAN einrichten, Switchports den VLANs tagged (mit VLAN ID) oder untagged zuordnen:


Small Business
cisco SG 200-08 Gigabit-Smart Switch mit 8 Ports
Alarm
Speichern
cisco
Sprache
Deutsch
Abmelden
Info
Hilfe
Erste Schritte
Status und Statistik
Administration
Portverwaltung
VLAN-Verwaltung
VLAN erstellen
Schnittstelleneinstellunge
Port zu VLAN
Port-VLAN-Mitgliedschaft
VLAN-Standardeinstellun
Sprache und Medien
Spanning Tree
MAC-Adresstabellen
Multicast
IP-Konfiguration
Sicherheit
Quality of Service
VLAN erstellen
VLAN-Tabelle
VLAN-ID
VLAN-Name
Typ
1 Default Standard
10 VLAN-10 Statisch
20 VLAN-20 Statisch
30 VLAN-30 Statisch
Hinzufügen ...
Bearbeiten ...
Löschen
Diese Tabelle kann sortiert werden.
Cisco –VLAN hinzufügen
VLAN
VLAN-ID:
(Bereich: 2-4094)
VLAN-Name:
(0 bis 32 Zeichen)
Bereich
VLAN-Bereich:
Übernehmen
Schließen

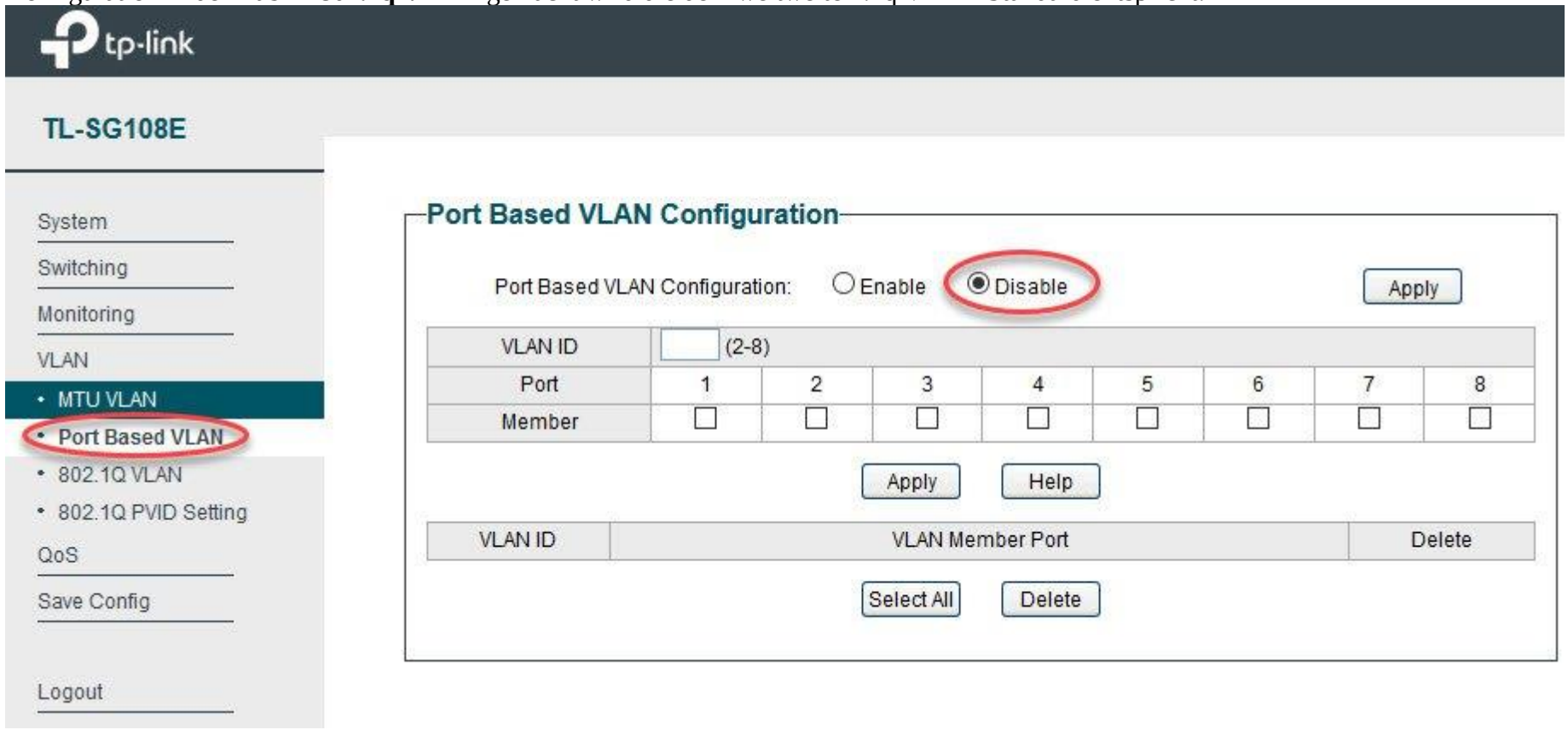


Der Port G8 ist hier der tagged Port im VLAN 10 der mit dem o.a. beschriebenen Router/Firewall verbunden ist.

Beispiel Konfiguration TP-Link SG108E Switch

Der TP-Link ist ein einfacher und preiswerter Websmart Switch der sich über sein internes GUI schnell konfigurieren lässt.
Zuerst schaltet man global die proprietäre Port based VLAN Funktion ab. Das klingt verwirrend ist aber normal, da die "richtige" VLAN

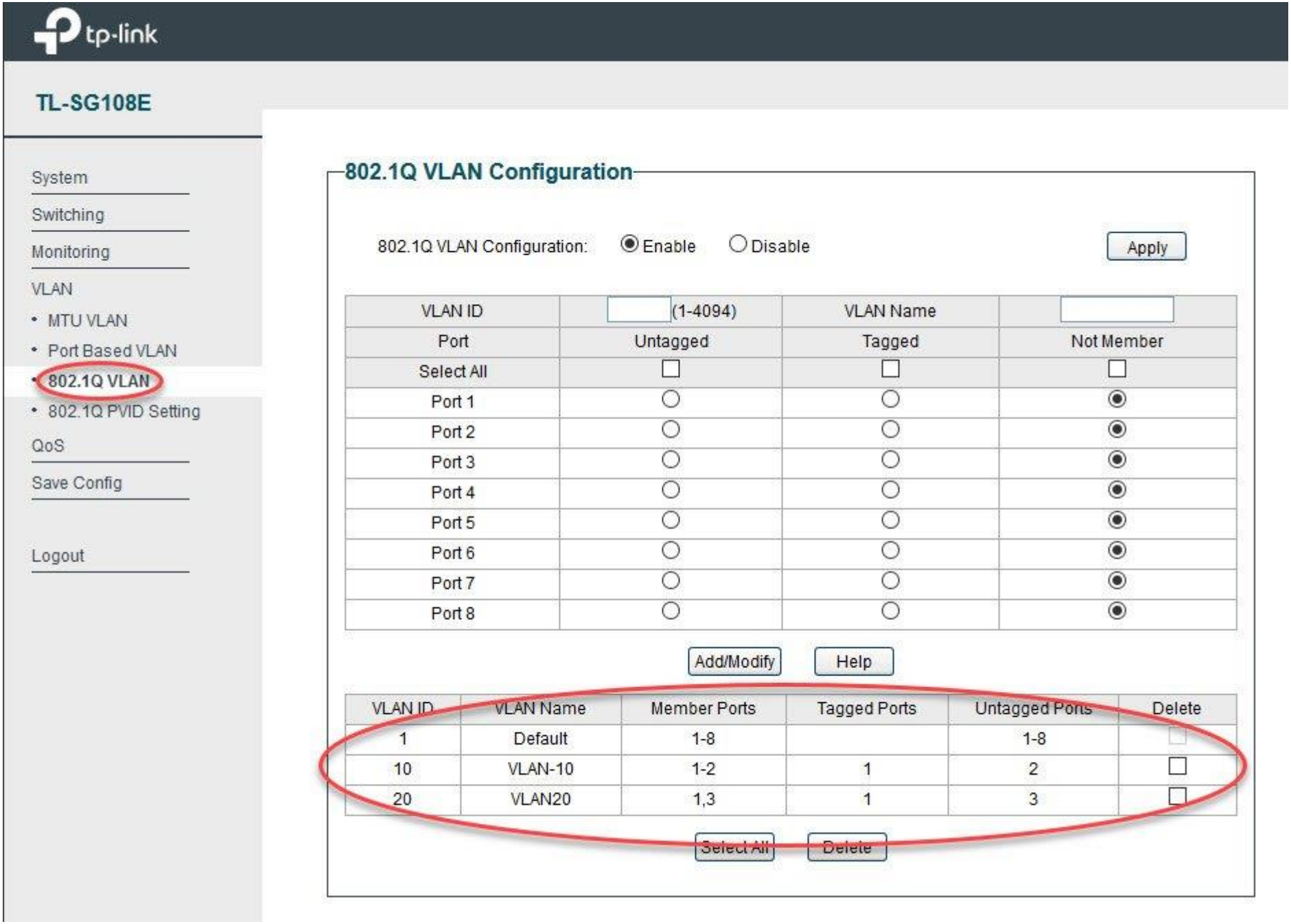
Konfiguration in der Rubrik **802.1q VLAN** gemacht wird die dem weltweiten .1q VLAN Standard entspricht.



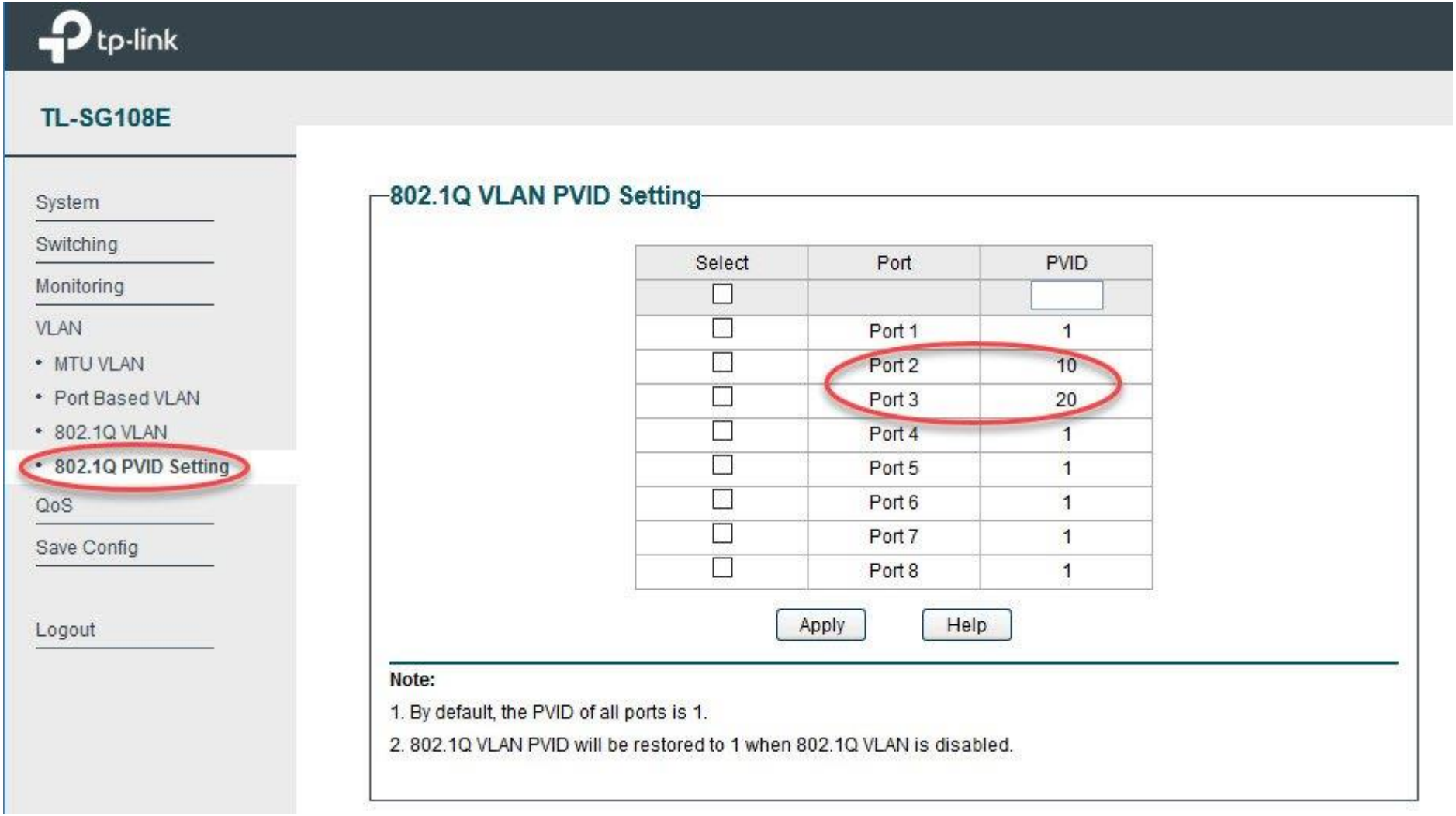
Danach legt man die beiden Beispiel VLANs 10 und 20 an und weist ihnen den Uplink Port als Tagged zu und die die jeweiligen Endgeräte Ports 2 und 3 als Untagged.
Hier im Beispiel ist folgende Port Zuordnung gemacht:

- Switchport 1 = Tagged Uplink auf den Router / Firewall mit VLAN 10 tagged, VLAN 20 tagged und Default VLAN 1 untagged
- Switchport 2 = Untagged als Endgeräteport im VLAN 10
- Switchport 3 = Untagged als Endgeräteport im VLAN 20

- Switchport 4-8 = Untagged als Endgeräteport im Default VLAN 1

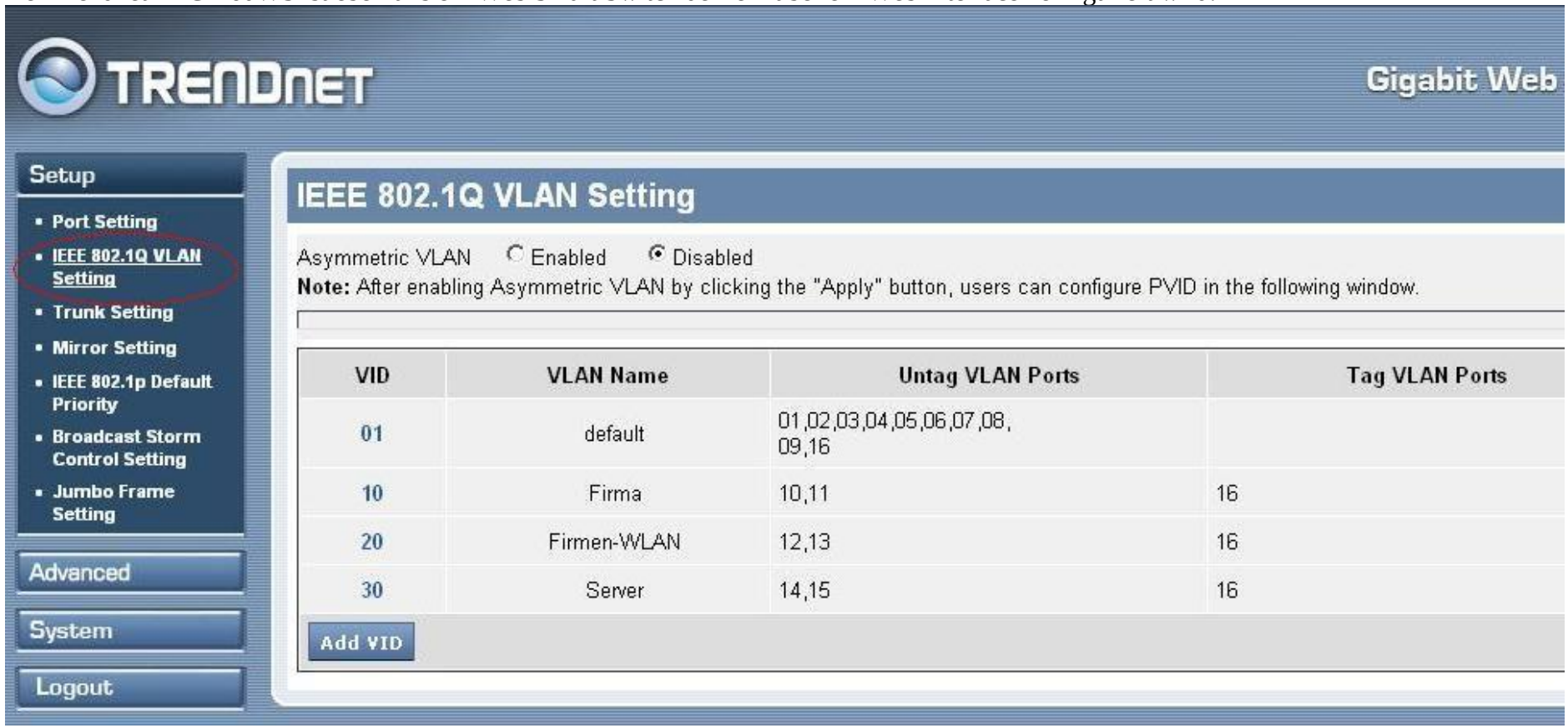

tp-link
TL-SG108E
System
Switching
Monitoring
VLAN
• MTU VLAN
• Port Based VLAN
• 802.1Q VLAN
• 802.1Q PVID Setting
QoS
Save Config
Logout
802.1Q VLAN Configuration
802.1Q VLAN Configuration: Enable Disable
Apply
VLAN ID (1-4094) VLAN Name
Port Untagged Tagged Not Member
Select All
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Add/Modify
Help
VLAN ID VLAN Name Member Ports Tagged Ports Untagged Ports Delete
1 Default 1-8 1-8
10 VLAN-10 1-2 1 2
20 VLAN20 1,3 1 3
Select All
Delete

Der TP-Link Switch ist wie der u.a. Netgear ein Switch OHNE Auto PVID im Gegensatz zum oben vorgestellten Cisco!
D.h. die Port VLAN ID muss zwingend manuell im Setup zugewiesen werden. Das ist die ID, die angibt in welches VLAN eingehende, ungetaggte Pakete geforwardet werden. Im Default steht dieser Wert immer auf 1 was für die oben konfigurierten Ports 2 und 3 (VLAN 10 und 20) fatal wäre, denn dann hätte man einen VLAN Mismatch.
Ausgehende Pakete kommen dann aus dem jeweiligen eingestellten VLAN aber eingehende Pakete werden immer ins VLAN 1 geforwardet was dann sofort zur Fehlfunktion führt!
Dieser Punkt wird leider sehr oft vergessen und falsch eingestellt und führt dann in der Konsequenz zu Fragethreads hier im Forum. Deshalb hat das Tutorial einen eintsprechenden Menüpunkt auch in den weiterführenden Links was das Thema PVID Einstellung anbetrifft. Bitte unbedingt beachten !!
Die PVIDs müssen also bei diesen Switches immer richtig zum korrespondierenden VLAN an den untagged Endgeräteports gesetzt werden !



Beispiel Konfiguration Web Smart Switch Trendnet TEG-160WS

Der Trendnet TEG-160WS ist ebenfalls ein Web Smart Switch der rein über ein Web Interface konfiguriert wird:

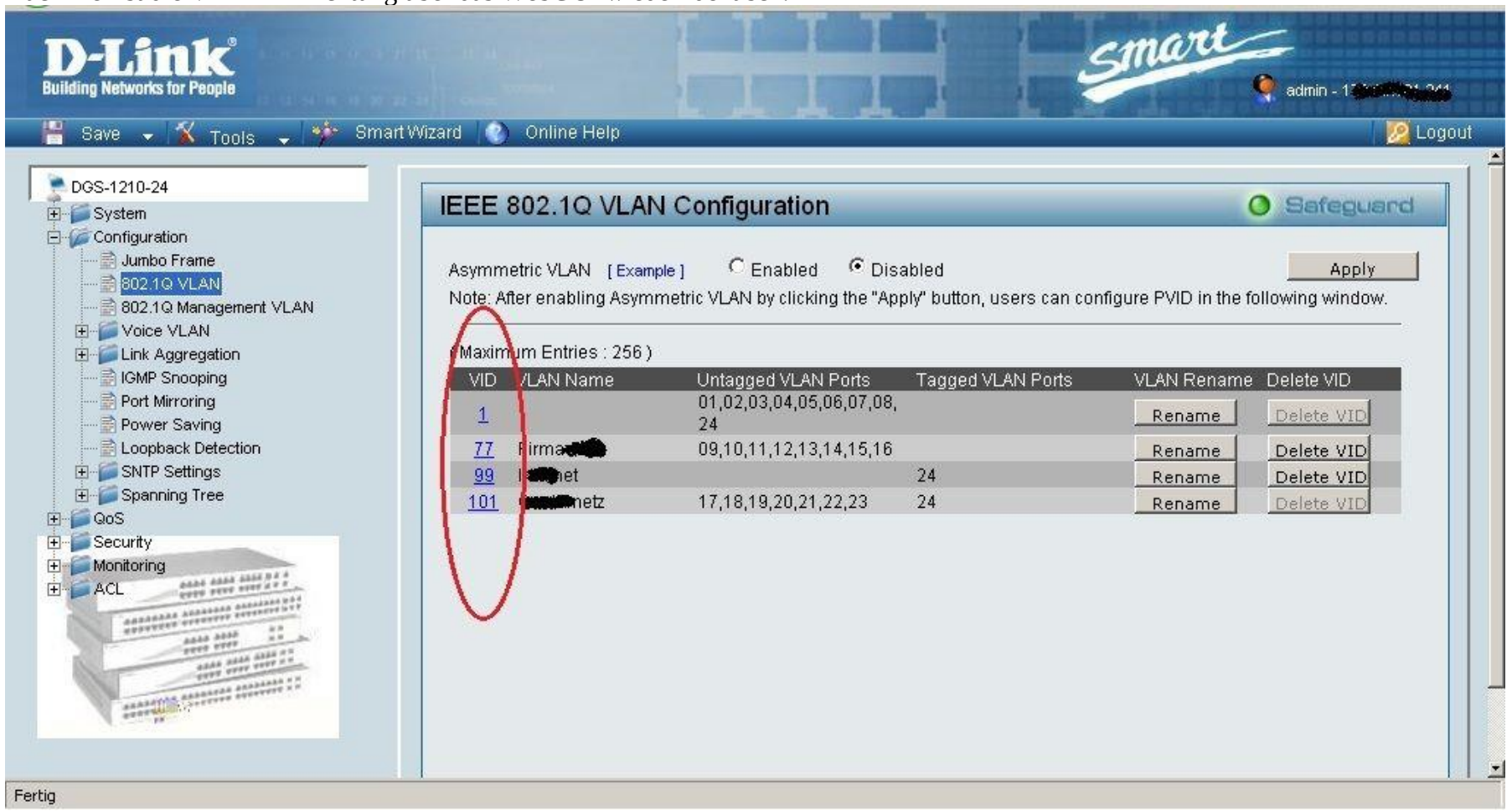


(Uplink Port zur VLAN Firewall Router ist hier Port 16 !)

Verbindet man nun den Uplink Port (Port 1) des Switches (Port 16 beim o.a. Trendnet Beispiel) mit dem VLAN Port der Firewall (LAN Port) steht einem ersten Test nichts mehr im Wege !
Ein Ping zwischen Endgeräten in den unterschiedlichen VLANs sollte nun problemlos möglich sein sofern die Firewall Regeln entsprechend stimmen !
Über diese Regel ist hinterher, sofern gewünscht, eine Einschränkung der Kommunikation sehr leicht möglich um z.B. Gast VLANs mit eingeschränkten Zugriffsrechten zu betreiben und andere VLANs vor unberechtigtem Zugriff zu schützen.

Beispiel Konfiguration Web Smart Switch D-Link DGS-1210

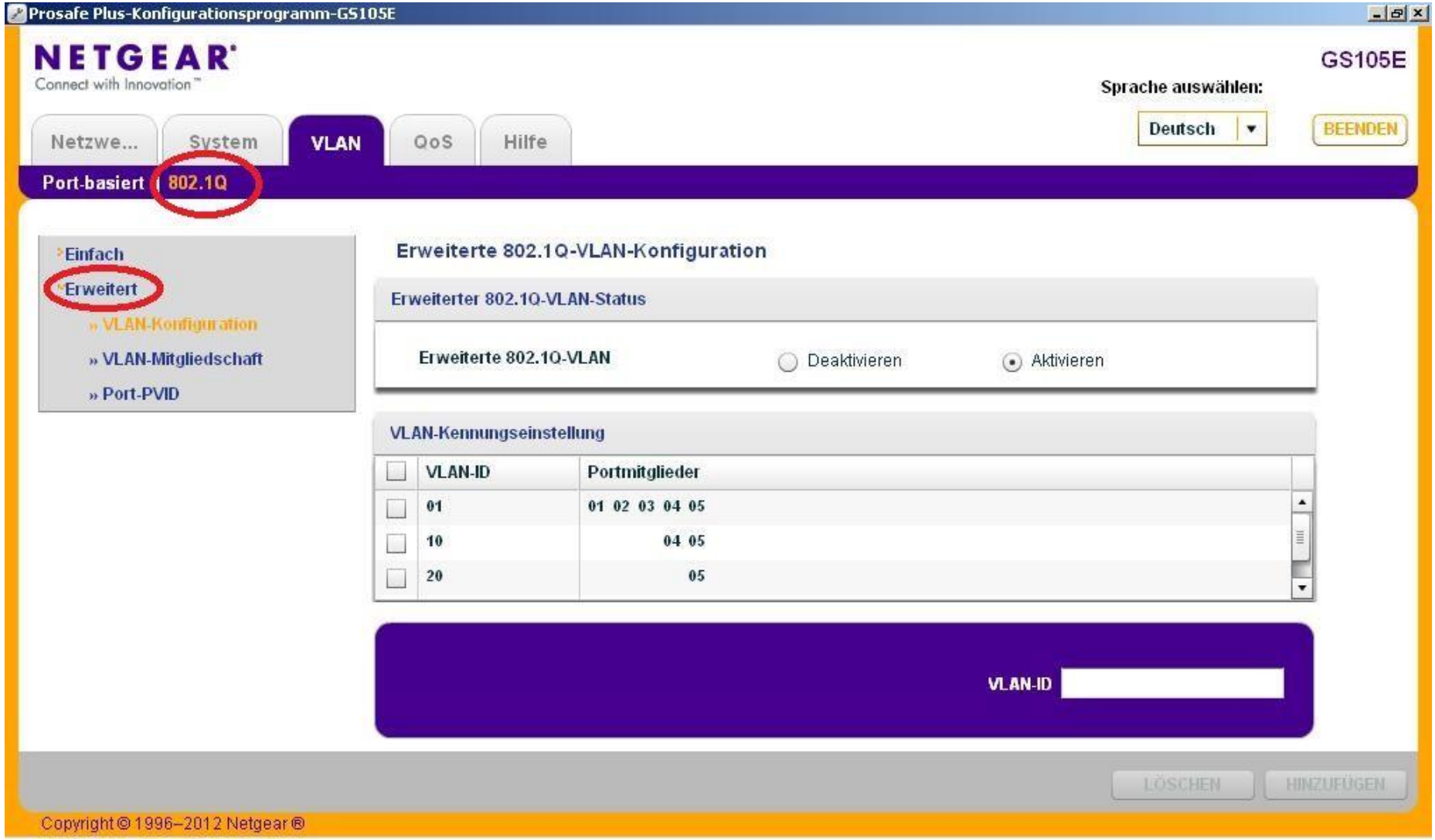
Auch hier ist die VLAN Einrichtung über das WebGUI wieder identisch:



Beispiel Konfiguration NetGear Prosafe GS10xE Serie

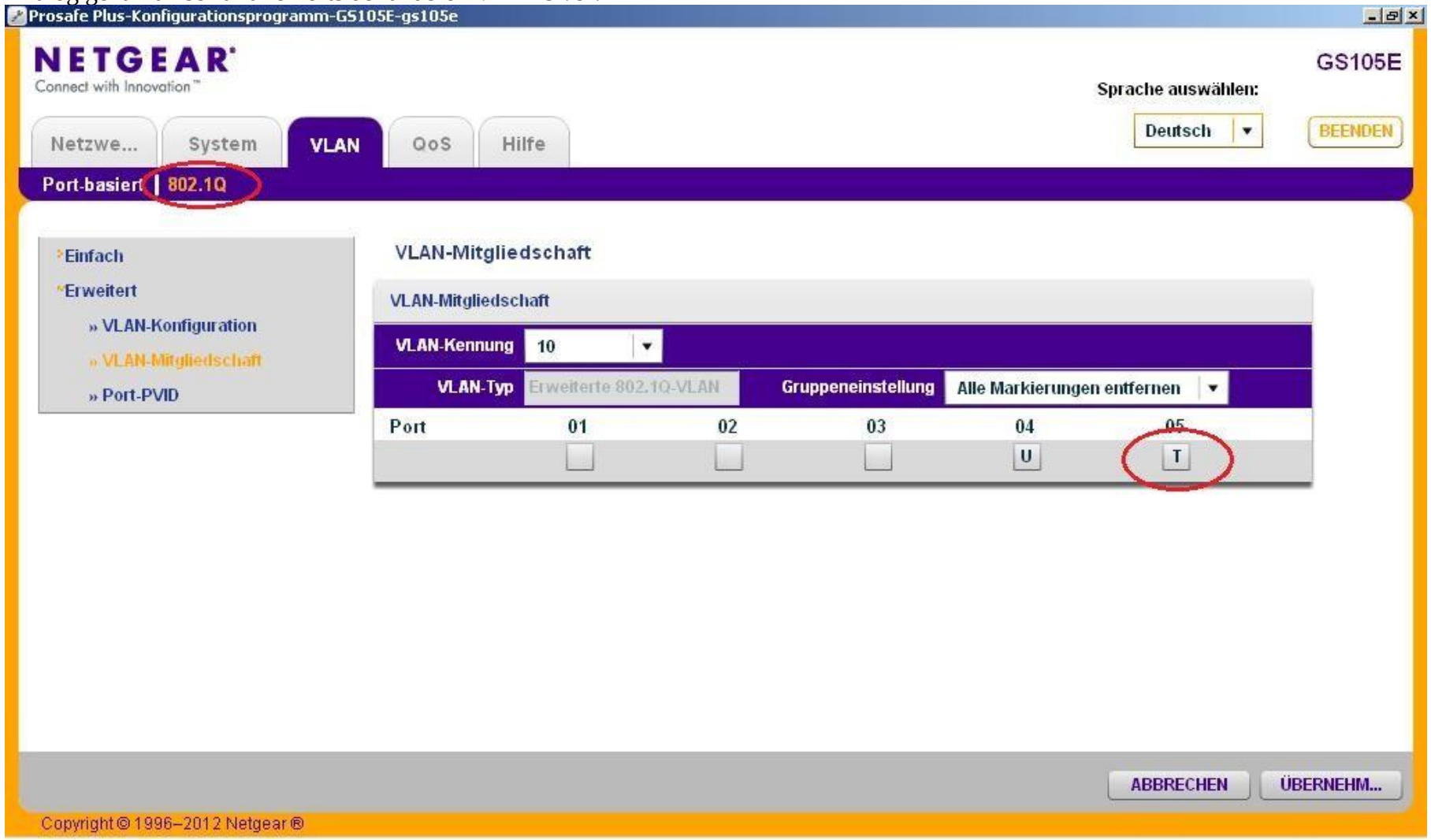
Eine Beispiel VLAN Konfig für das **GS108T** und baugleiche Modelle mit mehr Ports findet man HIER.
NetGear bietet mit dem GS105E und dem GS108E zwei konkurenzlos preiswerte VLAN Switches. Der GS105E dürfte mit 25 Euro Straßenpreis einer der günstigsten VLAN Switches neben dem TP-Link SG105E oder 108E am Markt sein.
Bei viel Freud gibt es auch wie immer einiges Leid, denn der NetGear bietet einige Fussfallen bei der VLAN Konfiguration wie es diverse Leidensthreads hier im Forum leider belegen.
Deshalb hier eine wasserdichte Anleitung wie man die etwas gewöhnungsbedürftige VLAN Konfiguration bei NetGear Switches sicher in den Griff bekommt.
Die kleinen NetGear Modelle GS105E und 108E bieten kein WebGUI das erst ab den 108Tv2 Modellen und aufwärts verfügbar ist.
(Update 04/2018: Mit aktueller Firmware ist auf den 105E und auch 108E Modellen nun ein Onboard GUI verfügbar. Dies gilt nur für die Modelle der Hardware Versionen 2 und 3 ! Für diese beiden HW Versionen (nicht v1 !) ist das ProSafe Too l *also nicht mehr erforderlich !)*
Das *ProSafe Installationstool* ist aber ähnlich zur WebGUI so das die Konfiguration bei den älteren v1 Hardware Modellen analog ähnlich wie mit dem WebGUI ist.
Hat man den Switch mit dem Tool im Netz erkannt, ist es ganz wichtig bei der VLAN Installation den Button **802.1q** und NICHT den Button "Port basiert" anzuklicken. "Port basiert" ist ein **nicht standardkonformes** NetGear Verfahren, kann also nicht mit anderen Switches kombiniert werden !
Fazit also: nur einzig "802.1q" klicken und dann "Erweitert".

Die darauf folgende Warnung das alle vorherigen VLAN Konfigs gelöscht werden kann man getrost abnicken !
1.) Der erste Schritt ist die Einrichtung der VLAN IDs (hier aus dem Tutorial Beispiel 10, 20 und 30):



2.) Der zweite Schritt ist die Zuweisung der Ports zu den VLANs. Im Beispiel Screenshot ist hier der Uplink Port (**T**agged) der Port 5 und der Endgeräteport (**U**ntagged) der Port 4 für das VLAN 10. NetGear kennzeichnet die Ports entsprechend mit "U" und "T" wenn man in den Port klickt.

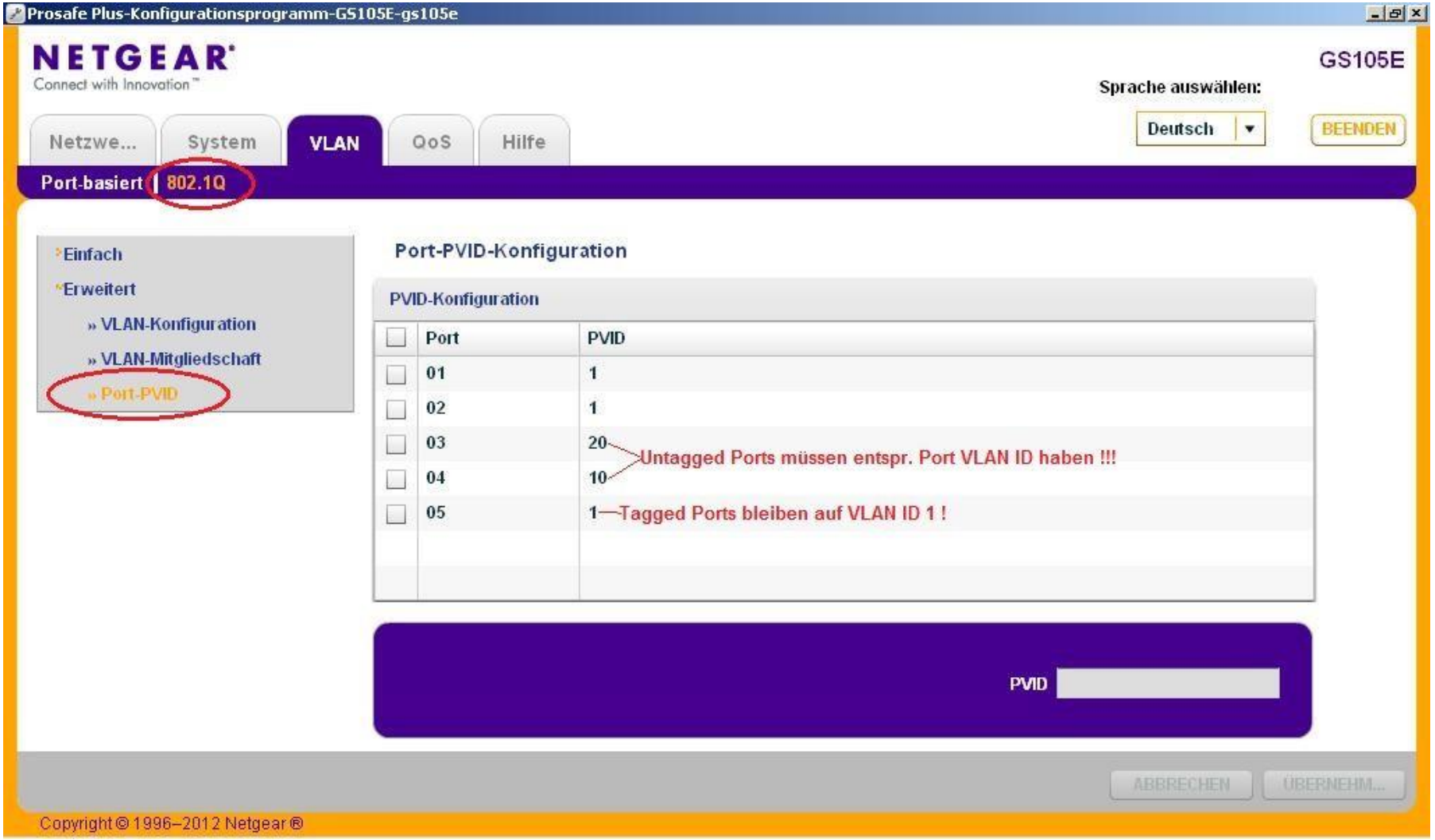
Analog geht man so für alle Ports der anderen VLANs vor:



3.) Der dritte Schritt ist eine NetGear Besonderheit (oder sollte man "Bosheit" sagen), die viel Verwirrung schafft und über die leider viele VLAN Anfänger stolpern bei NetGear Switch Hardware.

NetGear erzwingt bei untagged Ports, also Ports an dem Endgeräte wie PCs usw. angeschlossen werden, eine VLAN ID zu vergeben !
Andere Switchhersteller machen das automatisch mit der globalen VLAN Portzuweisung, nicht so NetGear. Hier gilt es also aufzupassen !
Man muss also untagged Ports **explizit** zusätzlich eine VLAN ID zuweisen, obwohl man diesen Port schon untagged in ein VLAN mit dem vorangegangenen Konfig Schritt gesetzt hat.
(Für die technisch interessierten: NetGear muss bei eingehendem untagged Traffic wissen in welches VLAN dieser Traffic geforwardet werden muss, deshalb die nochmalige dedizierte Zuweisung der zum Port gehörigen VLAN ID. Fehlt sie, landet der Traffic in VLAN 1)

Diese eigentlich überflüssige Prozedur von NetGear birgt leider gefährliches Fehlkonfigurations Potenzial !
Ist ein Port z.B. untagged in ein entsprechendes VLAN gesetzt worden, fehlt aber die dazu korrespondierende VLAN ID an dem untagged Port wird eingehender Traffic ins default VLAN 1 geforwardet. Ausgehender Traffic kommt aber aus einem anderen VLAN. Logisch das entsprechende VLAN Konfigs dann scheitern und Laien verstehen oft nicht warum. Leider ein großes "NetGear Problem".
Wichtig ist hier also zwingend darauf zu achten das entsprechende untagged Ports in den VLANs auch zusätzlich die korrekte, zu ihnen korrespondierende VLAN ID gesetzt bekommen !!!
Wenn man das Obige entsprechend aufmerksam beachtet und umsetzt funktioniert es aber fehlerlos.
Der folgende Screenshot zeigt wie es richtig und wasserdicht auszusehen hat:



Wichtig: Der Uplink Port (Tagged) bleibt hier in der Default VLAN ID 1 !! Logisch, denn eingehender Traffic der tagged ist mit einer entsprechenden VLAN ID sagt dem Switch ja schon in welches VLAN er gehört !
Die o.a. zusätzliche VLAN ID Zuweisung betrifft also außschliesslich NUR untagged Ports !

Beachtet man das alles klappt auch die NetGear VLAN Installation fehlerlos !

Beispiel Konfiguration Dell PowerConnect Switch


```
interface Ethernet 1
 description Tagged Link zur Firewall
 switchport mode trunk
 switchport trunk allowed vlan 10-40
!
interface Ethernet 10
 description Enduser Ports in VLAN 10
 switchport mode access
 switchport access vlan 10
!
interface Ethernet 11
 description Enduser Ports in VLAN 10
 switchport mode access
 switchport access vlan 10
!
interface Ethernet 12
 description Enduser Ports in VLAN 20
 switchport mode access
 switchport access vlan 20
!
interface Ethernet 13
 description Enduser Ports in VLAN 20
 switchport mode access
 switchport access vlan 20
!
interface Ethernet 14
 description Enduser Ports in VLAN 30
 switchport access vlan 30
 switchport mode access
!
```

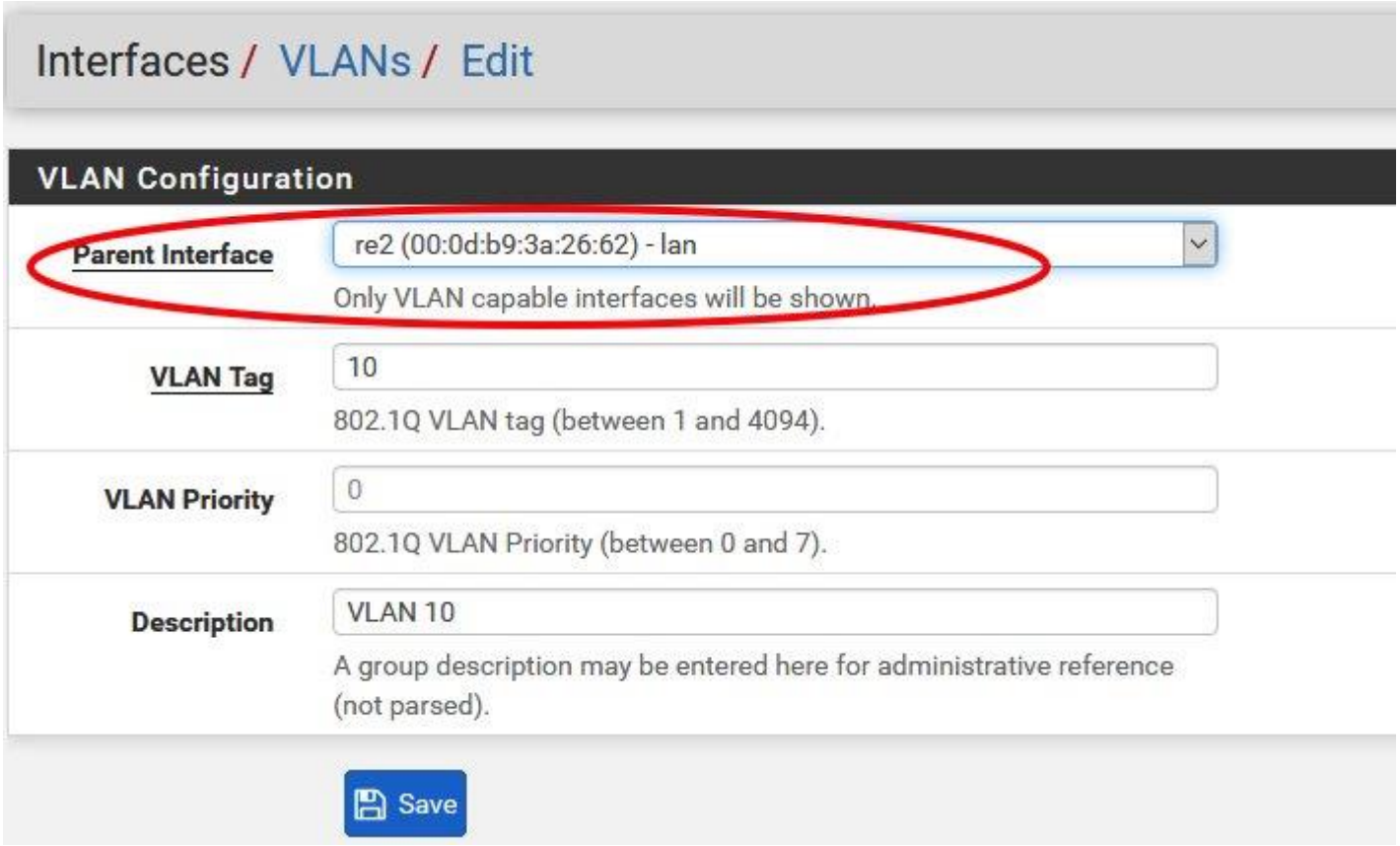
```
interface Ethernet 15
 description Enduser Ports in VLAN 30
 switchport access vlan 30
 switchport mode access
!
interface Ethernet 16
 description Enduser Ports in VLAN 40
 switchport access vlan 40
 switchport mode access
!
interface Ethernet 17
 description Enduser Ports in VLAN 40
 switchport mode access
 switchport access vlan 40
!
```

Bei Cisco und Dell sind vorher die VLANs mit dem Kommando ***vlan-database*** einzurichten ! Neuere Cisco IOS Versionen benötigen dies nicht mehr. Dort reicht z.B. ein *"vlan 10"* als Kommando.
Weitere Details zum Thema VLANs und deren Konfiguration speziell auf Cisco und HP Switches findet man auch HIER im hiesigen Forum.

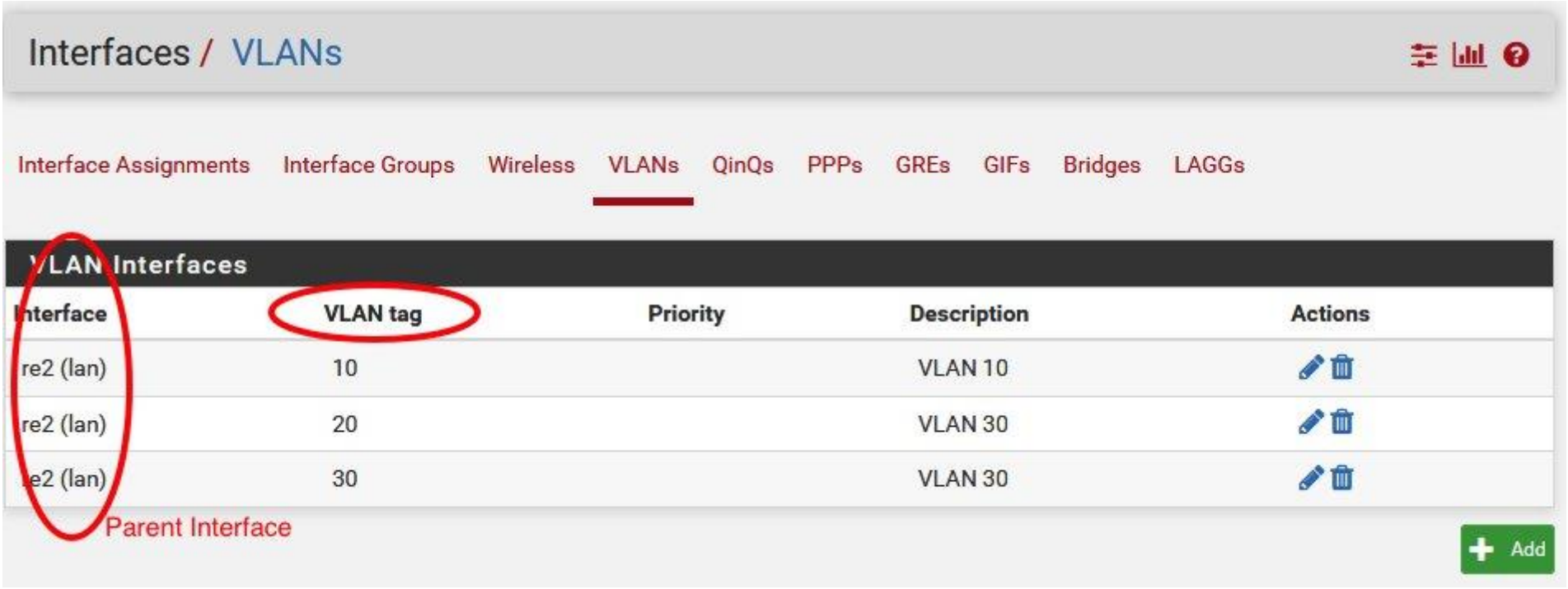
Der nächste Abschnitt beschäftigt sich nun mit der VLAN übergreifenden Kommunikation, also dem VLAN Routing !

VLAN Routing mit pfSense Firewall

In der Web Konfigurationsseite der pfSense klickt man auf *Interfaces* ***Assignments*** um zuerst die VLANs dort im Menüpunkt *VLANS* anzulegen mit einem Klick auf das **+Add** Symbol:

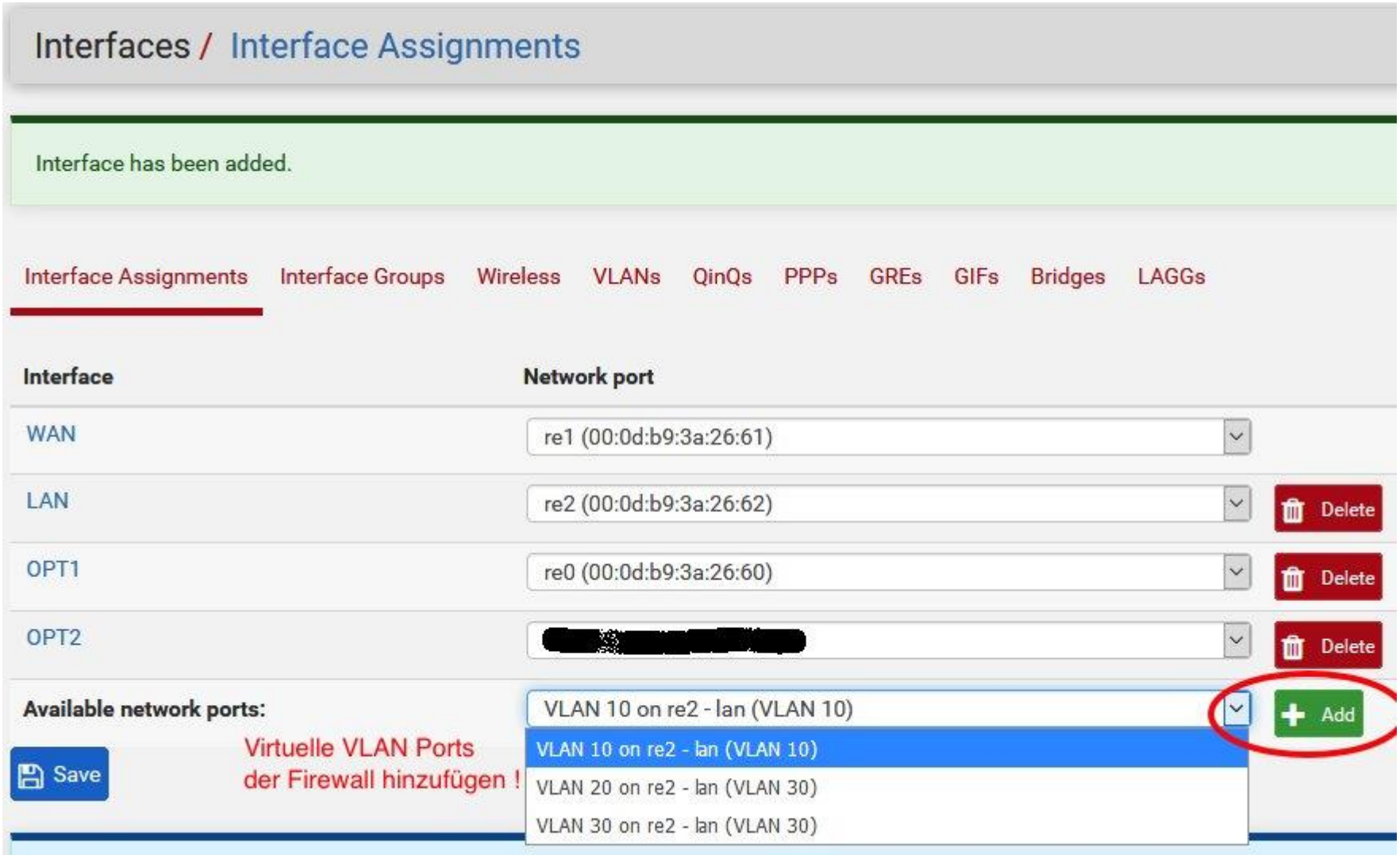


Wichtig ist hier das sog. ***Parent Interface*** !
Das ist das physische Firewall Interface über das die VLAN Pakete Tagged (also inklusive ihres VLAN Tags) auf den Netzwerk Switch in das dortige VLAN übertragen werden. (Hier im Beispiel das Interface *"re2"* was das LAN Interface ist. (APU Hardware)).
Unter **VLAN Tag** trägt man seine VLAN ID ein z.B. 10 für das VLAN 10. Unter *Description* fügt man eine Beschreibung des VLANs ein. Diese ist lediglich kosmetisch, erleichtert aber das Arbeiten später beim Mangement, da man das VLAN und dessen Funktion so leichter identifizieren kann.
Das macht man jetzt der Reihe nach für alle VLANs die man über die Firewall routen möchte:

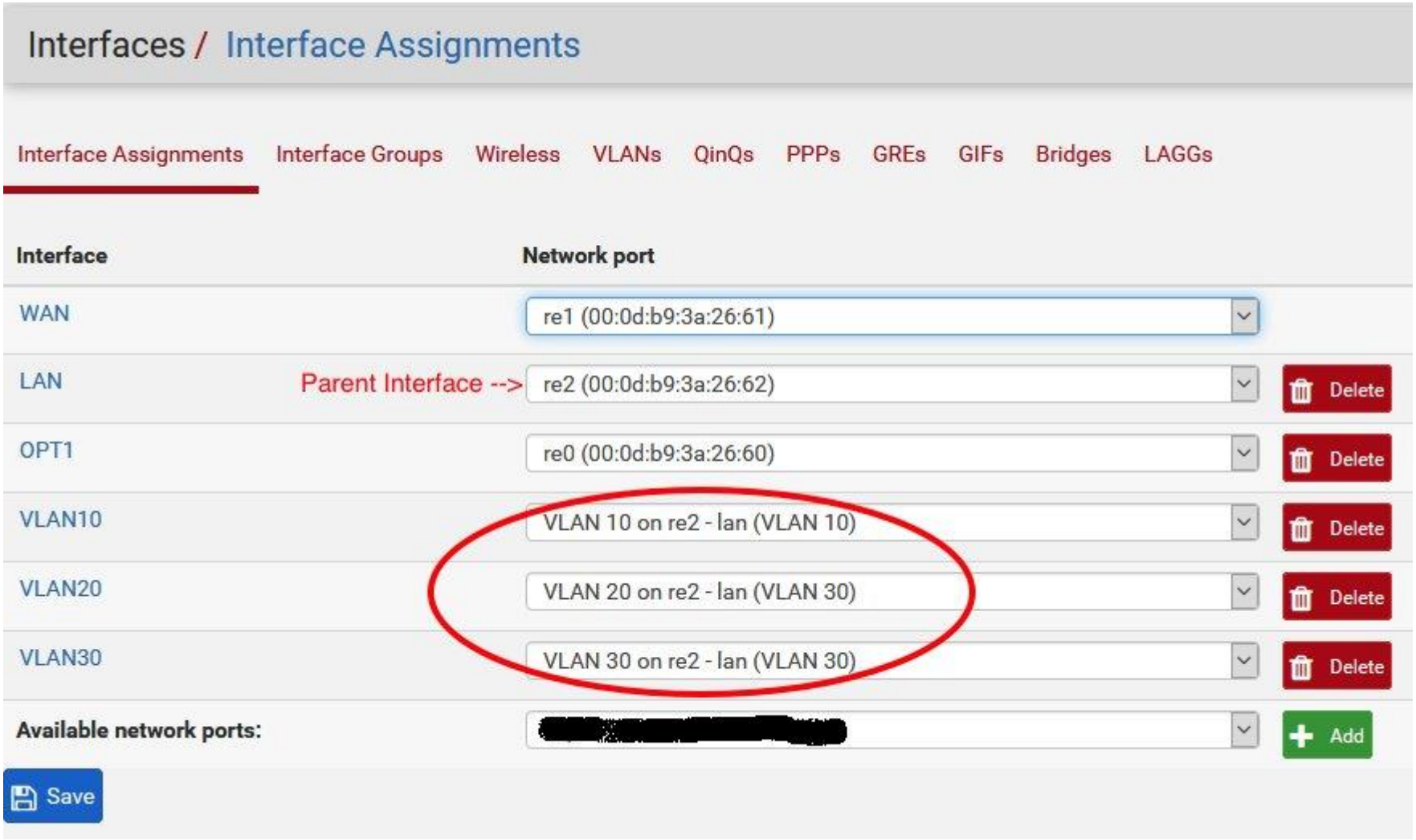


Wichtig und nicht vergessen !: Das Default VLAN 1 des Switches wird auf einem tagged Uplink Port immer untagged übertragen ! Dieses Default VLAN 1 entspricht dann dem nativen Port der Firewall (*re2* im Beispiel oben). Sprich die IP Adresse des Parent pfSense Interfaces liegt immer im VLAN 1 auf dem Switch !

Man wechselt jetzt wieder ins Menü *Interfaces* => ***Assignments*** und klickt wieder auf das **+Add** Symbol rechts unten um die virtuellen VLAN Interfaces der Firewall Interface Konfig hinzuzufügen. Danach sichert man mit *Save*.
Daraufhin erscheinen die Firewall VLAN Interfaces nun auch in der Interface Auswahl am linken Menürand als konfigurierbare Firewall IP Interfaces. Diese werden aus Konfigurastions Sicht wie physische Interfaces behandelt.

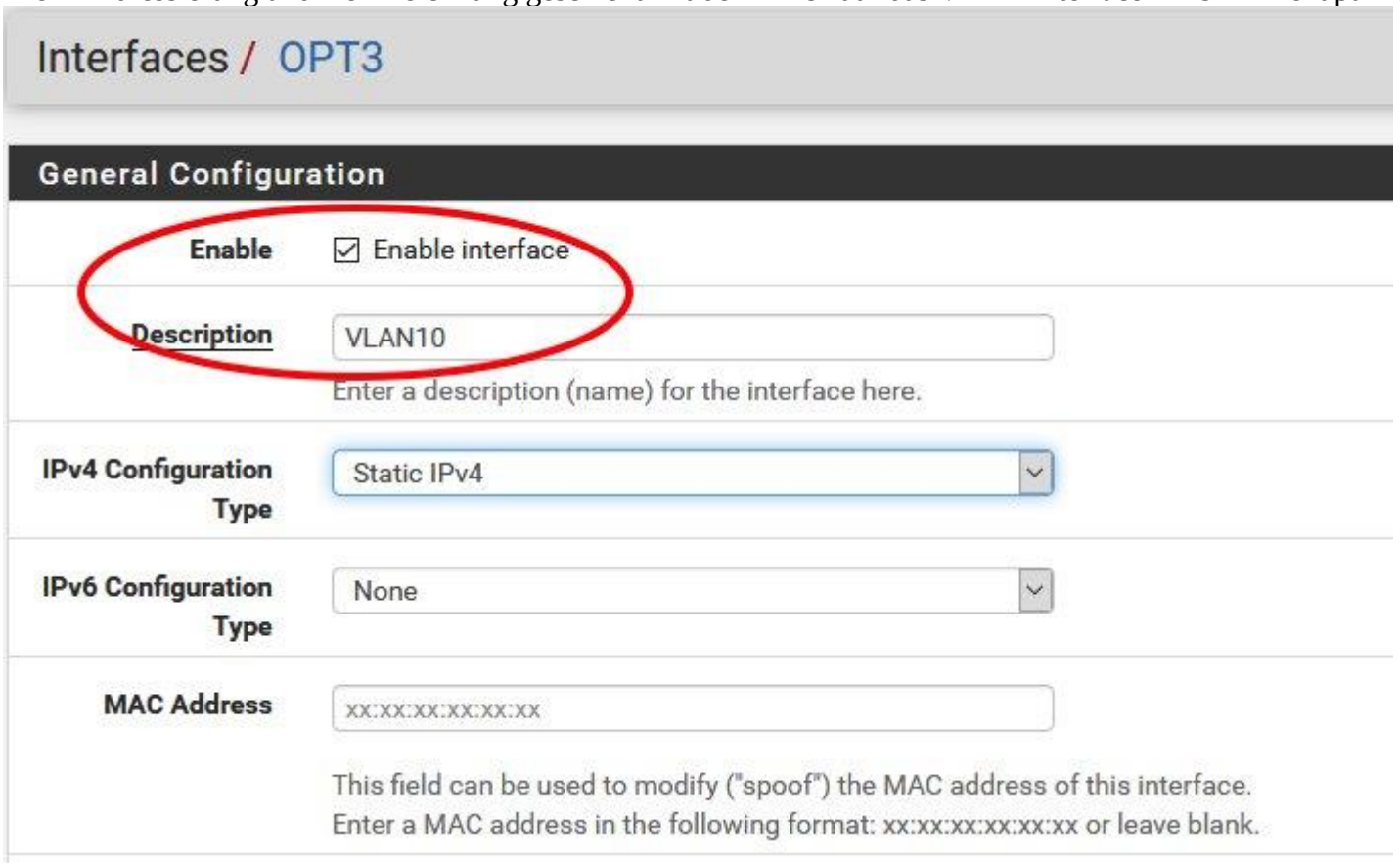


Sind alle Interfaces zugewiesen tauchen sie in der Gesamtübersicht der Interfaces entsprechend auf:

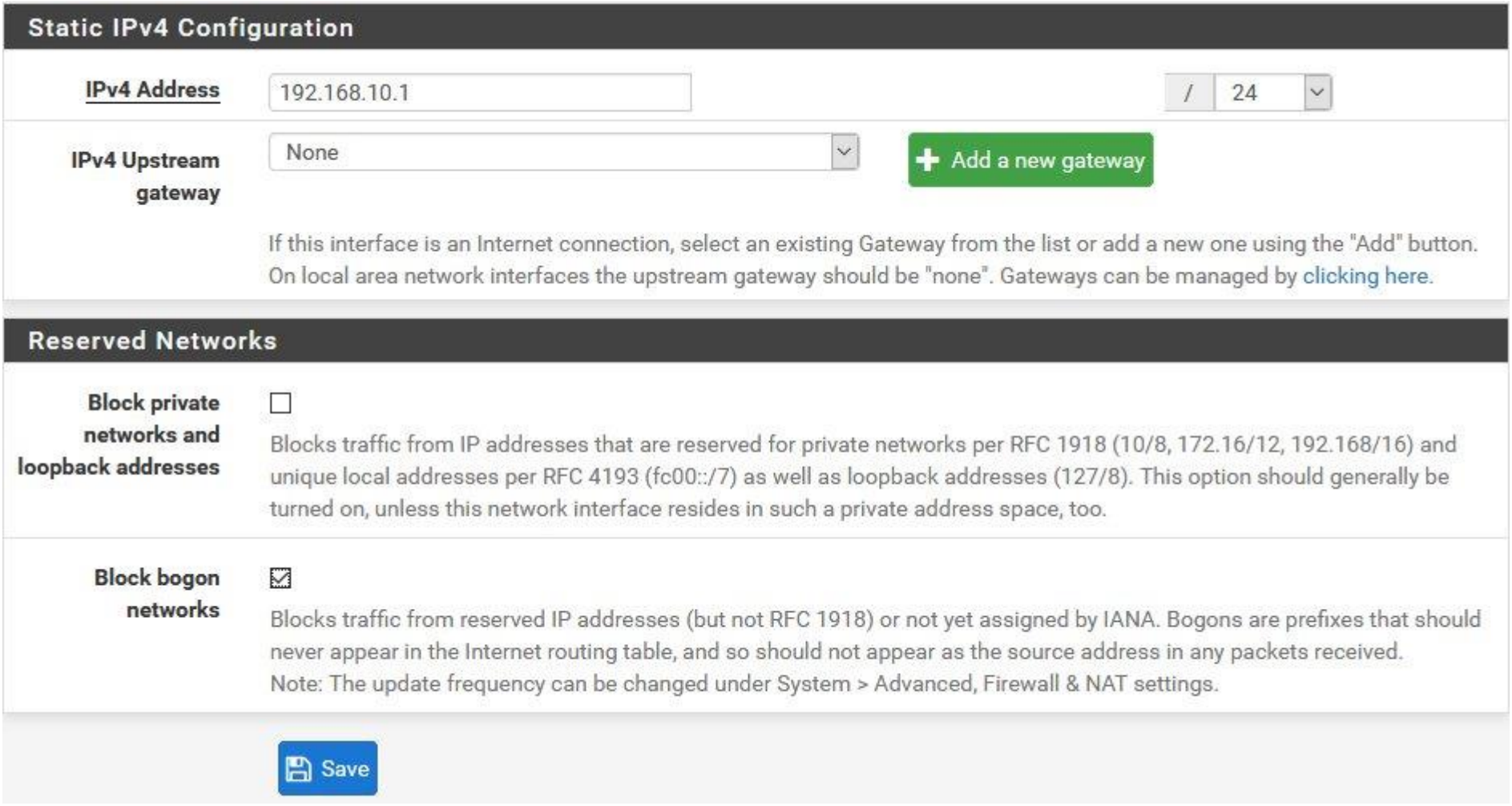


Im nächsten Schritt muss man diese VLAN Interfaces natürlich noch aktivieren (Haken "Enable") und ihnen IP Adressen zuweisen die später die Gateway IP Adressen der im VLAN angeschlossenen Endgeräte sind !
Auch entsprechende Firewall Regeln sind erforderlich da per Default alles geblockt ist wie bei Firewalls generell üblich.

Die IP Adressierung und Kennzeichnung geschieht mit dem Klick auf das VLAN Interface links im Menüpunkt *Interfaces*:



Bzw. IP Adressierung:



Über die DHCP Server Funktion der pfSense kann man dann bei Bedarf diesen VLANs noch einen DHCP Server konfigurieren.
Eingestellt und aktiviert wird der DHCP Server im Menüpunkt *"DHCP Server"* für das entsprechende VLAN Interface !

Ein weiterer wichtiger Punkt betrifft die Firewall Regeln für diese neuen Interfaces.

Es sei nochmals darauf hingewiesen das die pfSense eine **Firewall** ist und **kein** normaler Router.
Alle neu eingerichteten Interfaces sind per Default erstmal vollständig geblockt wie bei einer Firewall generell üblich !!!
Man muss also über die Firewall Regeln erst sein IP Netz, Adressen, Ports oder eine Kombination aus diesen für die Kommunikation freigeben !!!
Darin besteht ja auch der tiefere Sinn einer Firewall Netzwerk Verkehr zu regulieren !!!

Um aufkommenden Frust erst einmal kleinzuhalten kann man eine einfache *"Scheunentor"* Regel aufsetzten, die zum Testen erstmal alles erlaubt.
Das erreicht man unter *Firewall -> Rules* für das entsprechende Interface !
Hier legt man eine Regel:
PASS Source: any, Destination: any
an die dann allen Traffic erstmal durchlässt.
Ggf. muss (oder sollte) diese Regel später korrigiert werden wenn nicht jeder mit jedem kommunizieren soll (z.B. Gastnetz) oder nur bestimmte Anwendungen (Surfen, Mail, RDP) usw. erlaubt sein sollen für diese VLAN Segmente !

Die pfSsense VLAN Grundkonfiguration ist mit diesem Schritt erst einmal beendet und die Firewall mit VLAN Ports in die Switch Netzwerk Infrastruktur ist damit funktionsbereit.
Im nächsten Schritt ist jetzt der VLAN Switch wie oben beschrieben dran indem man den Anschlussport der Firewall dort als **Tagged Port** für die 3 VLANs 10 bis 30 definiert !

VLAN Routing mit Mikrotik Routern

--> ACHTUNG: VLAN Konfigurations Änderung ab Mikrotik Router OS 6.41 und neuer !!!:

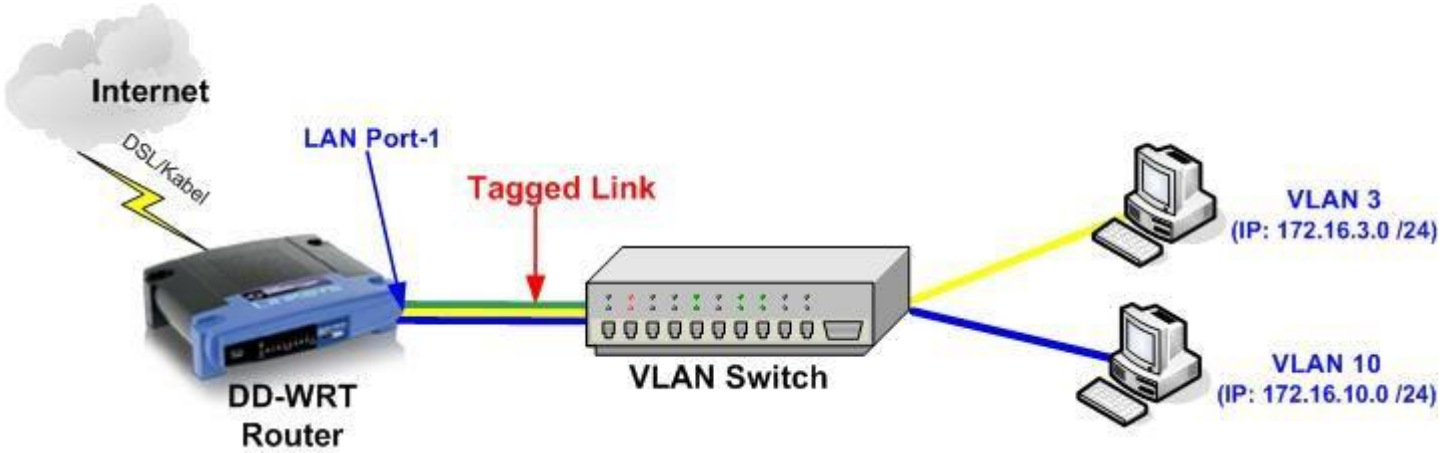
Mikrotik hat die grundlegende VLAN Konfiguration ab der Router OS Version 6.41 grundlegend verändert. Aus diesem Grund wurde der aktuellen Mikrotik VLAN Konfiguration ein_eigenes_VLAN_Tutorial gewidment !
Die folgende Anleitung wurde deshalb entfernt und es wird hier auf das neue o.a. Tutorial verwiesen !
Aktuelle Mikrotik Systeme sollten ausschliesslich nur noch mit dem aktuellen 6.41 Router OS und neuer im VLAN Umfeld betrieben werden weil die alte Konfig Syntax NICHT mehr supportet ist !

VLAN Routing ist recht einfach mit den kleinen und leistungsfähigen 5 Port Router der MikroTik_hexLite_Reihe möglich. Der Router ist hier bei Administrator.de beschrieben und ist mit ca. 35 Euro Strassenpreis (100Mbit Version) sehr preiswert und bietet eine Fülle von Features.
Die Gigabit fähige 750G3_Variante ist mit ca. 50 Euro nur geringfügig teurer und im Gigabit Umfeld vorzuziehen.
Größere Systeme wie der RB2011 oder RB3011 bieten entsprechend mehr Performance und mehr Ports sowie grafische Displays.

Der Mikrotik Router ist sehr einfach über sein Web Interface oder das mitgelieferte grafische WinBox Tool konfigurierbar.
Ein sehr einfaches Standard Routing zwischen 2 und mehr IP Netzen beschreibt ein separates Routing_Tutorial bei Administrator.de.
Die VLAN Routing Konfiguration baut darauf auf und ist ebenso mit ein paar Mausklicks über das intuitive Konfigurationstool "Winbox" zu erledigen.
Der Mikrotik hat ab Werk eine Standard *DSL Router Konfiguration* die NAT auf Port 1 macht und die Ports 2 bis 4 auf einem Switch zusammenfasst. Diese Konfiguration können wir für unser Vorhaben nicht brauchen und sie muss vorher mit dem Kommando **system reset-configuration skip-backup=yes no-default=yes** im CLI oder WebGUI gelöscht werden.
Der MikroTik ermöglich ein schnelles und auch preiswertes Routing in einer kleinen Box und ist im Preis- Leistungs Verhältnis unschlagbar, da er noch eine Fülle von Zusatzfunktionen bietet (WLAN, Dynamisches Routing, VPN Server und Client, Firewalling, Hotspot usw.)
Die Firewall Filter sind allerdings nicht so einfach und leicht zu implementieren wie bei einer pfSense_Firewall über das Websetup und erfordern ein klein wenig mehr Einarbeitung.

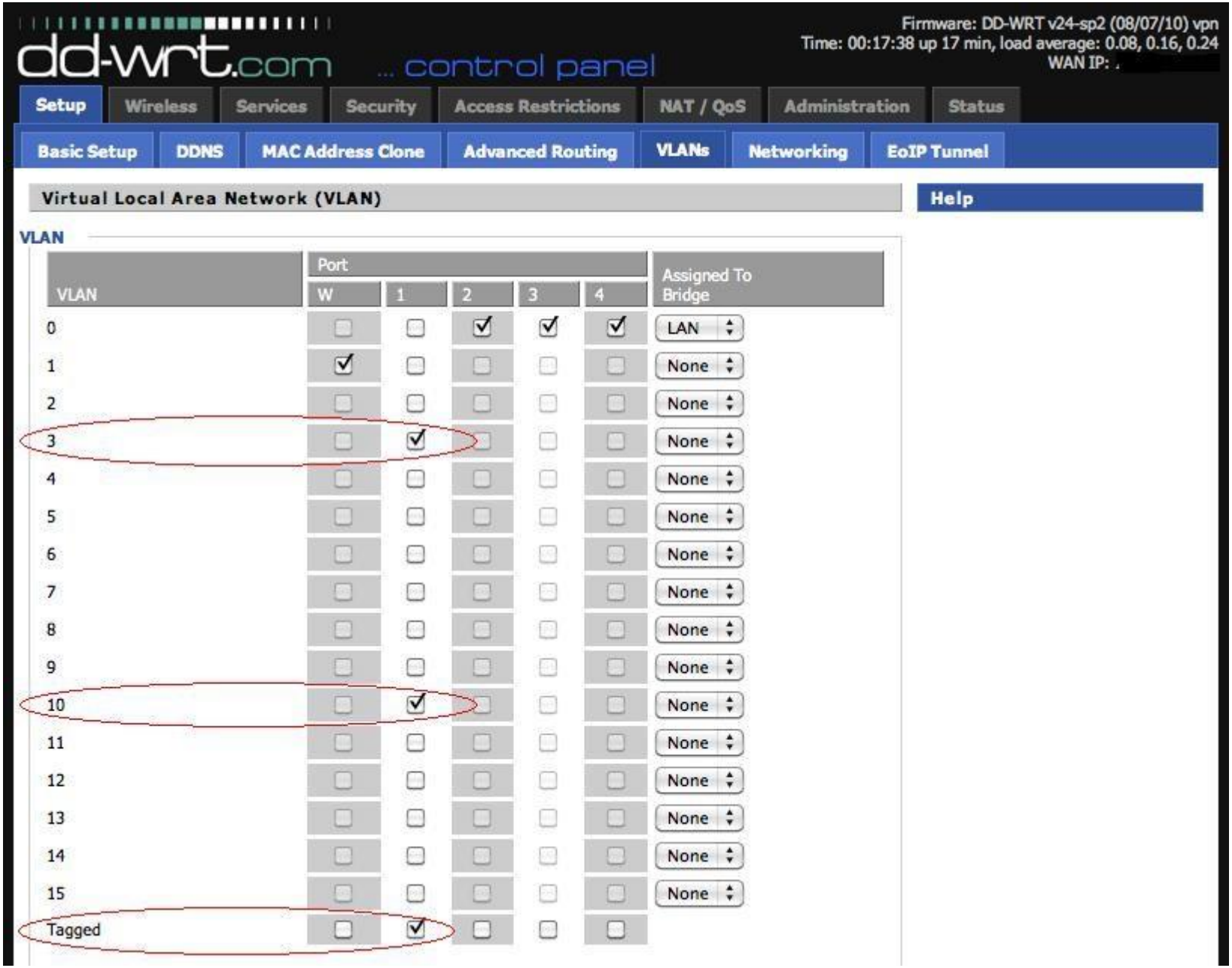
VLAN Routing mit DD-WRT Routern

Ein einfaches, schnelles und unkompliziertes VLAN Routing lässt sich mit einem Router auf Basis der sehr populären DD-WRT Firmware machen.
Die folgende Abbildung zeigt das Prinzip Diagramm eines solchen Designs: (VLAN Anzahl ist auf 2 wegen der besseren Übersichtlichkeit reduziert !)



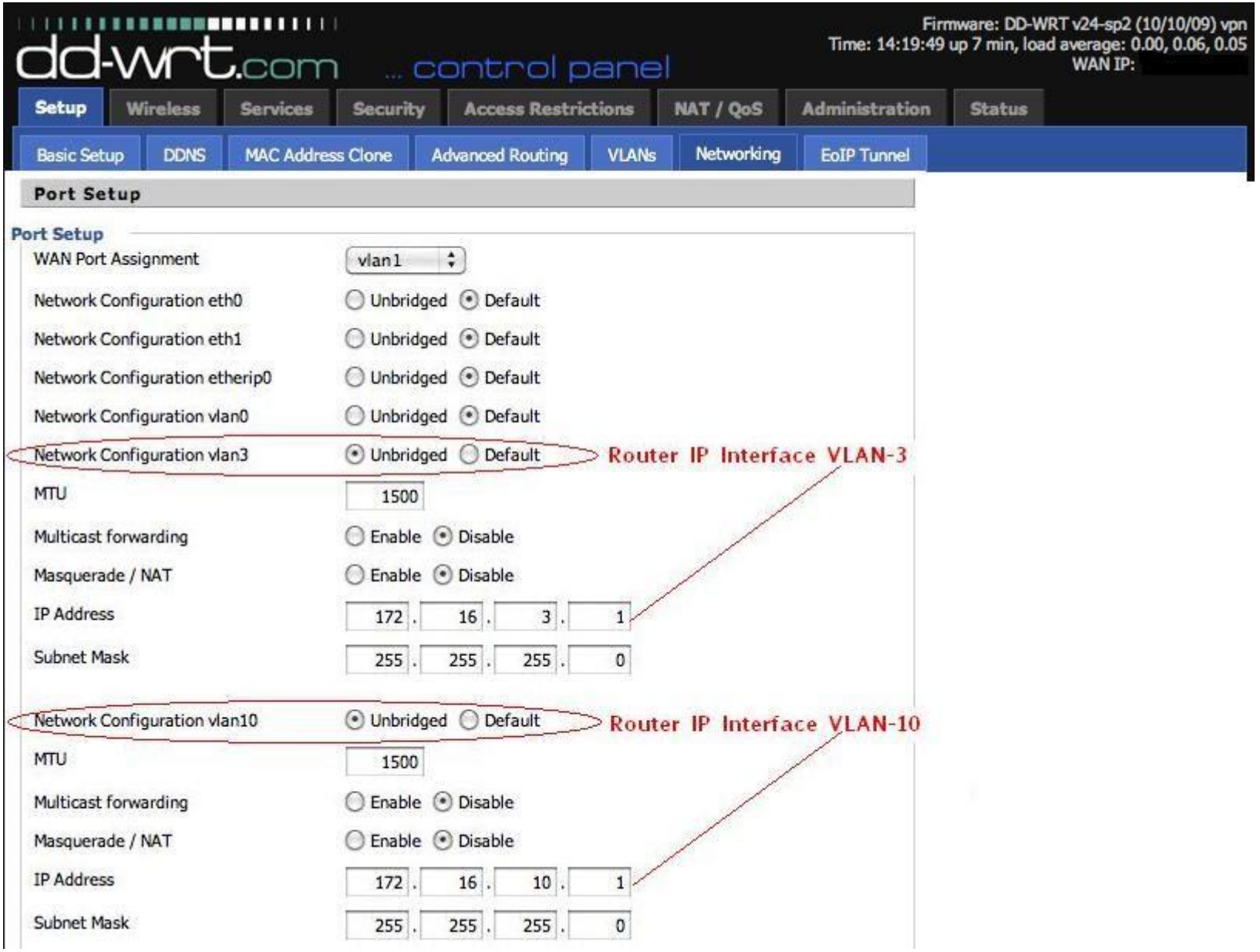
Als Trunk Port der alle VLANs vom Switch zum Router transportiert wurde am Router hier im Beispiel der **Port-1** am integrierten 4 Port Switch ausgewählt !
Die VLAN Einrichtung und die Zuweisung der Router IP Adressen pro VLAN ist mit ein paar Mausklicks im Router schnell erledigt:

Man startet dafür im Menüpunkt "Setup --> VLANs" wie die folgende Abbildung zeigt:


dd-wrt.com ... control panel
Firmware: DD-WRT v24-sp2 (08/07/10) vpn
Time: 00:17:38 up 17 min, load average: 0.08, 0.16, 0.24
WAN IP:
Setup
Wireless
Services
Security
Access Restrictions
NAT / QoS
Administration
Status
Basic Setup
DDNS
MAC Address Clone
Advanced Routing
VLANs
Networking
EoIP Tunnel
Virtual Local Area Network (VLAN)
Help
VLAN
VLAN
Port
W
1
2
3
4
Assigned To Bridge
0 LAN
1 None
2 None
3 None
4 None
5 None
6 None
7 None
8 None
9 None
10 None
11 None
12 None
13 None
14 None
15 None
Tagged

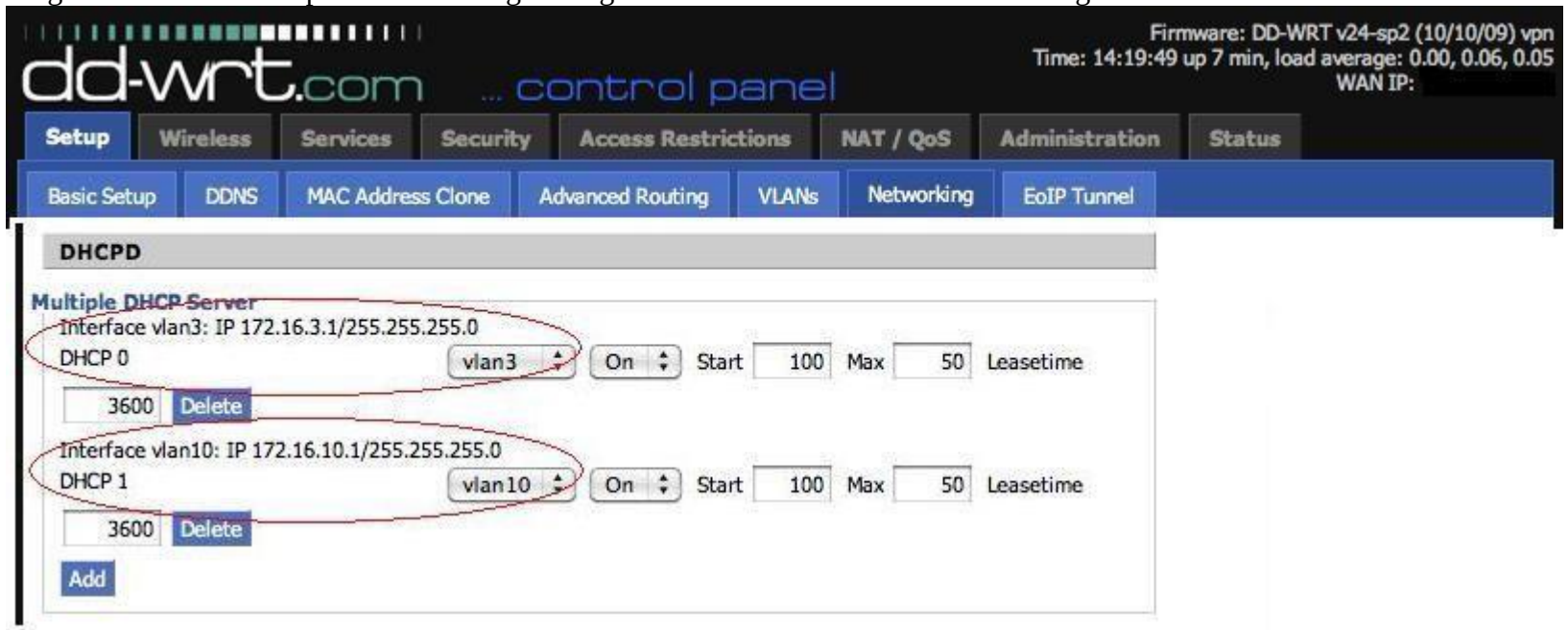
Hier erkennt man das der **Port-1** tagged konfiguriert ist für die VLANs 3 und 10. Hier wird auch der Trunk Uplink vom Switch angeschlossen !
Gleichzeitig sieht man hier im Setup auch die Einschränkung die die DD-WRT Firmware hat: Es sind nur maximal 15 VLANs erlaubt. Meist reicht das aber bei kleinen und mittleren Netzen problemlos aus, da dort nie mehr VLANs in Summe zum Einsatz kommen.
Sind die VLANs entsprechend so eingerichtet, klickt man unten auf "Apply" um die Konfiguration zuladen und dann auf "Save" um sie zu sichern !

Weiter geht es dann mit der Einrichtung der Router IP Interfaces pro VLAN im Menüpunkt "Setup --> Networking" was du untenstehende Abbildung zeigt:

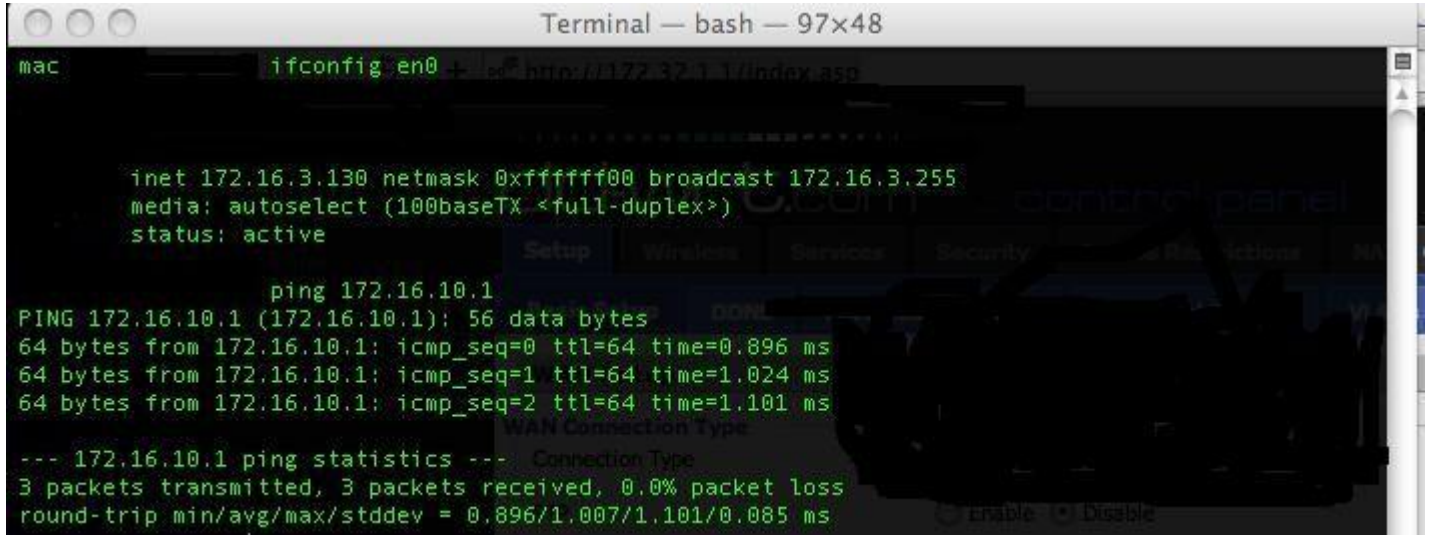

dd-wrt.com ... control panel
Firmware: DD-WRT v24-sp2 (10/10/09) vpn
Time: 14:19:49 up 7 min, load average: 0.00, 0.06, 0.05
WAN IP:
Setup
Wireless
Services
Security
Access Restrictions
NAT / QoS
Administration
Status
Basic Setup
DDNS
MAC Address Clone
Advanced Routing
VLANs
Networking
EoIP Tunnel
Port Setup
Port Setup
WAN Port Assignment
vlan1
Network Configuration eth0
Unbridged
Default
Network Configuration eth1
Unbridged
Default
Network Configuration etherip0
Unbridged
Default
Network Configuration vlan0
Unbridged
Default
Network Configuration vlan3
Unbridged
Default
Router IP Interface VLAN-3
MTU
1500
Multicast forwarding
Enable
Disable
Masquerade / NAT
Enable
Disable
IP Address
172 . 16 . 3 . 1
Subnet Mask
255 . 255 . 255 . 0
Network Configuration vlan10
Unbridged
Default
Router IP Interface VLAN-10
MTU
1500
Multicast forwarding
Enable
Disable
Masquerade / NAT
Enable
Disable
IP Address
172 . 16 . 10 . 1
Subnet Mask
255 . 255 . 255 . 0

Die Konfiguration ist fast selbsterklärend. Man kann die zur VLAN ID korrespondierenden IP Interfaces sehen die hier einfach für die beiden IP Netze 172.16.3.0 /24 in VLAN-3 und 172.16.10.0 /24 in VLAN-10 konfiguriert sind wobei die Router IP immer die **.1** im jeweiligen VLAN IP Netz ist.
Auch hier wieder auf "Apply" um die Konfiguration zuladen und dann auf "Save" um sie zu sichern nicht vergessen !

Bequemerweise bietet DD-WRT auch noch gleich separate DHCP Server für diese VLAN Netze an ! Wer also keine eigenen DHCP Server in diesen VLANs betreibt, kann dann bequemerweise DD-WRT mit der Verteilung von IP Adressen in diesen VLANs beauftragen !
Im gleichen Menü "Setup --> Networking" erfolgen die dafür erforderlichen Einstellungen:



Ab der Start IP Adresse **.100** werden so in jedem VLAN dann max. 50 IP Adressen bis zur .149 durch den Router vergeben ! Wer mehr braucht, passt das entsprechend an.
Fertig ist man mit dem VLAN Routing mit DD-WRT basierender Hardware !!
Der folgende Screenshot zeigt den Ping eines Apple Mac Rechners der sich am Switch im VLAN-3 befindet mit der per DHCP vom Router vergebenen IP Adresse 172.16.3.130. Dieser Mac (kann natürlich auch ein PC sein...) pingt erfolgreich das Router IP Interface im VLAN-10.



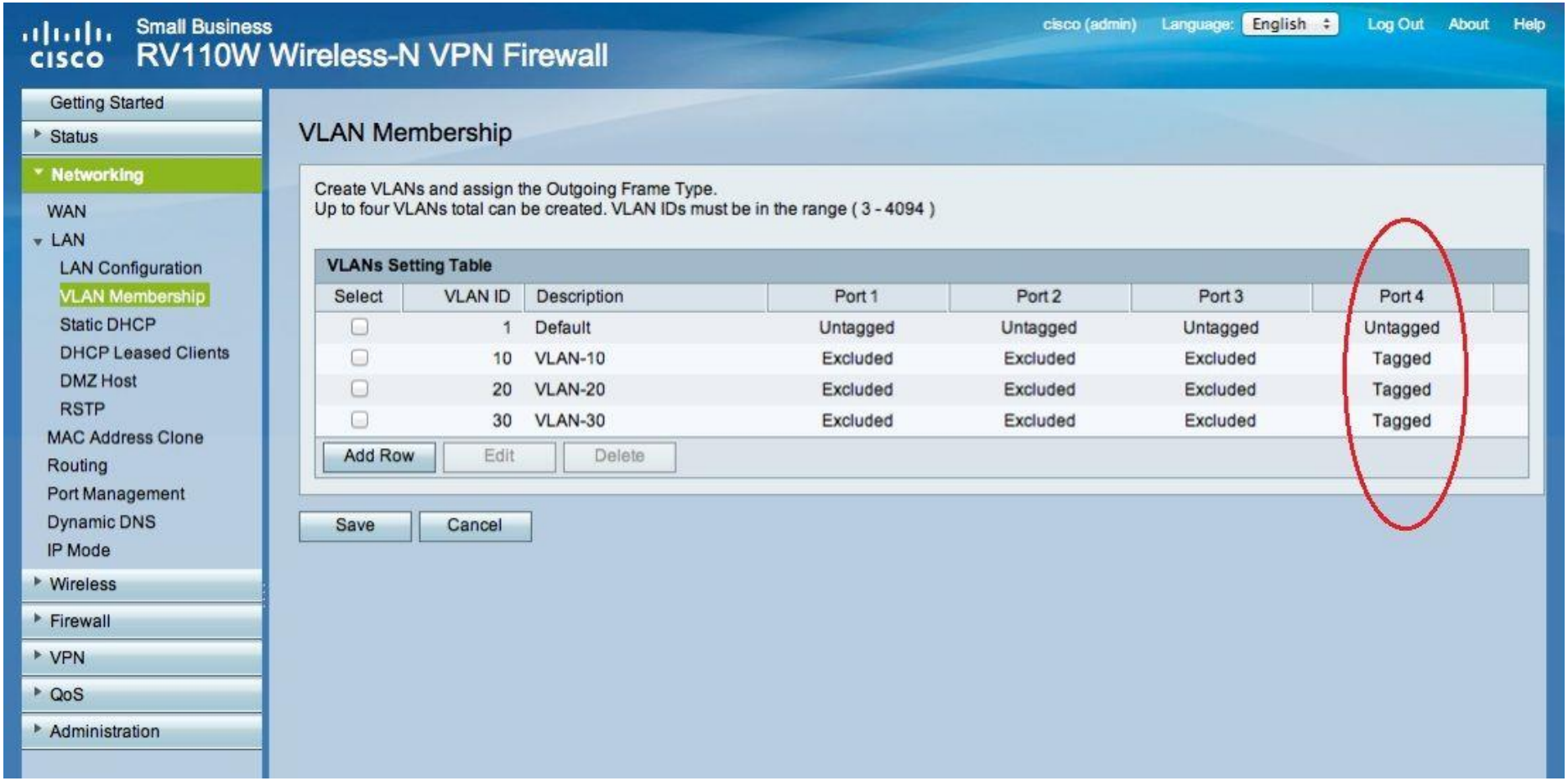
Sollen auch alle weiteren VLANs über den DD-WRT direkt ins Internet ohne einen weiteren Router im externen Netz, dann muss für diese VLAN IPs auch noch das Masquerading aktiviert werden unter Service -> "Local DNS" und "DNSmasq".
Hier dann im Feld "Additional DNSMasq Option" zusätzlich zu den bestehende Einträgen alle VLANs für die es relevant sein soll eintragen:
interface=vlan3
interface=vlan10
Je VLAN in dem auch NAT gemacht werden soll, eine Zeile!

Eine einfache, schnelle und preiswerte Möglichkeit eine Kommunikation zwischen VLANs zu realisieren wenn man auf weiteren Schnickschnack verzichten kann ! Ein zusätzlicher Thread hier beleuchtet noch einige weitere Details in der Praxis
Auf Goodies wie ein Captive Portal im Gästenetz muss man bei DD-WRT aber verzichten, da DD-WRT diese Option nicht bietet.

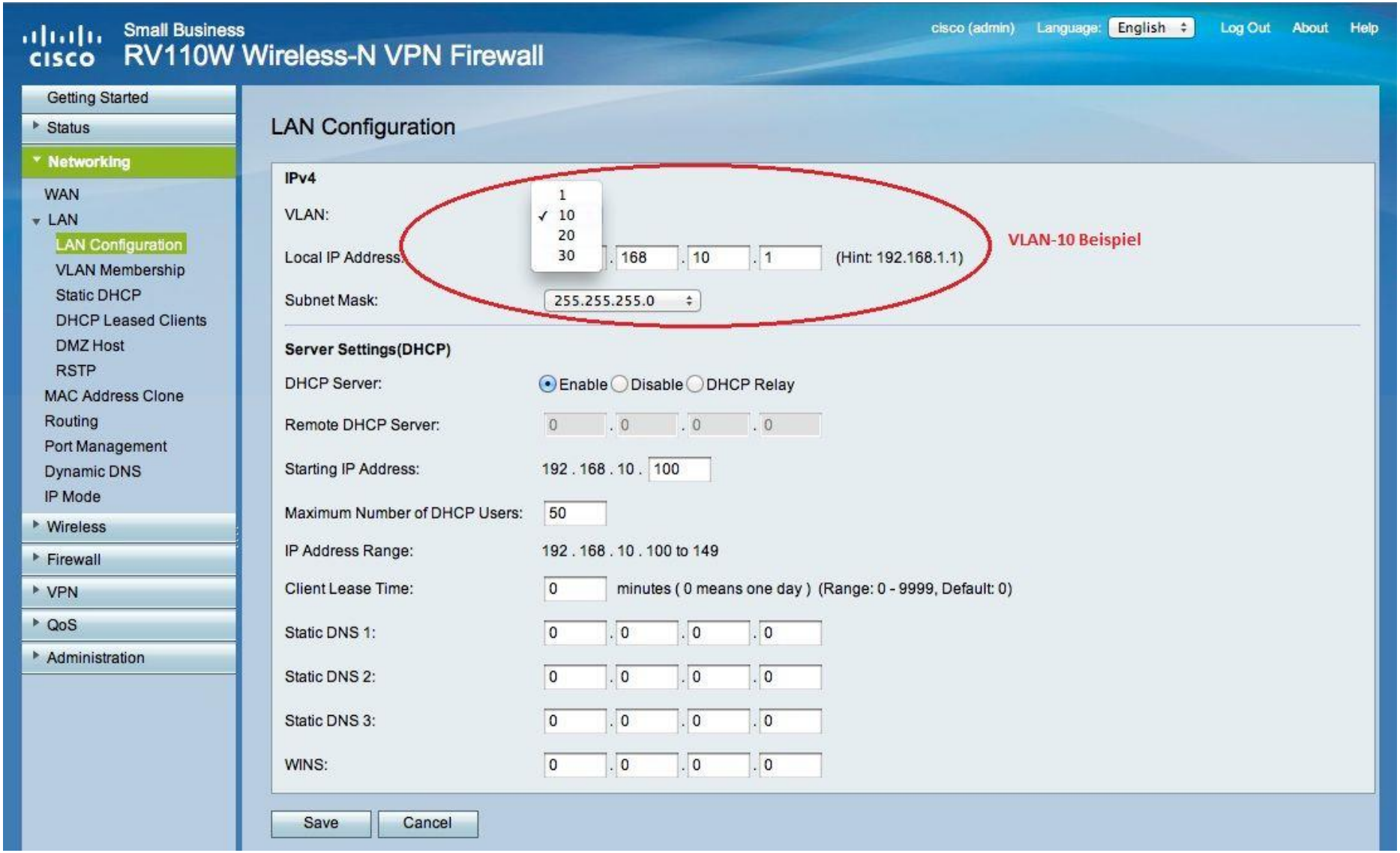
Es sei darauf hingewiesen das auch das freie Firmware Pendant **OpenWRT** analog ein solches VLAN Routing supportet !
Wie das auf einem 17 Euro Router **TP-Link WR841N** implementiert und umgesetzt wird beschreibt das Routing_Tutorial hier im Forum.

VLAN Routing mit Cisco RV110W

Wem das Flashen einer alternativen Firmware zu gefährlich ist findet aber auch kleine und preiswerte VLAN fähige Router "von der Stange". Ein Vertreter dieser Gattung ist der Cisco RV110W der zudem ein .11n fähigen WLAN Accesspoint integriert hat mit dem sich separate und sichere Gastnetze realsisieren lassen (Siehe "Praxisbeispiel" unten)
Die Konfigurationsschritte gleichen sich sehr stark denen der obigen Beispiele. Auch hier wieder die klassische Prozedur:
1.) VLANs und dazugehörige Ports einrichten (Tagged).
2.) IP Adressen und ggf. DHCP diesen VLANs zu ordnen:



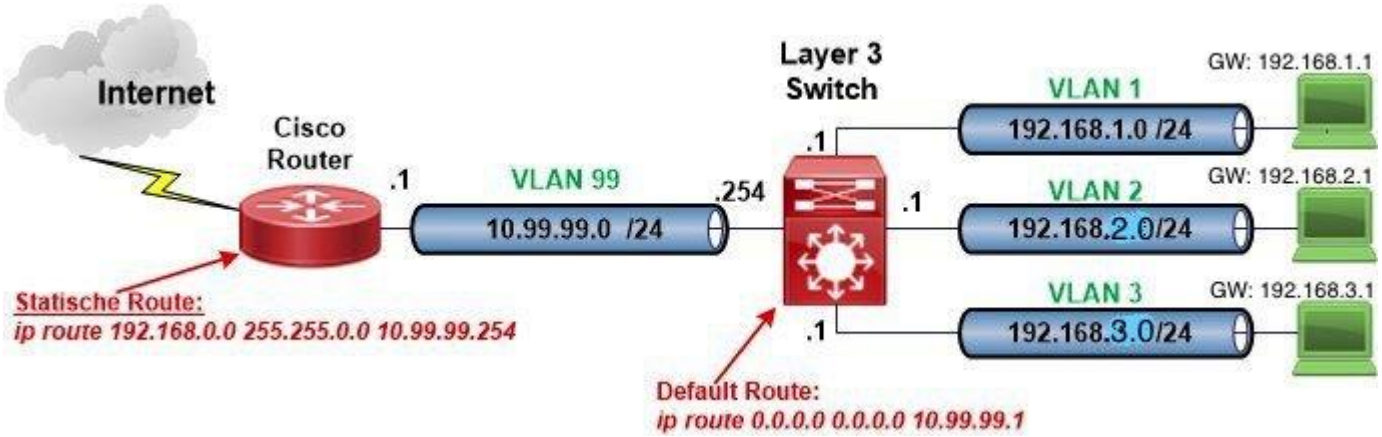
Hier die IP Adressierung und ggf. DHCP Server:



Als Beispiel ist hier der **Port 4** der tagged Uplink Port auf den VLAN Switch !

VLAN Routing mit Layer 3 Switch ohne externen Router:

In größeren VLAN Umbegungen ist es oft nicht mehr skalierbar und auch performant mit einem externen, per 802.1q Tagged Link angebundenen Router zu arbeiten wie es in den obigen Beispielen beschrieben wurde.
Hier macht es dann vielmehr Sinn einen Layer 3 Switch zu verwenden, also einen Switch der gleichzeitig einen integrierten Router hat und so zwischen den VLANs routen kann.
Damit kann man direkt auf der Backplane des Switches routen und muss so nicht die VLANs über einen externen Link an einen externen Router transportieren.
In Netzen ab einer bestimmter Größe ist das der Standard. Meist hat man für die Hochverfügbarkeit dann 2 redundante Core Switches in solchen Netzen die mit VRRP oder HSRP eine Gateway Redundanz emulieren oder in neueren Designs mit Full Stacking fähigen Switches einen Stack im Core bilden.
Die Internet Anbindung wird dann immer über ein Transfer- oder separates VLAN realisiert um diesen Traffic von Produktiv VLANs fernzuhalten, was auch der Sicherheit der internen VLAN Segmente entgegen kommt.
Ein klassisches Design aus Layer 3 Routing Sicht sähe dann so aus:



Ein Anwendungsbeispiel aus der Praxis

Die Anwendungen von VLANs in Netzwerken sind zahllos ! Immer aber sind sie eine sinnvolle Segmentierung von Netzwerken zur Performancesteigerung und zur Erhöhung der Zugriffssicherheit !
Jeder verantwortungsbewusste Netzwerk Admin segmentiert deshalb heutzutage sein Netzwerk in der einen oder anderen Art mit VLANs um Performance- und Sicherheits Standards hoch zu halten und damit eine optimierte LAN bzw. WLAN Infrastruktur zu betreiben.
Ein klassisches Beispiel ist das heute übliche Voice- bzw. Telefonie VLAN um VoIP Traffic in Unternehmen vertraulich und übertragungssicher (Quality of Service) vom allgemeinen Netzwerk abzutrennen. Auch aus rechtlicher Sicht ist das in nicht privaten Netzen ein Muß.

Als klassisches Anwendungsbeispiel dient hier ein sehr typisches WLAN / LAN Design in einem Firmennetzwerk und zwar die sichere Installation einer Firmen WLAN Infrastruktur mit 3 verschiedenen und getrennten WLANs unterschiedlicher Security über eine gemeinsame Hardware.
Das beinhaltet ein offenes Gäste- und Besucher WLAN mit einem professionellen Captive_Portal_Hotspot zum Login und Ticketverteilung, einem verschlüsselten Firmen WLAN und einem unsichtbaren und verschlüsselten WLAN für den Netzwerkadmin zum bequemen, drahtlosen Administrieren seiner Netzwerkkomponenten und Server auf dem Firmen Campus.

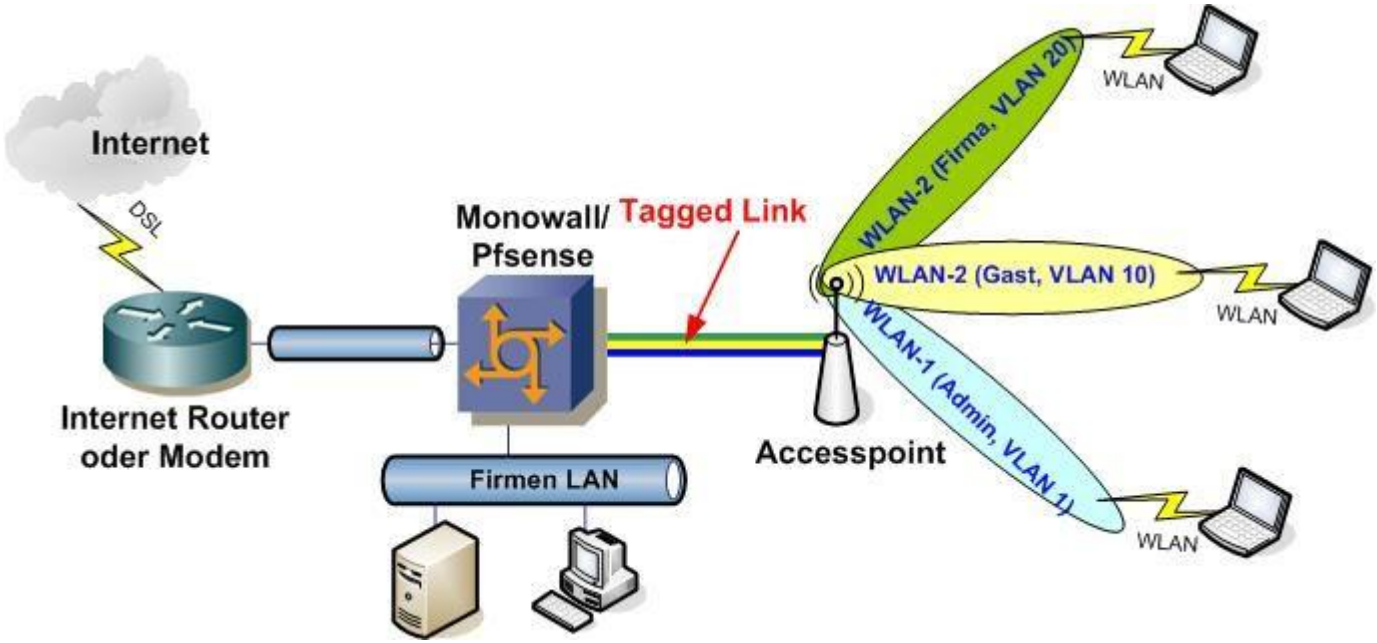
All dies realisiert man einfach über VLAN fähige WLAN Accesspoints mit MSSIDs (ESSIDs) sowie VLAN Switches.
Dies sind heutige, aktuelle WLAN Accesspoints die mit einem einzigen physischen Accesspoint mehrere SSIDs (WLANs) gleichzeitig aufspannen können und diese WLANs bzw. ihre SSIDs (WLAN Kennungen) dann entsprechend VLAN Nummern (IDs) zuordnen können.
Siehe dazu auch hier:
http://www.dummies.com/programming/networking/cisco/multiple-ssids-with ...
Z.B. Traffic aus dem WLAN mit der SSID *"Firma-intern"* geht ins VLAN 10 und Traffic aus dem WLAN mit der SSID *"Besuchernetz"* geht ins VLAN 20 usw.
Ein klassischer Vertreter dieser Art ist z.B. der Linksys WAP-200 wie er HIER in einem Bericht bei Administrator.de getestet wurde.
Auch im preiswerten Consumer Segment supporten mehr und mehr WLAN Accesspoints multiple ESSIDs mit einem VLAN Mapping wie z.B. der **Cisco RV110W** (http://www.cisco.com/en/US/products/ps11762/index.html) erhältlich z.B. hier
Oder der **Edimax EW-7416**: (http://www.edimax-de.eu/de/produce_detail.php?pl1_id=1&pl2_id=5& ...)
den man z.B. hier oder im lokalen Handel preisgünstig erwerben kann.
Ein weiterer preiswerter und leistungsstarker Vertreter dieser Zunft ist der Mikrotik_cAP_lite
Accesspoint Modelle aller bekannter Hersteller wie Lancom, Mikrotik (siehe oben), Ubiquity, Cisco, TP-Link u.a. supporten dieses VLAN zu SSID Feature (MSSID) bei diversen Modellen in ihrem Portfolio ebenso.
Ein genauer Blick ins Datenblatt **VOR** dem Kauf eines WLAN Accesspoints ist also immer ratsam, da dieses sinnvolle Feature (MSSID Support oder Multiple WLANs) kaum Mehrkosten verursacht, im Betrieb aber erhebliche Vorteile bietet wie dieses Praxisbeispiel zeigt !

Das Praxis Tutorial verwendet deshalb hier stellvertretend 2 Beispiele im high und lowcost Bereich:
a.) Mit einen Cisco Accesspoint für die gehobenen Ansprüche oder gebraucht bei eBay.
b.) Mit einem kleinen und preiswerten .11n fähigen Consumer AP Edimax_EW7416 (andere ESSID fähige APs funktionieren ebenso)

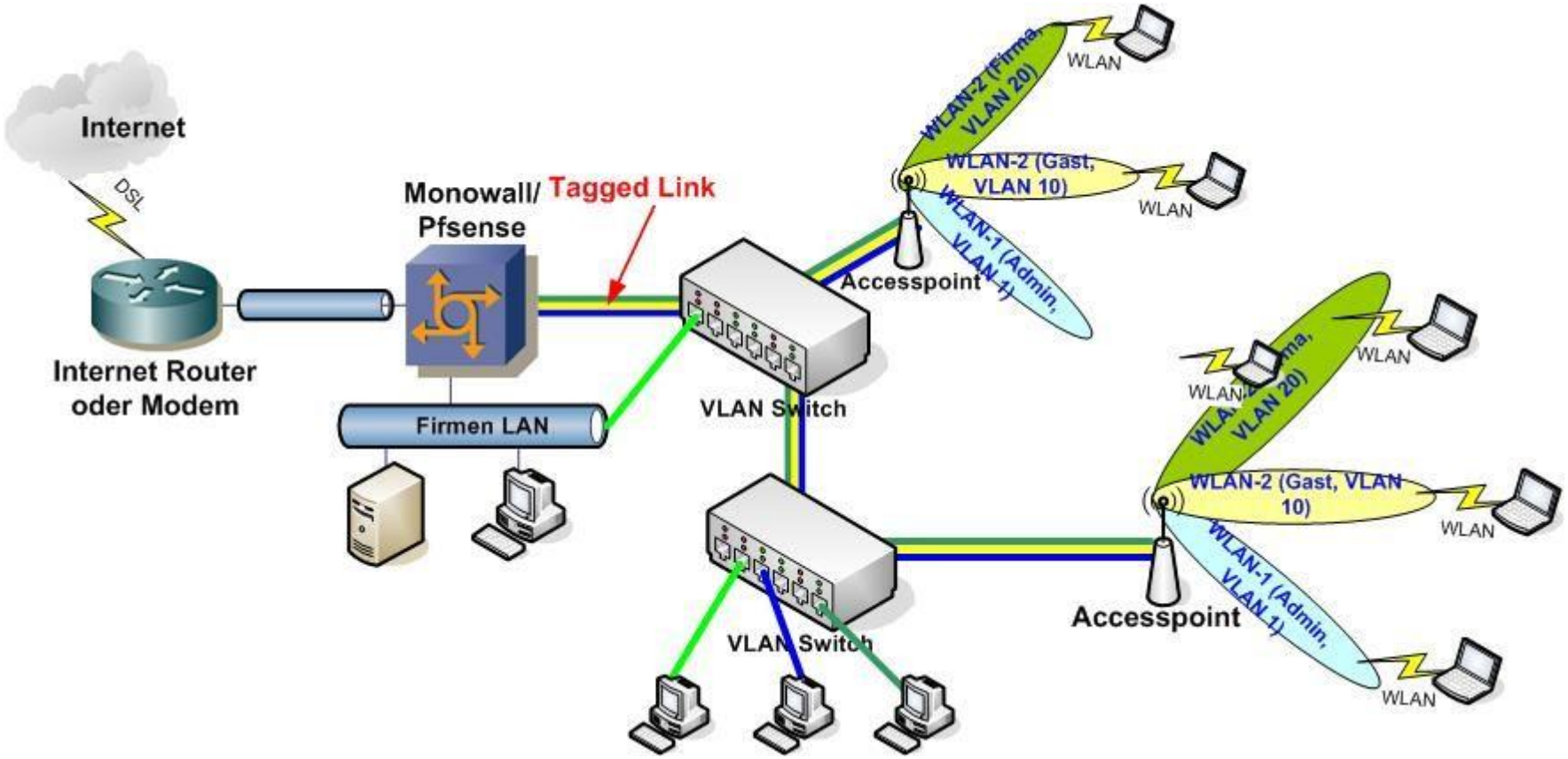
Die Schritte zur VLAN Einrichtung sind die gleichen wie oben bereits im VLAN Tutorial beschrieben:

- pfSense als Captive Portal mit VLANs einrichten, korrekte VLAN IDs vergeben und ggf. DHCP auf den VLAN Interfaces aktivieren. VLAN Port entweder direkt auf den AP stecken oder wenn schone eine VLAN Infrastruktur vorhanden auf den VLAN Switch verbinden wie oben beschrieben und nur die APs in die zu ihnen gehörenden VLANs stecken.
- Für das Gast WLAN die Captive Portal Funktion aktivieren und anpassen wie HIER beschrieben. Ggf. Filterreglen setzen um den Gästen nicht alles zu erlauben (P2P filtern etc.)
- Ggf. eine sichere User Authentifizierung fürs Firmen WLAN aufsetzen wie HIER beschrieben. Die zentrale Radius Authentifizierung lässt sich auch für das Captive Portal und die Gäste nutzen wer es möchte. Ansonsten einfach WPA-2 und pre-shared Passwörter verwenden.
- Damit wären schon alle Installationsarbeiten abgeschlossen !

Schematisch sähe so ein Netzwerk so aus:

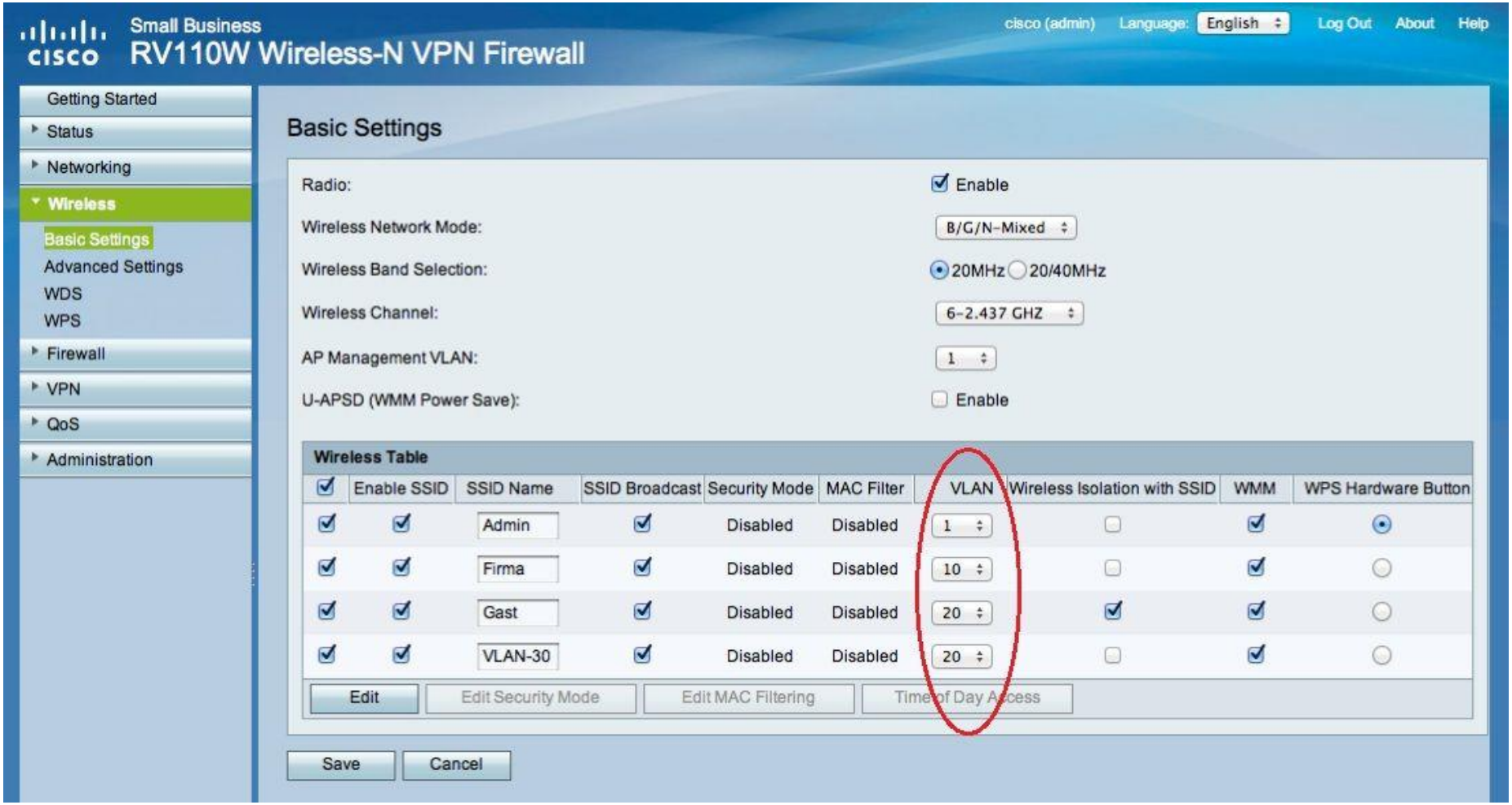


bzw. analog bei vorhandener VLAN Switch Infrastruktur



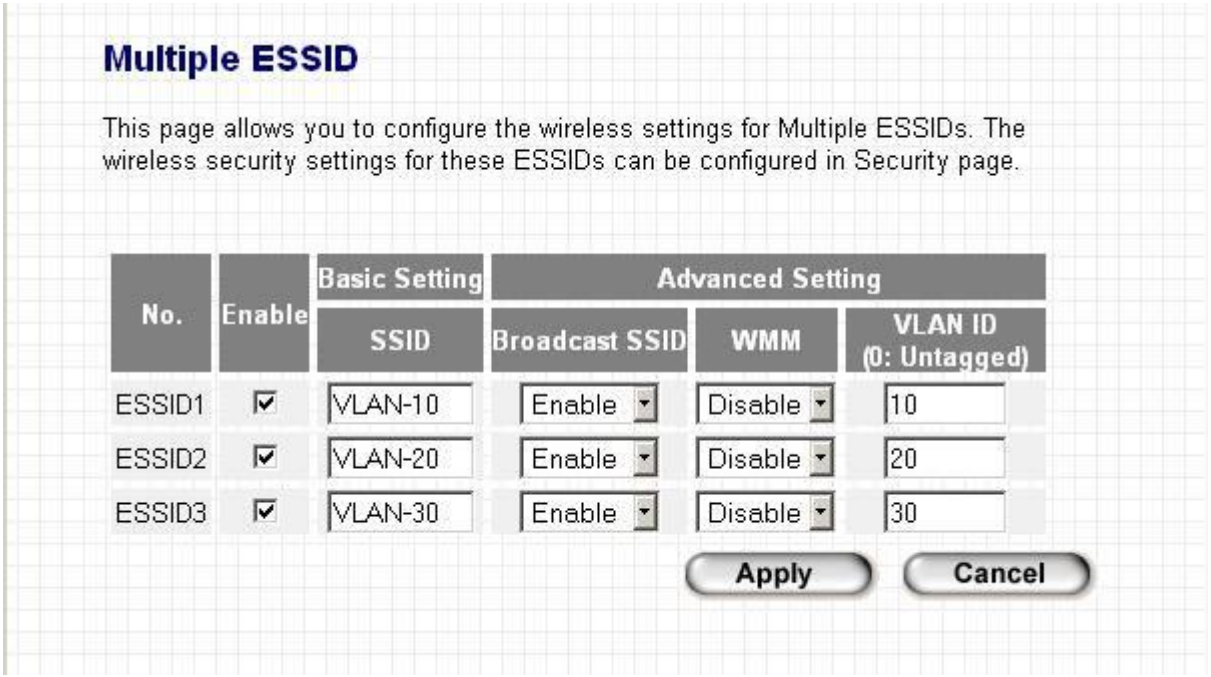
Beispiel WLAN Accesspoint Konfiguration:

Für den oben beschriebenen Accesspoint/Router **Cisco RV110W** ist die Konfiguration einfach und mit ein paar Mausklicks erledigt indem man die ESSIDs definiert und sie den eingerichteten VLAN IDs zuordnet.

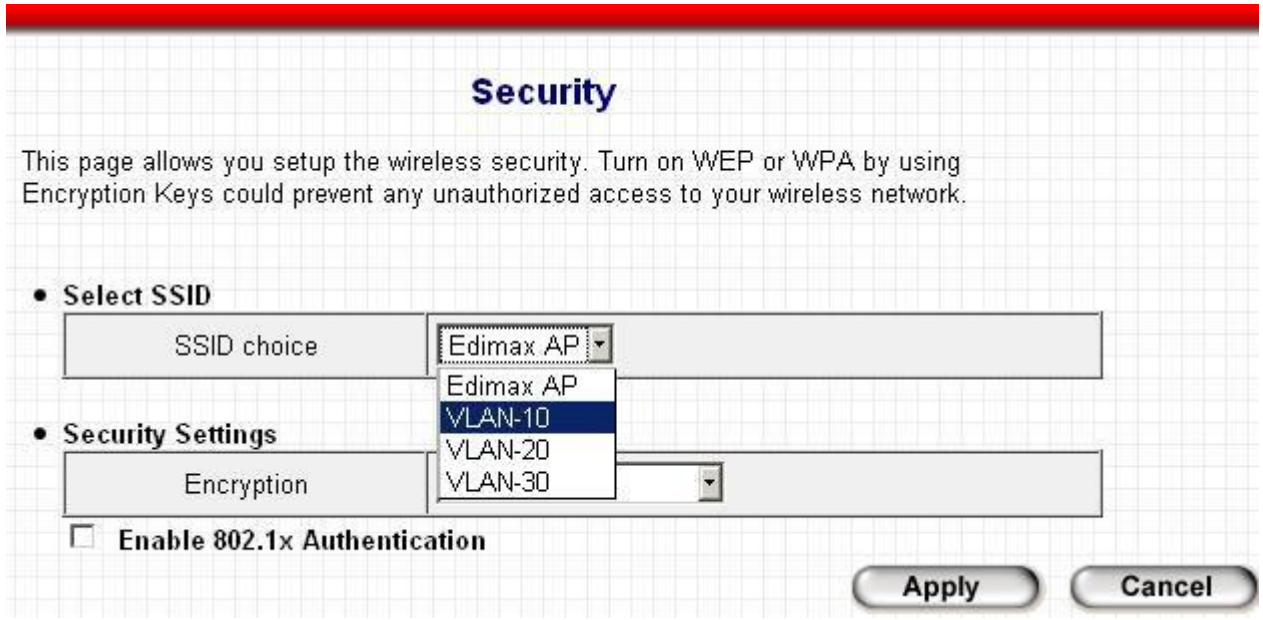


Der Cisco beitet zudem noch die Option den Zugriff auf das WLAN Gastnetz zeitlich zu limitieren. (Gilt für alle SSIDs)

Ebenso die identische Konfiguration mit dem preiswerten Edimax AP über sein WebGUI. Man definiert auch hier einfach die ESSIDs und die dazugehörigen VLAN Nummern (Tags):



Im Security Setup wird dann einfach für jede SSID noch die Verschlüsselung gesetzt. Das Gastnetz mit dem Captive Portal bleibt dabei unverschhlüsselt und offen, da die Authentifizierung ja über das Hotspot Portal auf der angeschlossenen Monowall oder pfSense gemacht wird.



Eine passende Plug and Play Konfig für den Cisco High End Accesspoint der Aironet Serie sähe so aus:
Quelltext | Drucken

service tim

```
01.
service timestamps log datetime localtime
02.
!
03.
hostname Cisco_AP
04.
!
05.
clock timezone MET 1
06.
clock summer-time MEST recurring last Sun Mar 2:00 last Sun Oct 3:00
```

```
!
dot11 syslog
!
dot11 ssid Mitarbeiter
   vlan 20
   authentication open
   authentication key-management wpa
   mbssid guest-mode
   wpa-psk ascii Geheim123
!
dot11 ssid Gast-WLAN
   vlan 10
   authentication open
   mbssid guest-mode
!
dot11 ssid IT-Admin
   vlan 1
   authentication open
```

```
   authentication key-management wpa
   wpa-psk ascii Geheim321
!
username Admin password Admin
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 1 mode ciphers aes-ccm tkip
!
 encryption vlan 20 mode ciphers aes-ccm tkip
 !
 ssid IT-Admin
 !
```

```
 ssid Mitarbeiter
 !
 ssid Gast-WLAN
 !
 mbssid
speed basic-1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
no dot11 extension aironet
world-mode dot11d country-code DE both
!
interface Dot11Radio0.1
 description WLAN unter VLAN-1 (verschlüsselt nicht sichtbar Management)
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
!
interface Dot11Radio0.10
 description WLAN unter VLAN-10 (offen unverschlüsselt, Gast WLAN für Hotspot)
```

```
 encapsulation dot1Q 10
 no ip route-cache
 bridge-group 10
!
interface Dot11Radio0.20
 description WLAN unter VLAN-20 (verschlüsselt, sichtbar)
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet0.10
```

```
 description VLAN-10
 encapsulation dot1Q 10
 no ip route-cache
 bridge-group 10
!
interface FastEthernet0.20
 description VLAN-20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
!
interface BVI1
 ip address dhcp client-id FastEthernet0  (DHCP oder feste IP vergeben Management)
 no ip route-cache
```

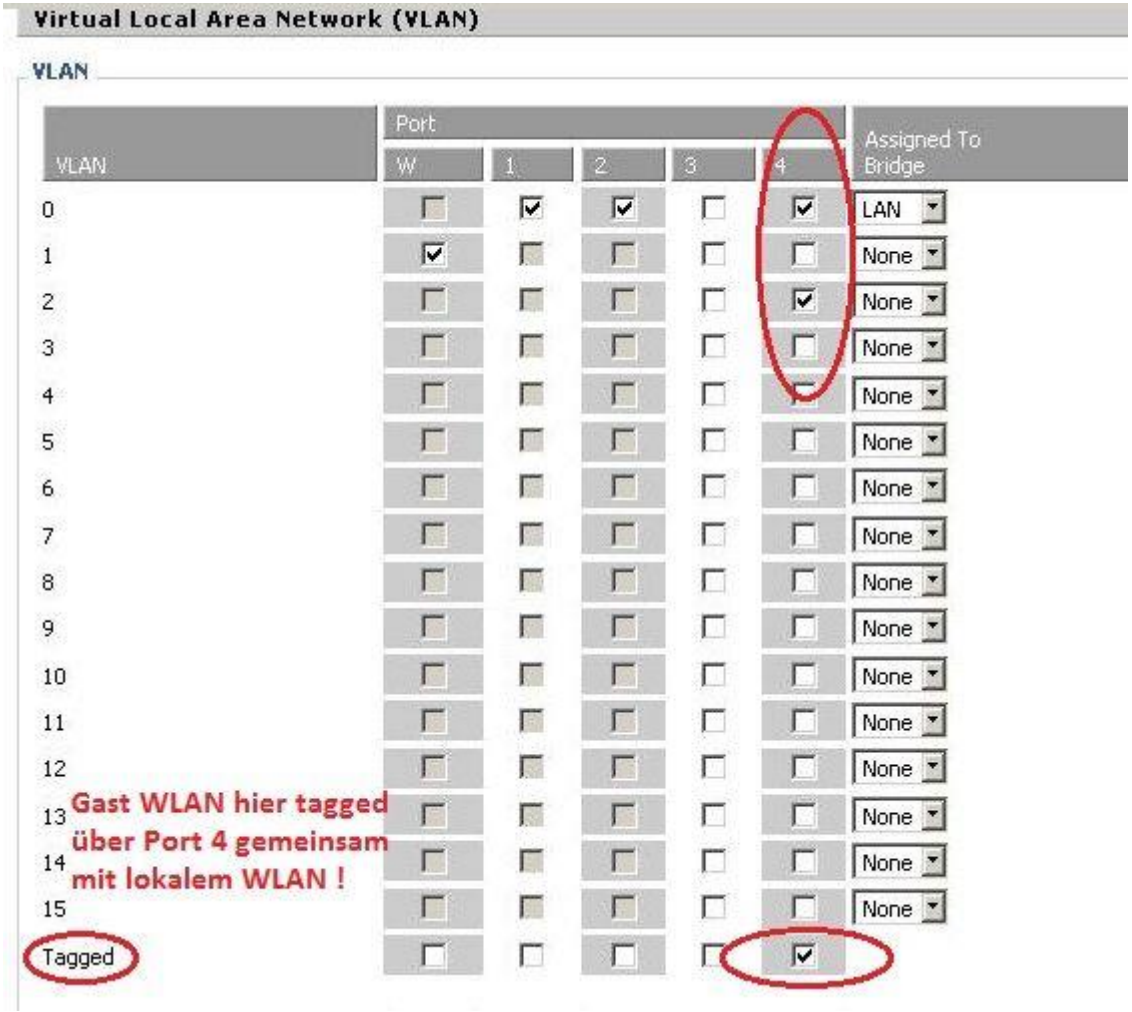
DD-WRT WLAN Router als Multi SSID Accesspoint konfigurieren:

Natürlich kann man auch einen DD-WRT WLAN Router als Multi SSID Accesspoint konfigurieren. Das folgende Beispiel hier zeigt wie man es macht !

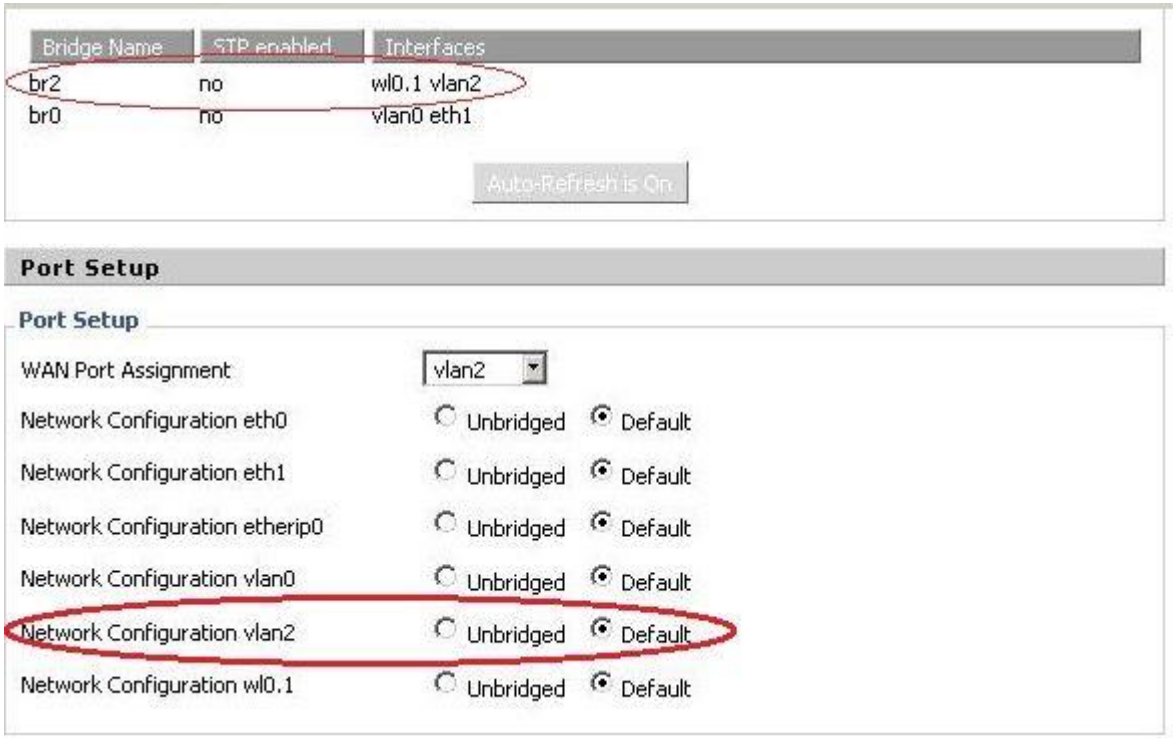
Nur zur Erinnerung in diesem Beispiel wir der Router nur rein als Accesspoint benutzt NICHT als WLAN Router für 2 SSIDs was aber auch möglich ist. Tips dazu im folgenden Text:

Im **1. Schritt** ist unter Setup -> Networking -> Create Bridge eine neue Bridge mit dem Namen "br2" einzurichten:

und dann mit "Apply Settings" und "Save" zu sichern.
Im **Schritt 2** ist unter Setup -> VLANS ein VLAN für den Gastzugang einzurichten (Beispiel hier VLAN 2) und dem Port 4 **tagged** zuzuweisen:

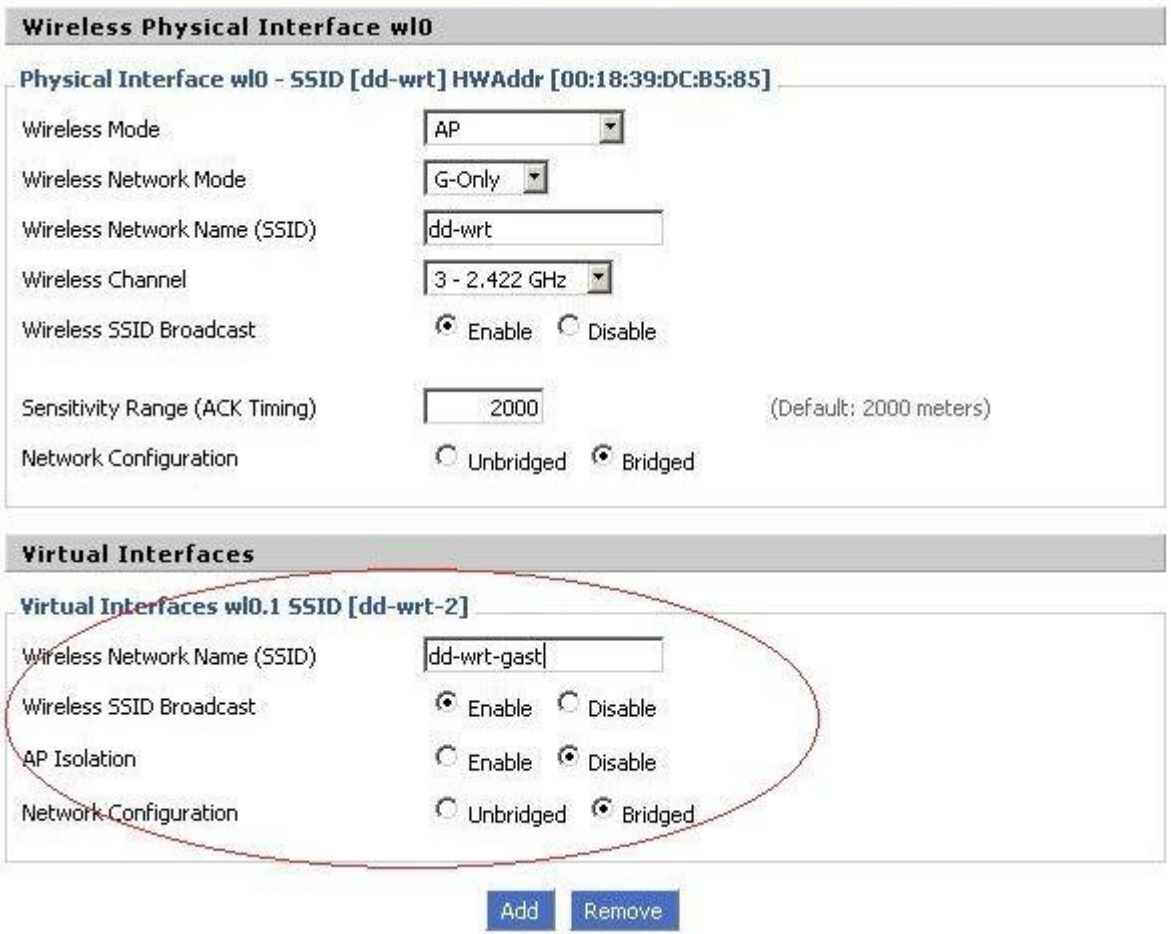


Das VLAN 2 bleibt bei der Verwendung als reiner AP im Setting Setup -> Networking -> Port Setup im "Default" Mode.



(Achtung: Wer den DD-WRT auch als Router benutzt muss hier auf *unbridged* klicken und dem VLAN eine IP Adresse aus dem Gastnetz zuweisen ! Bei der Verwendung als nur AP entfällt dies natürlich!)

Im **4. Schritt** wird das 2te WLAN bzw. die 2te SSID eingerichtet unter Wireless -> Basic Setting -> Virt.Interface



Im **letzten Schritt** werden die beiden Interfaces "vlan2" und "wlan0.1" der Bridge 2 zugeordnet unter Setup -> Networking -> Assign to Bridge

Fertig !
Danach muss man den DD-WRT Accesspoint einmal kaltstarten. Im Testaufbau funktioniert ohne den Kaltstart der tagged Link nicht auf den Switch.

Das Native Interface oder Parent Interface:

Wichtig ist zu beacxhten das der Anschlussport am VLAN Switch für diesen WLAN MSSID Accesspoint oder generell bei tagged Uplinks immer auf **tagged** (bzw. Trunk beim Cisco) für alle VLANs gesetzt werden muss.
Klar...denn der AP ordnet ja, wie oben bereits bemerkt, die WLAN ESSIDs (WLAN Name) oder generell VLAN ID getaggte Pakete den entsprechenden VLAN Tags (VLAN ID) zu um sie dann im korrespondierenden VLAN zu forwarden.!
Einzige **Ausnahme** ist hier immer das default **VLAN 1** das immer untagged am Port anliegen muss !!
Auf einem tagged Uplink wird das default VLAN oder auch *native VLAN* immer untagged übertragen.
Das ist insofern wichtig als das die Mangement IP Adresse des WLAN Accesspoints oder einens VLAN Switches dann immer in diesem default VLAN-1 liegt die man erreichen möchte.
Sinnvoll ist dann immer ein Gastnetz NICHT in dieses Default VLAN / WLAN 1 zu legen, sondern immer eine separate ESSID bzw. VLAN dafür zu verwenden, um Gästen schon hardwareseitig den Zugang zu solchen Management IPs zu versperren !
Das VLAN 1 sollte dann ausschliesslich dem management vorbehalten sein. Oder alternativ kann man untagged Pakete in ein anderes VLAN forwarden sofern die Switchkonfig das auch supportet.

Damit hat man mit wenig Aufwand eine einfache, preiswerte und zudem sichere WLAN Installation umgesetzt, die sehr preiswert mehrere getrennte WLANs auf einem gemeinsamen Accesspoint betreibt um Besuchern ein einfaches Login inklusive Ticketsystem mit Einmalpasswörtern zu ermöglichen und sich selbst rechtlich abzusichern (Logging) !

In Verbindung mit einer kostenfreien 802.1x_Benutzer_Authentifizierung im WLAN sind damit sogar hochsichere Firmen (...und auch Privat) WLANs in Verbindung mit einem einfachen Besucherzugang umsetzbar und das alles ohne große Mehrkosten.
Gleichzeitig trennt diese Lösung auf gemeinsam genutzter Switch- und AP Hardware absolut zugriffssicher das Gästenetz vom Firmennetz und Firmen WLAN ohne einen teuren Hardware- und Administrations Aufwand !

Dieses klassische Captive Portal Design ist mit der preiswerten M0nowall/pfSense_Firewall und auch preiswerten Consumer WLAN Accesspoints wie dem o.a. Edimax u.a. problemlos auch mit sehr kleinem Budget umzusetzen und bietet damit einen erheblichen Mehrwert an Sicherheit mit gleichzeitigem Benutzerkomfort !

Weiterführende Links und Konfig Beispiele zum Thema VLAN:

Forumstutorial zu IP Routing Grundlagen:
https://www.administrator.de/contentid/56073

ct' Wissens Artikel zum Thema VLAN:
http://www.heise.de/netze/artikel/VLAN-Virtuelles-LAN-221621.html

VLAN Tutorial vom Forumsmitglied Edi:
http://www.schulnetz.info/2011/04/

VLANs in der Wikipedia:
http://de.wikipedia.org/wiki/Virtual_Local_Area_Network

VLAN Konfiguration Mikrotik ab Router OS Version 6.41 und höher:
https://www.administrator.de/wissen/mikrotik-vlan-konfiguration-router-o ...

VLANs mit Mikrotik auf HP ProCurve Switch im Detail:
https://www.administrator.de/contentid/245872#comment-942279

VLANs auf HP ProCurve 1910 Switch und pfSense:
https://www.administrator.de/content/detail.php?id=366738&token=945

VLANs mit Mikrotik auf TP-Link Switch im Detail:
https://www.administrator.de/wissen/vlan-mit-mikrotik-rb750gl-und-tp-lin ...

VLANs mit FritzBox, Mikrotik auf NetGear Switches (GS105E, GS108E, GS724) im Detail:
https://www.administrator.de/wissen/-315005.html
https://www.administrator.de/forum/mikrotik-system-reset-configuration-e ...

Mysterium "PVID" bei VLAN Setup erklärt...:
https://www.administrator.de/forum/gibt-pvid-vlans-325880.html
Dazu auch: Tips zum Default VLAN Verhalten auf einem tagged Uplink eines Switches:
https://www.administrator.de/content/detail.php?id=249356&token=583

Interner VLAN Switch im Mikrotik Router anpassen:
https://www.administrator.de/content/detail.php?id=329880&token=293

VLAN Design und Internet Anbindung mit Layer 3 (Routing) Switch:
https://www.administrator.de/forum/verständnissproblem-routing-sg30 ...
https://www.administrator.de/forum/bestehendes-netzwerk-vlans-trennen-ei ...
https://www.administrator.de/content/detail.php?id=329622&token=813

Bandbreite zwischen Switch und Router Uplink mit 802.3ad/LACP LAG (Trunk) vervielfachen:
https://www.administrator.de/content/detail.php?id=314020&token=315# ...
https://www.administrator.de/wissen/netzwerk-management-server-raspberry ...

VLANs mit DD-WRT auf HP 1810 Switch im Detail:
https://www.administrator.de/content/detail.php?id=264417

Wichtig: Erklärung des Firewall Filter- und Regelwerks am Beispiel eines gesicherten Schul Netzes:

https://www.administrator.de/forum/pfsense-drucker-vlan-getrennten-wlan- ...

VLANs auf einem Server realisieren:
https://www.administrator.de/contentid/58974 (Windows)
https://www.administrator.de/contentid/191718 (Linux)

Dynamische VLAN Zuweisung mit 802.1x:
https://www.administrator.de/contentid/154402

WLAN Netz mit Multi SSID und VLAN auf DD-WRT:
http://www.dd-wrt.com/phpBB2/viewtopic.php?t=64098
und auch
http://www.flashsystems.de/articles/1730

pfSense Firewall mit Gast-WLAN / VLAN:
https://www.administrator.de/wissen/preiswerte-vpn-fähige-firewall- ...
https://www.administrator.de/wissen/wlan-oder-lan-gastnetz-einrichten-mi ...
Tagging Anfänger Hürden überwinden:
https://www.administrator.de/content/detail.php?id=315534&token=243# ...

Details zum hiesigen "Praxisbeispiel" Gast WLAN Setup mit Mikrotik RB 751U:
https://www.administrator.de/contentid/233966

Raspberry Pi als VLAN Router:
https://www.administrator.de/contentid/191718#toc-13

Mikrotik Router in Verbindung mit IP-TV Multicast (Entertain)
https://www.administrator.de/content/detail.php?id=262139&nid=72026
Mikrotik mit gerouteten Multicast (IP PIM) VLAN Segmenten:
https://www.administrator.de/contentid/268367
Mikrotik mit gerouteten Multicast (IP PIM) VLAN Segmenten und mDNS (Bonjour) Proxy mit Rasberry Pi:
https://www.administrator.de/forum/upnp-mikrotik-routerboard-hex-poe-d-l ...

Praxisbeispiel 2 Netze u. 2 Internet Router ohne stat.Routing
https://www.administrator.de/contentid/228775

"Praxisbeispiel" VLAN Setup mit Cisco RV110 und D-Link Switch:
https://www.administrator.de/contentid/255428

Redundantes Routing Umfeld mit VRRP:
https://www.administrator.de/forum/vrrp-einrichtung-335355.html

Subnetze dynamisch routen mit OSPF (Mikrotik):
https://www.administrator.de/content/detail.php?id=361951&token=426# ...

pfSense Firewall Konfiguration mit IP-TV Multicast (Entertain)
https://www.administrator.de/forum/telekom-entertain-iptv-tp-link-switch ...

Beispiel direktes L3 Routing ohne externen Router
http://vmfocus.com/2012/09/26/how-to-configure-layer-3-static-routes-vl ...

VDSL und ADSL Modem Übersicht bei Breitband Routern:
https://www.administrator.de/forum/suche-adsl2-vdsl-modem-291077.html