23. VLAN

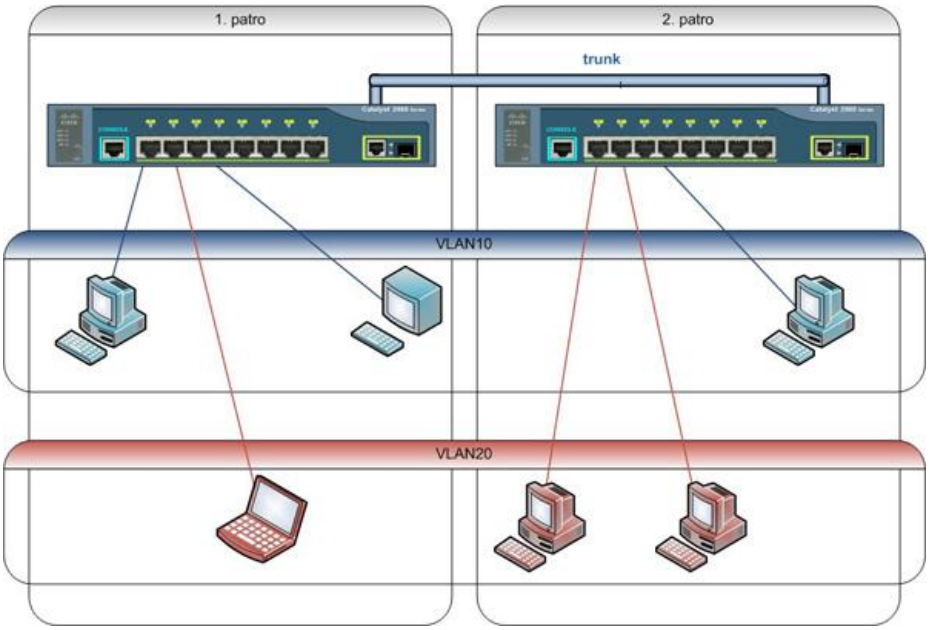
Virtuální LAN slouží k logickému rozdělení sítě nezávisle na fyzickém uspořádání. Lze síť segmentovat na menší sítě uvnitř fyzické struktury původní sítě.

Obvykle bývá realizována na switchích, jehož porty se rozdělí na několik logicky samostatných částí. Jde o dělení sítě už na úrovni 2. vrstvy ISO/OSI, v porovnání s podsítěmi na 3. vrstvě.

Pomocí VLAN lze dosáhnout stejného efektu, jako když je skupina zařízení připojených do jednoho (několika propojených) switche a druhou skupinu do jiného (jiných) switche. Jsou to dvě nezávislé sítě, které spolu nemohou komunikovat (jsou fyzicky odděleny). Pomocí VLAN lze takovéto dvě sítě vytvořit na jednom (nebo několika propojených) switchi.

V praxi se samozřejmě často potřebuje komunikovat mezi těmito sítěmi. S VLAN lze pracovat stejně jako s normálními sítěmi. Tedy použít mezi nimi jakýkoliv způsob routování. Často se dnes využívá L3 switch (switch, který funguje na třetí vrstvě OSI) pro inter-VLAN routing – směrování mezi VLAN.

Jsou dvě patra, na každém patře je switch, switche jsou propojeny páteří s trunkem. Má-li se propojit zařízení do dvou nezávislých skupin (modrá VLAN10 a červená VLAN20). Pomocí VLAN je to takto jednoduché. Tradiční technikou by museli být switche oddělené a každou skupinu (modrou a červenou) propojit do jednoho switche, což by byl problém, protože jsou na různých patrech



Hlavní důvody proč vznikly VLANy:

- Seskupování uživatelů v síti podle skupin či oddělení nebo podle služeb místo podle fyzického umístění a oddělení komunikace mezi těmito skupinami
- Snížení broadcastů v síti, které začaly být problémem již před několika lety
- Zmenšení kolizních domén v době, kdy se nepoužívaly switche, ale třeba huby

Praktické výhody VLAN

- **Snížení broadcastů**
  - Vytvoření více (menších) broadcastových domén → zlepšení výkonu sítě snížením provozu (traffic)
- **Zjednodušená správa**
  - K přesunu zařízení do jiné sítě stačí překonfigurovat zařazení do VLANy → konfigurace SW (zařazení do VLAN) a ne HW (fyzické přepojení)
- **Zvýšení zabezpečení**
  - Oddělení komunikace do speciální VLANy, kam není jiný přístup
  - Toho se dá samozřejmě dosáhnout použitím samostatných switchů, ale často se toto uvádí jako bonus VLAN
- **Oddělení speciálního provozu**
  - Dnes se používá řada provozu, který nemusí být propojen do celé sítě, ale přesto je potřeba ho dostat na různá místa, navíc není žádoucí, aby ovlivňoval běžný provoz. Příkladem je například IP telefonie, komunikace mezi AP v centrálně řízeném prostředí, management (zabezpečení správcovského přístupu k zařízením).
- **Snížení HW**
  - Nesnižuje se potřebný počet portů (až na speciální případy jako IP telefonie), ale tím, že mohou být různé podsítě na stejném switchi, jej lze lépe využít (například pro propojení tří zařízení není potřeba speciální switch, který má minimálně 8 portů).

Čísla VLAN

VLANy se běžně identifikují pomocí čísla, například VLAN 10. Pro jednodušší zapamatování a orientaci se k nim ještě přiřazují jména.

Cisco switche by v posledních letech měly podporovat tyto číselné rozsahy pro VLANy. Starší zařízení nepodporují čísla nad 1005, navíc tyto VLANy nejsou přenášeny pomocí VTP (VLAN Trunking Protocol) a neukládají se do VLAN databáze.

VLANy	Popis
0 a 4095	Rezervované pro systémové použití
1	Defaultní VLAN; standardně obsahuje všechny porty; nedá se smazat; pro switch
2-1001	Běžný rozsah pro ethernetové VLANy
1002-1005	Speciální defaultní VLANy pro Token Ring a FDDI; nedají se smazat
1006-4094	Extended VLAN – rozšířené VLANy pro ethernet; nejsou vždy podporovány

Zařazení do VLAN

Přiřazení do VLANy se nastavuje typicky na switchi (pouze v některých speciálních případech přichází označená komunikace přes trunk z jiného zařízení). Na switchích, které podporují VLANy, vždy existuje alespoň jedna VLANa. Jedná se o defaultní VLAN číslo 1, kterou není možno smazat či vypnout. Pokud se nenastaví jinak, tak jsou všechny porty zařazeny do VLAN 1.

Pro zařazení komunikace do VLANy existují čtyři základní metody, ale v praxi je nejvíce využívána možnost první - zařazení dle portu.

Zařazení dle portu

Port switche je ručně a napevno zařazen (nakonfigurován) do určité VLANy. Veškerá komunikace, která přichází přes tento port, spadá do zadané VLANy. To znamená, že pokud se do portu připojí další switch, tak všechny zařízení připojená k němu budou v jedné VLANě. Jedná se o nejrychlejší a nejpoužívanější řešení. Není třeba nic vyhodnocovat pro zařazení do VLAN. Definice zařazení do VLAN je lokální na každém switchi. Jednoduše se spravuje a je přehledné.

Lze do VLAN zařazovat podle Mac adresy, síťového protokolu nebo síťových adres uzlů, skupinového IP vysílání.

Provedení

Princip je jednoduchý, k Ethernetovému paketu se ještě připojí značka, která určuje do které VLANy daný paket patří.

Při vstupu do switche se pakety vždy otagují, při výstupu ze switche se buď odtagují a nebo ne, podle toho v jakém modu je daný port nastaven.

VLANy používají dva druhy portu: Access a Trunk

Značení portu

Fyzické porty switche se označují (adresují) typem, dnes hlavně FastEthernet, GigabitEthernet, TenGigabitEthernet, a číslem portu. Číslo portu je řetězec, který má tvar {slot}/{port}. Běžné (nemodulární) switche jsou brány, jako by byli ve slotu 0.

Switch port může pracovat v jednom z následujících módů

- **Access** – typicky pro koncové zařízení (PC, server, tiskárna…), přijímá netagované pakety (bez určení VLANy) a zařazuje je do té VLANy, kterou má nastavenu
- **Trunk** – jiný switch či aktivní prvek, komunikace je tagována a přenáší se vybrané VLANy
- Dynamic – vyjednává o stavu portu (access nebo trunk) pomocí protokolu DTP
- Tunnel – využívá IEEE 802.1q tunneling pro přenos informace o VLANě přes síť ISP

Access mode

Defaultní mód switch portu. Pokud je port v přístupovém módu, měl by být zařazen do správné VLANy. Může být členem pouze jedné VLANy, ve výchozím stavu jsou všechny porty ve VLAN 1.

```
SWITCH(config-if)#switchport access vlan 100
```

Mimo manuálního zařazení portu do VLANy lze také využít dynamické zařazení pomocí VLAN Membership Policy Server (VMPS).

Pokud na access port dorazí tagovaný paket (s označenou VLANou pomocí ISL nebo 802.1q), tak je zahozen.

Standardní hodnota MTU (Maximum Transmission Unit) pro Ethernet je 1518 B, (1500B velikost paketu + 18B hlavička a zakončení rámce). Když se použije IEEE 802.1q, tak může přijít rámec o 4B větší, tedy 1522B, když se použije ISL, tak o 30B větší, což je 1548B. Pokud port není nastaven jako trunk a přijde takto velký rámec, tak se zahodí a hlásí se jako Giant (Jumbo frame). V počítadlech pro interface se giant pakety zobrazují.

Trunk mode

Slouží primárně k tomu, aby šlo propojit více switchů mezi sebou a komunikace zůstala ve správné VLANě. Dnes se také často používá pro připojení některých serverů, které potřebují komunikovat do více VLAN. Pokud by se switche propojili Access portem, tak by se přenášela pouze komunikace ve VLANě, ve které by byl nastaven daný port a na druhém switchi by byl paket ve VLANě tohoto portu.

Pokud je port v Trunk módu, je bodů pro konfiguraci více. U vyšších modelů switchů (obecně L3 switchů a výše) se volí metoda, která se k paketům doplňuje informace o zařazení do VLANy. K dispozici je

- **IEEE 802.1q** – standardizovaná metoda, kterou podporují všechny switche. Funguje na principu tagování, do hlavičky paketu přidá 4B informaci (2B – 0x8100 = je to 802.1q/802.1p, 2B – priorita + číslo VLANy) a přepočítá CRC. Používá se také pro QoS.
- **Cisco ISL** – Cisco proprietární metoda, kterou podporují pouze vyšší řady switchů. Vezme celý původní paket a zabalí jej (encapsulate) jako obsah nového paketu. Přidává tedy 30B k obsahu.

Následně lze určit, které VLANy se mají přenášet v daném trunku. Defaultně se přenáší všechny, ale kvůli bezpečnosti a provozu se některé VLANy omezují. Zadáním čísla VLANy (nebo čísel oddělených čárkou či rozsah s pomlčkou) se nastaví a předchozí hodnoty se smažou.

```
SWITCH(config-if)#switchport trunk allowed vlan 100,200
SWITCH(config-if)#switchport trunk allowed vlan add 300
```

Souvisejícím údajem je nastavení nativní VLANy, ta slouží k přenosu paketů, které nebyly zařazeny do žádné VLANy. Jinak řečeno, pokud se do portu, který je nakonfigurován jako trunk, připojí normální stanice (která nepodporuje trunk), tak bude komunikovat v této VLANě. Ve výchozím nastavení je to VLAN 1. Důležité je, aby na obou stranách trunku byla nastavena stejná nativní VLANa.

Nastavení portu pro uživatele

Enable → conf t → interface faX/X → shutdown (je lepší, aby port byl vypnutý) → SWITCHPORT MODE ACCESS → DESCRIPTION cosi → no shutdown

Nastavení portu pro propojení mezi switchi – trunk

Enable → conf t → interface faX/X → shutdown (je lepší, aby port byl vypnutý) → SWITCHPORT MODE TRUNK allowed vlan 2-2OO → SWITCHPORT TRUNK native vlan 1 → SWITCHPORT MODE TRUNK → SWITCHPORT NONEGOTIATE (Vypnutí DTP protokolu) → DESCRIPTION cosi → no shutdown