

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 vlna	<ul style="list-style-type: none"> - Na každém portu switche může být pouze 1 - Na klientskem zarizeni není potřeba provádět žádná nastavení, pokud je připojen do portu s netagovanou vlnou - Pokud přichází paket není označen tagem, defaultně spadá vždy do vlny, která je na portu nastavená jako netagovaná - Netagovaná vlna musí být zároveň zadána ve switchi v položce PVID, aby switch vedel, do které vlny má zaradit neoznačené pakety na portu
tagovaná vlna	<ul style="list-style-type: none"> - Na každém portu switche může být více tagovaných vln, dokonce je možné kombinovat s jednou netagovanou vlnou - Každý paket je označen značkou (tagem), aby switch vedel o jeho příslušnosti ke konkrétní vlně - Každé zařízení, které má pracovat s tagovanou vlnou nejprve musí své pakety označit značkou, do které vlny pakety mají být zarazeny, jinak je switch v závislosti na nastavení portu buď zaradí do netagované vlny, nebo paket zahodí

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 měnit
2-4092	volně k dispozici
4093-4094	Na některých switchích jsou tyto vlny 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:

nastavení portu	význam
ACCESS	<ul style="list-style-type: none"> - Na portu je pouze 1 netagovaná VLAN - Nelze používat více vln, všechny pakety jsou zarazeny do vlny, nastavené na portu - Používá se např. na portech k ubinám, k zákazníkům apod. - PVID portu musíme nastavit na číslo netagované vlny

GENERAL	<ul style="list-style-type: none"> - Na portu je povolena ! 1 netagovaná VLAN a libovolný počet tagovaných VLAN - Která VLAN je na portu tagována a která netagována je potřeba specifikovat v dalším nastavení switchu - Používá se např. na portech, kam je zapojen router - management síť je většinou netagována a ostatní linky pak tagovány - PVID musíme nastavit na číslo netagované vlany - Někdy může být tato možnost také označena jako HYBRID
TRUNK	<ul style="list-style-type: none"> - Na portu jsou povoleny pouze tagované vlany - Pakety, které na port dorazí a nejsou opatřeny správnou značkou jsou zahazeny - Používá se např. na propojení switchu různých sítí apod. - Nastavení PVID se v tomto případě ignoruje

Poznámka: některé switchy toto rozdělení nerespektují a umožňují pouze nastavit, jestli je VLAN tagovaná nebo netagovaná. Pokud chceme na portech akceptovat pouze tagované vlany - tj. používat TRUNK - je nutné ve switchi hledat volbu odpovídající volbu (např. untag frame = drop atd.)

Pravidla pro přidělování VLAN

- V rámci jednoho routeru a routerů, kam vedou připojené linky MUSÍ být číslo vln unikátní.
- Stejně číslo vln MUSÍ být stejné na obou stranách spoje (např. u bezdrátových linek apod.)
- Pokud na portu nastavujeme netagovanou vln, je nutné zároveň specifikovat i PVID - uvádíme stejné číslo, jako je číslo zamýšlené netagované vln - 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 netagovaná vln na portu fungovat**
- Defaultně nechávám VLAN 1 jako management vln a tudíž na některých portech najdete stále defaultní 1 jako netagovanou. Veškerý ostatní provoz je přesunut do jiných VLANu.
- Dejte pozor, aby jste si při nastavení vlnu nekde špatně nezakruhovali. VLANy se chovají stejně, jako když zapojujete fyzické kabely, takže pokud s vlnem udeláte něco podobného jako že propojíte dva switchy dvěma fyzickými kabelama, dojde ke stejnému pruseru !!
- **Pokud vlnu na daném portu již nepotřebujete, např. tím že se linka zrusila nebo nekam přesunula, tak zrušte nastavení na switchi, případně zrušte celou vln i na routeru.**
- **Nastavení dokumentujte**
- **VLAN musíte nastavit na každém switchi po cestě mezi routerem a switchem, kam je zařízení zapojeno. Někdy to mohou být i další 2 switchy po cestě**



- V každé vlance může být libovolný počet portů, na kterých lze kombinovat nastavení (na některých portech může být vlana tagována, na některých může být netagována popř. může být na všech portech pouze tagována)
- Některé switchy vyžadují minimálně 2 porty ve vlance

Debian - Routery

Přidání nové vlany na Debianu je velmi jednoduché. Potřebujeme k tomu akorát zavedený modul 8021q - na routerech už všude 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`
- Vypnutí interface `ifdown vlan1045`

V linuxu nastavujeme jen tagované vlany, protože netagované je automaticky všechno co přijde na síťovku 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 tagovací protokol (pokud to jeste neni)

Tag VLAN Global Setting					
Port	PVID	Untag Frame	Port	PVID	Untag Frame
1	533	Pass ▼	2	1041	Pass ▼
3	1041	Pass ▼	4	1043	Pass ▼
5	1	Pass ▼	6	1044	Pass ▼
7	1041	Pass ▼	8	1041	Pass ▼
9	1	Pass ▼	10	1045	Pass ▼
11	1	Pass ▼	12	1	Pass ▼
13	1	Pass ▼	14	1	Pass ▼

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

Tag VLAN Setting		
VLAN: 8 ▼	VLAN ID(1 - 4094): 1045	
Port	Member	Egress Frame
1	<input type="checkbox"/>	Drop Tag ▼
2	<input type="checkbox"/>	Drop Tag ▼
3	<input type="checkbox"/>	Drop Tag ▼
4	<input type="checkbox"/>	Drop Tag ▼
5	<input type="checkbox"/>	Drop Tag ▼
6	<input type="checkbox"/>	Drop Tag ▼
7	<input type="checkbox"/>	Drop Tag ▼
8	<input type="checkbox"/>	Drop Tag ▼
9	<input type="checkbox"/>	Drop Tag ▼
10	<input checked="" type="checkbox"/>	Drop Tag ▼
11	<input type="checkbox"/>	Drop Tag ▼
12	<input type="checkbox"/>	Drop Tag ▼
13	<input type="checkbox"/>	Drop Tag ▼
14	<input type="checkbox"/>	Drop Tag ▼
15	<input type="checkbox"/>	.. ▼
16	<input type="checkbox"/>	Drop Tag ▼
SFP1	<input checked="" type="checkbox"/>	Add Tag ▼
SFP2	<input type="checkbox"/>	.. ▼
T1	<input type="checkbox"/>	.. ▼
T2	<input type="checkbox"/>	.. ▼
T3	<input type="checkbox"/>	.. ▼
T4	<input type="checkbox"/>	.. ▼
All Ports	<input type="checkbox"/>	.. ▼

3. Nastavíme zaskrtnutím, 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

VLAN Config Port Config

VLAN Port Config

Select	Port	Link Type	PVID
<input checked="" type="checkbox"/>		ACCESS ▾	<input type="text"/>
<input type="checkbox"/>	1	GENERAL	2
<input type="checkbox"/>	2	GENERAL	771
<input type="checkbox"/>	3	GENERAL	771
<input type="checkbox"/>	4	ACCESS	771
<input type="checkbox"/>	5	ACCESS	771
<input type="checkbox"/>	6	ACCESS	771
<input type="checkbox"/>	7	GENERAL	771
<input type="checkbox"/>	8	ACCESS	771
<input type="checkbox"/>	9	ACCESS	771
<input type="checkbox"/>	10	ACCESS	771

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

VLAN Info.

VLAN ID: (2-4094)
Description: (16 characters maximum)

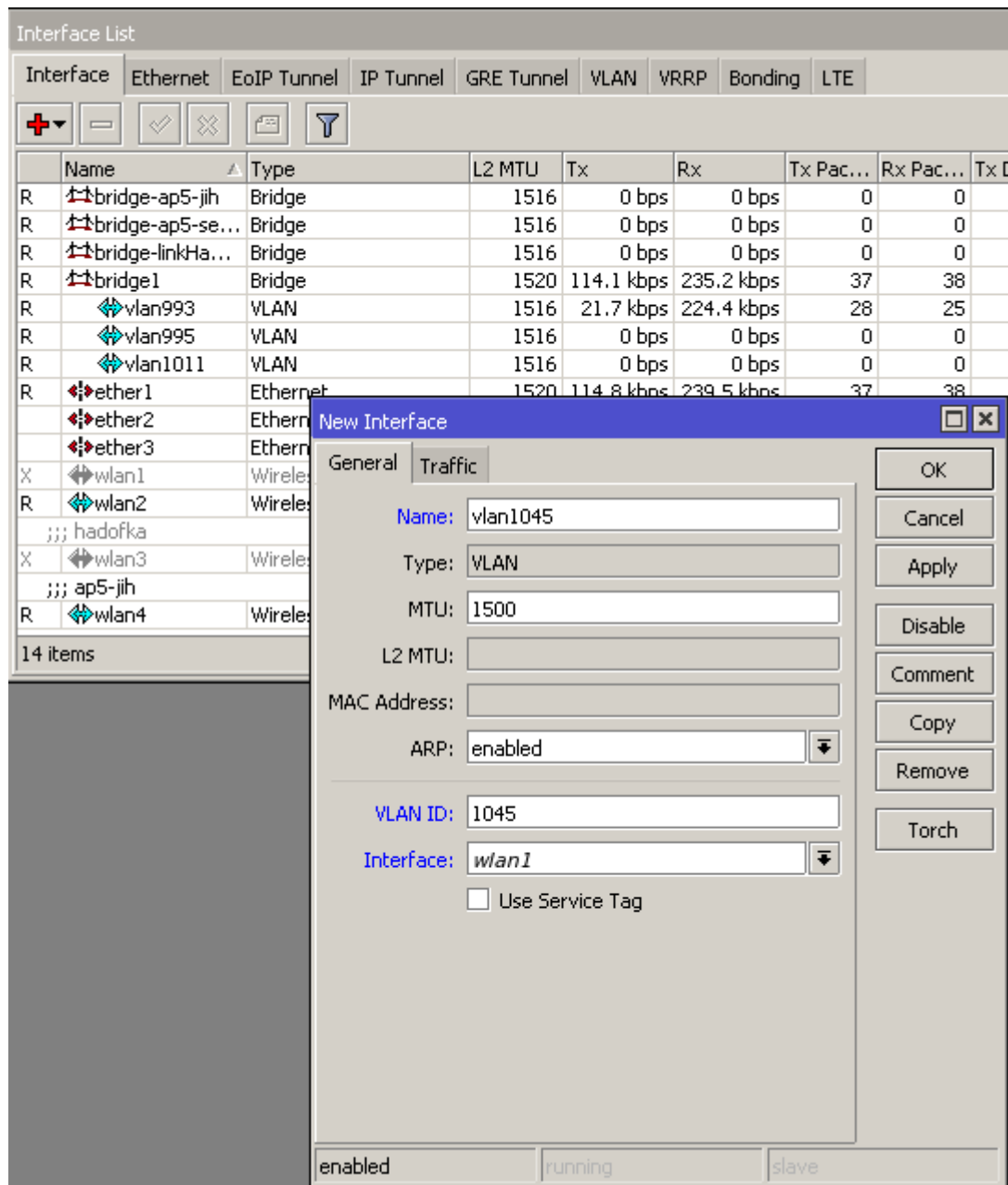
VLAN Members

VLAN Members				Port
Select	Port	Link Type	Egress Rule	
<input checked="" type="checkbox"/>	1	GENERAL	TAG ▼	
<input checked="" type="checkbox"/>	2	GENERAL	UNTAG ▼	
<input checked="" type="checkbox"/>	3	GENERAL	UNTAG ▼	
<input checked="" type="checkbox"/>	4	ACCESS	UNTAG	
<input checked="" type="checkbox"/>	5	ACCESS	UNTAG	
<input checked="" type="checkbox"/>	6	ACCESS	UNTAG	
<input checked="" type="checkbox"/>	7	GENERAL	UNTAG ▼	
<input checked="" type="checkbox"/>	8	ACCESS	UNTAG	
<input checked="" type="checkbox"/>	9	ACCESS	UNTAG	
<input checked="" type="checkbox"/>	10	ACCESS	UNTAG	
<input checked="" type="checkbox"/>	11	ACCESS	UNTAG	
<input checked="" type="checkbox"/>	12	ACCESS	UNTAG	
<input checked="" type="checkbox"/>	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 bridgeujícím interface !!

Stejně nastavení lze provést také 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 jednotlivych 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, Huawei (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
```

```
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
```

Taky existuje nejaky GVRP klient demon gvrpcd, který údajne naopak nasloucha GVRP oznámením a zjistuje tak, jaky vlany anoncuju sousedi, aby je mohl u sebe zakladat. Prijde mi, ze v README se pise pravej opak. Ale nevím 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 zvlášt filtr, ale GVRP vzdy pouziva specialni vyhrazenou MAC adresu 01:80:c2:00:00:21, takže 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
- 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?rev=1542313892>

Last update: **2018/11/15 21:31**

