VLAN - Virtual LAN

VLAN si lze představit jako virtuální linky po existujících fyzických linkách
Po jedné fyzické lince je možné teoreticky provozovat až 4094 virtuálních linek, jsme pouze omezeni fyzickou kapacitou linky
Nejpoužívanější je tagovací protokol **IEEE 802.1Q**

netagovaná vlana	- Na každém portu switche může být pouze 1 - Na klientskem zarizeni neni potreba provadet zadna nastaveni, pokud je pripojen do portu s netagovanou vlanou - Pokud prichozi paket není označen tagem, defaultně spadá vždy do vlany, která je na portu nastavená jako netagovaná - Netagovana vlan musi byt zaroven zadana ve switchi v polozce PVID, aby switch vedel, do ktere vlan ma zaradit neoznacene pakety na portu
tagovaná vlana	- Na každém portu switche může být více tagovaných vlan, dokonce je možné kombinovat s jednou netagovanou vlanou - Kazdy paket je oznacen znackou (tagem), aby switch vedel o jeho prislusnosti ke konkretni vlane - Kazde zarizeni, ktere ma pracovat s tagovanou vlanou nejprve musi sve pakety oznacit znackou, do ktere vlany pakety maji byt zarazeny, jinak je switch v zavislosti na nastaveni portu bud zaradi do netagovane vlanmy, nebo paket zahodi

Každou VLANu označujeme číslem. Z důvodu kompatibility se všemi prvky nelze používat libovolně všechna čísla, která máme k dispozici:

Podporovaná čísla VLAN

VLAN	Význam
0	nepoužívá se
1	výchozí VLAN; defaultně všechny porty; nelze smazat ani menit
2-4092	**volne k dispozici**
4093-4094	Na některých switchích jsou tyto vlany rezervovány pro zvláštní použití např. pro stackování apod. proto je nebudeme používat.

Nastavení portů na switchi

Při nastavení VLANu na port switche rozeznáváme 3 druhy nastavení portu:

nastaveni portu	vyznam
ACCESS	- Na portu je pouze 1 netagovana VLAN - Nelze pouzivat vice vlan, vsechny pakety jsou zarazeny do vlany, nastavene na portu - Pouziva se napr. na portech k ubinam, k zakaznikum apod. - PVID portu musíme nastavit na cislo netagovane vlany

GENERAL	- Na portu je povolena ! 1 netagovana VLAN a libovolny pocet tagovanych VLAN - Ktera VLAN je na portu tagovana a ktera netagovana je potreba specifikovat v dalsim nastaveni switche - Pouziva se napr. na portech, kam je zapojen router - management sit je vetsinou netagovana a ostatni linky pak tagovany - PVID musime nastavit na cislo netagovane vlany - Nekdy muze byt tato moznost take oznacena jako HYBRID
TRUNK	- Na portu jsou povoleny pouze tagovane vlany - Pakety, ktere na port dorazi a nejsou opatřeny správnou značkou jsou zahozeny - Pouziva se napr. na propojeni switchu ruznych siti apod. - Nastaveni PVID se v tomto pripade ignoruje

Poznamka: některé switche toto rozdělení nerespektují a umožnují pouze nastavit, jestli je VLAN tagovaná nebo netagovaná. Pokud chceme na portech akceptovat pouze tagovane vlany - tj. pouzivat TRUNK - je nutné ve switchi hledat volbu odpovídající volbu (napr. untag frame = drop atd.)

Pravidla pro přidělování VLAN

- V rámci jednoho routeru a routerů, kam vedou připojené linky MUSÍ být číslo vlan unikátní.
- Stejné číslo vlan MUSÍ být stejné na obou stranách spoje (např. u bezdrátových linek apod.)
- Pokud na portu nastavujeme netagovanou vlan, je nutné zároveň specifikovat i PVID - uvádíme stejné číslo, jako je číslo zamýšlené netagované vlan - PVID říká switchi, že všechny pakety, které na něj přijdou bez značky označí automaticky značkou vlany, uvedené v PVID. **Pokud zapomenete nastavit PVID na portu, nebude netagovana vlan na portu fungovat**
- Defaultně nechávám VLAN 1 jako management vlan a tudíž na některých portech najdete stále defaultní 1 jako netagovanou. Veškerý ostatní provoz je přesunut do jiných VLANu.
- Dejte pozor, aby jste sit pri nastavení vlanu nekde spatne nezakruhovali. VLANy se chovaji stejne, jako kdyz zapojujete fyzicke kabely, takze pokud s vlanem udelate neco podobneho jako ze propojite dva switche dvema fyzickýma kabelama, dojde ke stejnemu pruseru !!
- **Pokud vlanu na daném portu jiz nepotrebujete, napr. tim ze se linka zrusila nebo nekam presunula, tak zruste nastaveni na switchi, pripadne zruste celou vlan i na routeru.**
- **Nastavení dokumentujte**
- **VLAN musíte nastavit na každém switchi po cestě mezi routerem a switchem, kam je zařízení zapojeno. Nekdě to mohou být mi další 2 switche po cestě**

- V kazde vlane muze byt libovolny pocet portu, na kterych lze kombinovat nastaveni (na nekterych portech muze byt vlana tagovana, na nekterych muze byt netagovana popr. muze byt na vsech portech pouze tagovana)
- Nektere switche vyzaduji minimalne 2 porty ve vlane

Debian - Routery

Přidání nové vlany na Debianu je velmi jednoduché. Potřebujeme k tomu akorát zavedený modulu `8021q` - na routerech uz vsude je.

Následně editujeme `/etc/network/interface`

/etc/network/interface

```
# nova linka
auto vlan1045
iface vlan1045 inet static
        address 10.11.30.49
        netmask 255.255.255.248
        vlan_raw_device eth0
```

- **vlan1045** = uvedene cislo vlany, ktere si zvolime a ktere budeme potom nastavovat na switchi. Cislo v debianu uvedeme slovem *vlan*
- **vlan_raw_device** = zde uvedeme fyzický interface, na kterem bude tento vlan nastaven jako tagovaný
- Zapnutí interface `ifup vlan1045`
- Vypnuti interface `ifdown vlan1045`

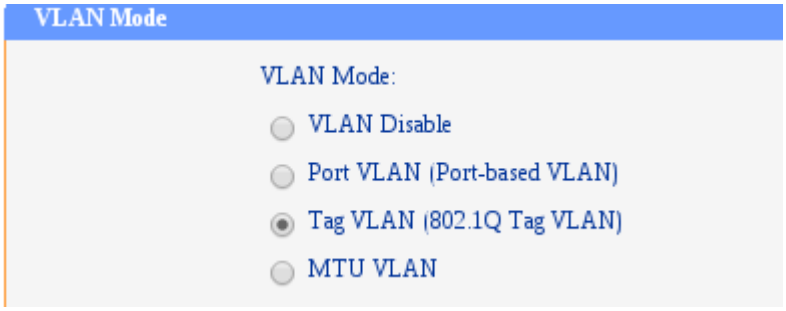
V linuxu nastavujeme jen tagované vlany, protože netagované je automaticky všechno co přijde na sítovku bez značek.

- Nově připravený interface zapneme následně po uložení konfiguračního souboru pomocí příkazu **IFUP**
- **NIKDY nepoužíváme /etc/init.d/networking restart !!!**

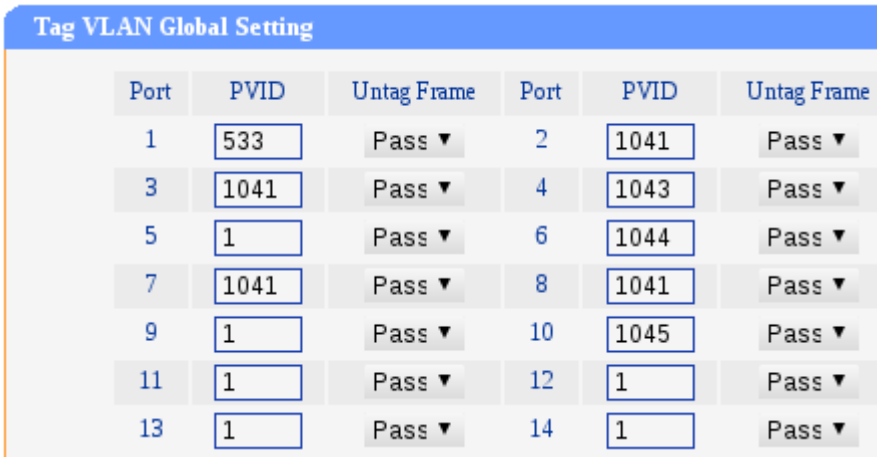
Switche

Tady ukážu nastavení v několika druzích switchů

Stara verze TP-LINK

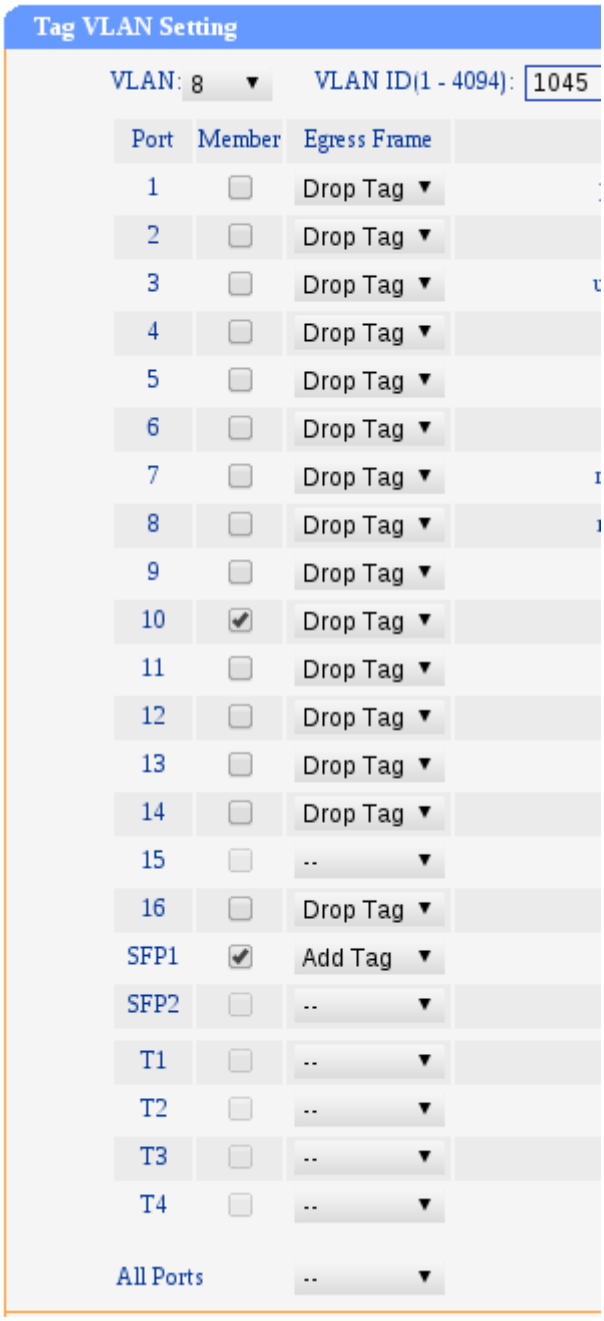


1. Nejprve zapneme tagovaci protokol (pokud to jeste neni)



2. Nastavime PVID popr. zakazeme netagovane pakety na prislusnem portu

- PVID musi obsahovat cislo vlany, ktere na portu zamýšlíme používat jako netagovanou
- UNTAG FRAME = nastavime na DROP, pokud chceme ignorovat netagovane pakety a PVID na uvedenem portu

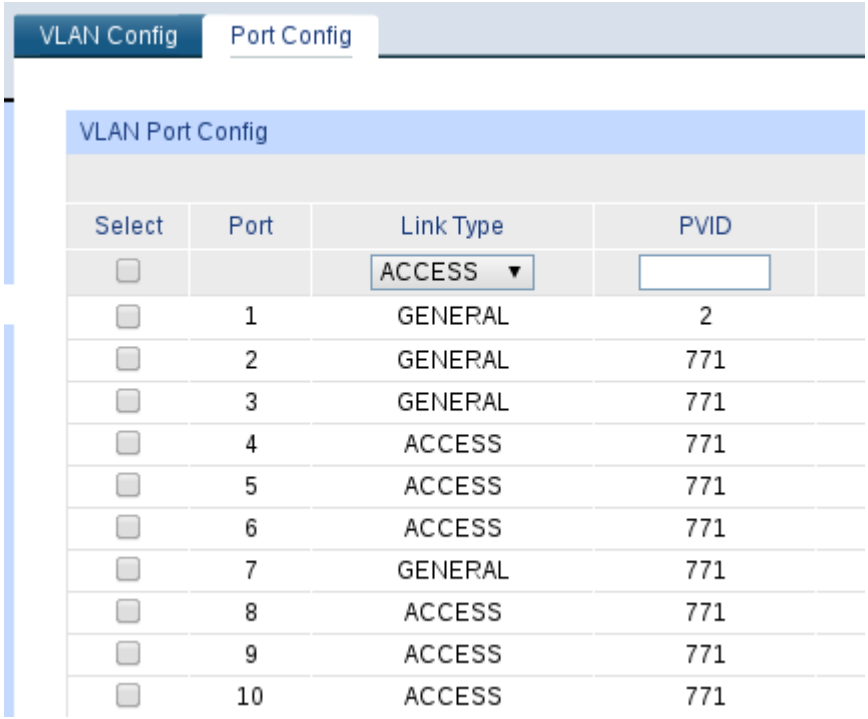


3. Nastavíme zaskrtnutim, které porty mají být členem konkrétní vlany

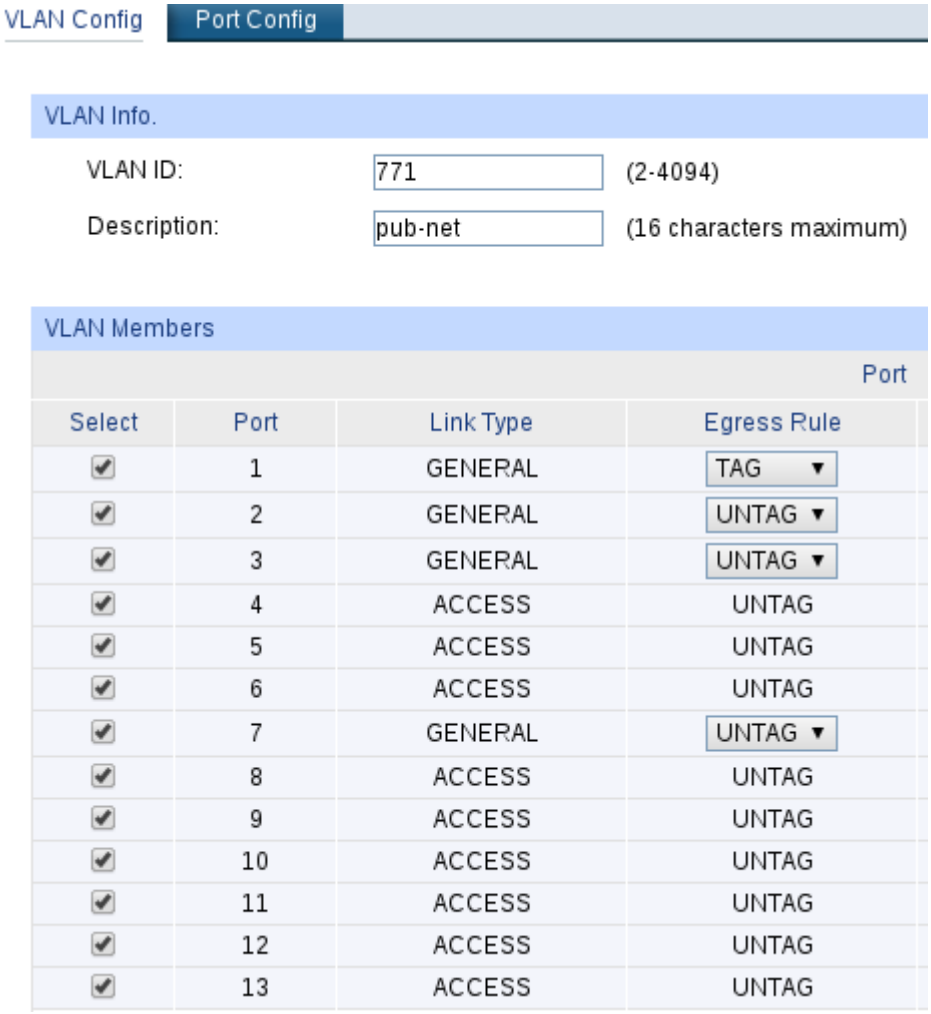
- DROP TAG = na uvedenem portu bude vlan defaultni tj. netagovana = nesmime zapomenout nastavit jeste PVID
- ADD TAG = na uvedenem portu bude vlan jako tagovana

JetStream

V nove verzi TP-Linku je nastavení jednodušší



1. Zde nastavujeme port. ACCES ; GENERAL ; TRUNK - viz. tabulka vyse. PVID musime nastavit jen v pripade, ze zvolime ACCESS nebo GENERAL



VLAN Config | Port Config

VLAN Info.

VLAN ID: 771 (2-4094)

Description: pub-net (16 characters maximum)

VLAN Members

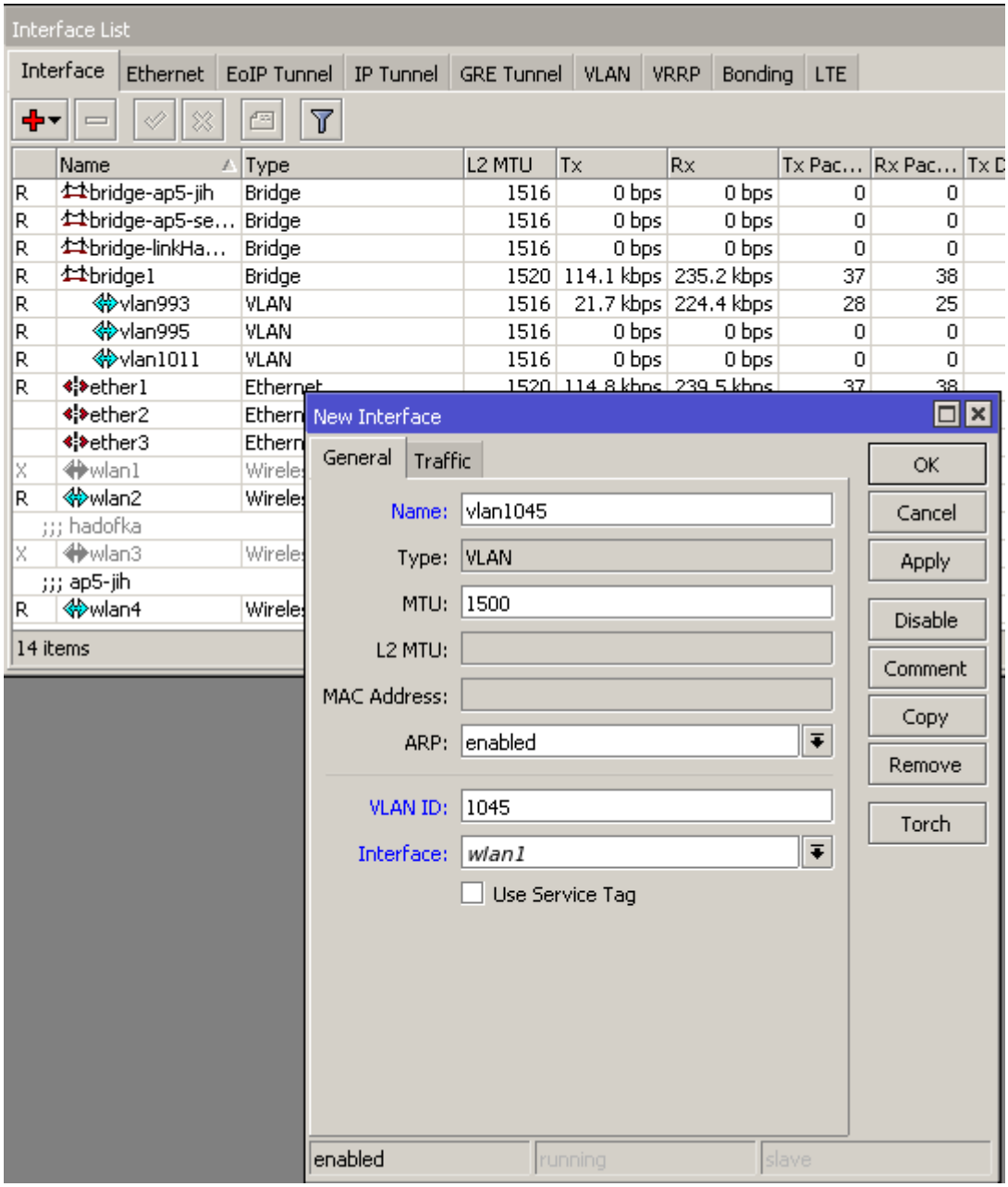
Port

Select	Port	Link Type	Egress Rule
☑	1	GENERAL	TAG
☑	2	GENERAL	UNTAG
☑	3	GENERAL	UNTAG
☑	4	ACCESS	UNTAG
☑	5	ACCESS	UNTAG
☑	6	ACCESS	UNTAG
☑	7	GENERAL	UNTAG
☑	8	ACCESS	UNTAG
☑	9	ACCESS	UNTAG
☑	10	ACCESS	UNTAG
☑	11	ACCESS	UNTAG
☑	12	ACCESS	UNTAG
☑	13	ACCESS	UNTAG

2. Zakrtnutim nastavujeme clenstvi portu v jednotlivych vlan. Pokud je port nastaven jako GENERAL, pak je mozne vybrat, jestli uvedena vlana bude na portu tagovana nebo netagovana.

Mikrotik

V mikrotiku vytváříme tagovaný vlan tak, že založíme nový interface typu VLAN



1. klikneme na **interface** > **+** > **VLAN**
2. **name** - libovolny nazev ⇒ **doporucuju pouzivat stejna oznaceni jako na debianu**
3. **VLAN ID** - cislo vlanu, ktere potom musim dodrzet na switchi a musi byt v ramci switche i routeru unikatni - viz. predchozi pravidla
4. **Interface** - zvolim interface, kde se ma vlan pouzivat. Pokud mame na mikrotiku fyzické porty v bridgi, musíme vlan vytvořit az na bridgeujicim interface !!

Stejné nastavení lze provést take pomocí terminálu

```
[admin@altair2] > interface vlan add name=vlan1045 vlan-id=1045
interface=bridge1
[admin@altair2] > interface vlan print
Flags: X - disabled, R - running, S - slave
 #    NAME
MTU ARP        VLAN-ID INTERFACE
 0 R  vlan995
1500 enabled        995 bridge1
```

```
 1 R  vlan993
1500 enabled        993 bridge1
 2 R  vlan1011
1500 enabled       1011 bridge1
 3 R  vlan1045
1500 enabled       1045 bridge1
[admin@altair2] >
```

GVRP / MVRP

MVRP je novejsi alternativa GVRP, je to prakticky to samy. Lisi se hlavne tim, ze GVRP bezi nad protokolem GARP, zatim co MVRP bezi nad protokolem MRP. Starsi switche asi umi jen GVRP.

GMRP/MMRP je neco jako GVRP/MVRP, ale misto vlanu se tim prihlasujou multicastovy skupiny. S VLANama to nesouvisi a zminuju to tu jen pro uplnost.

GVRP je protokol, kterej umoznuje automaticky protahovani vlanu pres switche, ktere to umi a porty na kterych je to povoleny (je to potreba povolit jak globalne, tak na jednotlivejch portech). Pokud mam propojene dva switche pres TRUNK, ktery ma na obou stranach povolene GVRP a na nejaky dalsi port pridam VLAN, tak switch zacne pres GVRP porty anoncovat, ze tam ten VLAN je a ostatni switche mu ho do toho TRUNKu poslou. Na koncovych portech tedy VLANy musi byt pridany staticky, do trunku po ceste se pridaji dynamicky. Nevim jak u ostatnich vyrobcu, ale na TP-Linku se mi nepodarilo zapnout GVRP na portu v rezimu GENERAL. Musi byt TRUNK.

V TP-Linku, Huaweii (a asi i dalsich) muze mit kazdy port se zapnutym GVRP 3 rezimy:

- **Normal** - Vsechny staticke VLANy se propaguji a zaroven se pridavaji a ubiraji dynamicke VLANy
- **Fixed** - Pouze se propaguji staticke VLANy nakonfigurovane na tomto switchi (takze "readonly")
- **Forbidden** - Nic se dynamicky nekonfiguruje ani nepropaguje. S vyjimkou propagace VLAN 1 (defaultniho vlanu)

Pokud mam TRUNK port s povolenym GVRP a pripojim k nemu Linux, tak si muzu na sitovce nahodit VLAN a nasledujicim zpusobem ho zacit anoncovat do switche pres GVRP:

Zkontroluju podporu v kernelu:

```
# grep -i vrp /boot/config-*
/boot/config-4.9.0-5-686-pae:CONFIG_VLAN_8021Q_GVRP=y
/boot/config-4.9.0-5-686-pae:CONFIG_VLAN_8021Q_MVRP=y
```

Vytvorim vlan a zapnu GVRP a MVRP:

```
vconfig add eth0 220
ip link set eth0.220 type vlan gvrp on mvrp on loose_binding on
```

Pripadne muzu GVRP zapnout rovnou pri vytvareni vlanu:

```
ip link add link eth0 eth0.103 type vlan id 103 gvrp on mvrp on
loose_binding on
```

```
ip link set eth0.103 up
```

Overim, jestli to dany interface ma fakt zapnuty:

```
ip -d link show type vlan | grep --color '.VRP\|$'
```

Taky existuje nejaky GVRP klient demon gvrpcd, ktery udajne naopak naslouchá GVRP oznamenim a zjistuje tak, jaky vlany anoncujou sousedi, aby je mohl u sebe zakladat. Prijde mi, ze v README se pise pravej opak. Ale nevim presne, jeste jsem to nenastudoval:

- http://zagrodzki.net/~sebek/gvrpcd/

Pokud chci debugovat GVRP traffic, tak si ho muzu vyfiltrovat pomoci tcpdumpu. tcpdump na to nema zvlast filtr, ale GVRP vzdy pouziva specialni vyhrazenou MAC adresu 01:80:c2:00:00:21, takze to lze filtrovat podle ni:

```
tcpdump -X -i eth0 ether dst 01:80:c2:00:00:21 #GVRP i MVRP
tcpdump -X -i eth0 ether proto 0x88F5 #Jen pro Ethernet II rámce (=Asi jen MVRP)
```

Podporovane switche(?):

- TP-Link JetStream
- Brocade (Bohuzel asi ne FastIron CX 648S)
- Huawei
- Cisco
- Ubiquiti
- Allied Telesis
- HP

Zdroje:

- http://confluence.wartungsfenster.de/display/Adminspace/Linux+GVRP+usage
- http://wh.cs.vsb.cz/sps/images/c/c5/STP-Linux.pdf
- http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.137.1189&rep=rep1&type=pdf

From:
https://wiki.spoje.net/ - **SPOJE.NET**

Permanent link:
https://wiki.spoje.net/doku.php/howto/network/vlan

Last update: **2019/07/29 15:03**