# 6. VLAN a ACL

## Teoretická část

**Popište a vysvětlete teorii VLAN, jejich použití, včetně důvodu jejího vzniku a výhody VLAN. Vysvětlete, jakým způsobem pracuje a jak VLAN rozdělujeme (podle čeho se řídí).** **Popište, jak funguje komunikace VLAN v rámci jednoho či více switchů.  
Popište, k čemu slouží** **a jak funguje ACL (Access control list).** **Kde byste ho použili?** Existuje podobná funkce? Pokud ano, jaká?

## Praktická část

1. **Vyberte jeden ze způsobů tvorby VLAN a nakreslete 2 VLAN na 1 switch.**
2. **Vyberte jeden ze způsobů tvorby VLAN a nakreslete 2 VLAN na 2 switche.**
3. **Nakreslete použití routerů ve třech VLAN, následně popište způsob funkce.**
4. V Excel dokumentu předveďte tvorbu VLAN IP pool.

## Doplňující otázky

1. **K čemu slouží Trunk port?**
2. **Kdy a k čemu použijeme IEEE 802.1q? (tagging)**

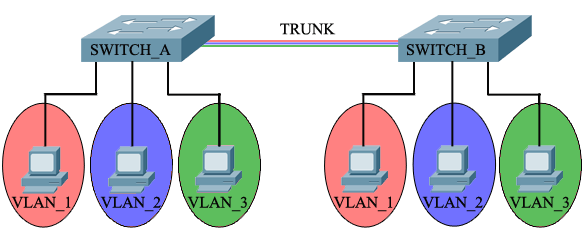
# VIRTUÁLNÍ LOKÁLNÍ SÍTĚ

Virtuální LAN (zkráceně VLAN) slouží k logickému rozdělení sítě nezávisle na fyzické topologii. Můžeme tedy síť segmentovat na menší podsítě uvnitř fyzické struktury původní sítě. Pomocí VLAN můžeme dosáhnout stejného efektu, jako když máme skupinu zařízení připojených do jednoho přepínače a druhou skupinu do jiného přepínače, tím vzniknou dvě nezávislé sítě, které spolu nemohou komunikovat, protože jsou fyzicky oddělené. Díky této technologii můžeme takovéto dvě sítě vytvořit na jednom nebo několika propojených přepínačích. Jde o dělení sítě už na úrovni 2. vrstvy ISO/OSI modelu.

## Zařazení do VLAN

Přiřazení do VLAN se nastavuje typicky na přepínači (pouze v některých speciálních případech přichází označená komunikace přes trunk port z jiného zařízení). Na přepínačích, které podporují VLAN, vždy existuje alespoň jedna výchozí VLAN číslo 1, kterou není možno smazat či vypnout. Pokud nenastavíme jinak, tak jsou všechny porty a tedy veškerá komunikace zařazena do VLAN 1. Stanice v rámci virtuální sítě nejsou vázány na fyzické umístění, ale jsou seskupovány do celků podle potřeby, i když fyzicky mohou být v různých segmentech sítě. Pro zařazení komunikace do VLAN existují čtyři základní metody:

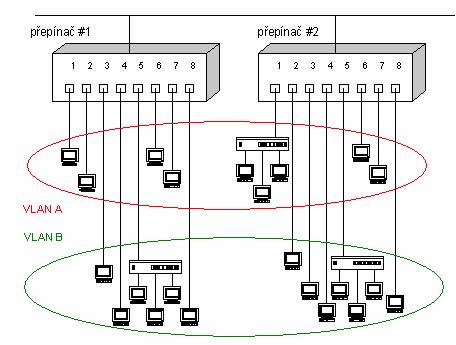
* podle portů,
* podle fyzické MAC adresy,
* podle IP adresy
* podle skupinové adresy (multicast).



## Přiřazení podle portů

Rozdělení zařízení do jednotlivých VLAN je provedeno na základě čísel portů pří- slušných přepínačů.

Podle obrázku porty 1,2,6 a 7 přepínače A a porty 1,6 a 7 přepínače B tvoří VLAN A, porty 3,4,5,8 přepínače A a porty 2,3,5,8 přepínače B tvoří VLAN B. Porty přepínače jsou napevno zařazeny do určité VLAN. Veškerá komunikace, která přichází na tyto porty, spadá do zadané virtuální LAN sítě. To znamená, že pokud do portu připojíme další přepínač, tak všechny zařízení připojená k němu budou v jedné virtuální LAN síti. Jedná se o nejrychlejší a nejpoužívanější řešení, není třeba nic vyhodnocovat pro zařazení do VLAN.



## Přiřazení podle MAC adresy

Rámce respektive porty se zařadí do VLAN podle zdrojové MAC adresy koncového zařízení. Musíme tedy spravovat tabulku se seznamem MAC adres pro každé zařízení spolu s číslem sítě VLAN. Výhodou je, že se jedná o dynamické zařazení, takže pokud přepojíme zařízení do jiného portu, automaticky se zařadí do správné virtuální lokální sítě.

Existují zde dvě možnosti, jak tato metoda funguje. Buď se podle zdrojové MAC adresy prvního rámce nastaví zařazení portu do příslušné VLAN a toto nastavení zůstane, dokud se port nevypne nebo se každý rámec zařazuje samostatně do VLAN podle MAC adresy, toto řešení je však velmi náročné na výkon.

## Přiřazení podle IP adresy

Takto definované virtuální sítě jsou založeny na informacích ze síťové vrstvy podle ISO/OSI modelu. V multiprotokolových sítích mohou být přiřazeny uzly do jednotlivých VLAN podle provozovaných síťových protokolů nebo např. v sítích TCP/IP podle IP adresy nebo rozsahu. Zařízení musí mít napevno definovanou IP adresu a přepínač se musí dívat do třetí vrstvy, to způsobí zpomalení průchodu rámce přepínačem.

Způsob definice VLAN podle síťové vrstvy má také zřejmé výhody. Patří mezi ně mobilita uživatelů či přesněji řečeno jejich stanic bez nutnosti překonfigurování členství ve VLAN, možnost vytváření skupin specifických pro jistou službu nebo aplikaci a eliminaci potřeby značkování rámců informací o členství ve VLAN při vzájemné komunikaci přepínačů.

## Přiřazení podle multicastové adresy

Multicast je členství podle skupinového adresování. Skupinově adresovaný paket (IP adresa třídy D) je zasílán na všechny členy dynamicky vytvořené skupiny. Členství ve skupině se vytváří tak, že uzel kladně odpoví na oznámení existence skupiny. Skupina pak tvoří dynamickou VLAN síť, ze které se uzly skupiny průběžně přihlašují a odhlašují.

# Proč vznikly VLANy

Technologie VLAN začala vznikat kolem roku 1995, ale zprvu se jednalo o různá proprietární řešení. V praxi se však více rozšířili až před několika lety a to hlavně ve středních a velkých firmách, přestože již delší dobu existuje standard.

Hlavní důvody proč vznikly VLAN byly asi tyto:

* 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

Idea pro logické seskupování uživatelů, která se uvádí v řadě materiálů, a tedy vytváření VLAN je:

* podle organizační struktury - pokud je většina komunikace v rámci oddělení, kde jsou vlastní tiskárny, file servery, atd. a mezi jednotlivými odděleními není komunikace, pouze pár služeb (mail) je společných pro všechny
* podle služeb - do VLAN se seskupují pracovníci, kteří využívají stejné služby (účetnictví, DB, atd.)

# Jaké jsou praktické výhody VLAN

* **Snížení broadcastů -** hlavní výhodou VLAN je vytvoření více, ale menších, broadcastových domén. Tedy zlepšení výkonu sítě snížením provozu (traffic).
* **Zjednodušená správa -** k přesunu zařízení do jiné sítě stačí překonfigurovat zařazení do VLANy, tedy správce konfiguruje 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.
* **Oddělení speciálního provozu -** dnes se používá řada provozu, který nemusí být propojen do celé sítě, ale přesto jej potřebujeme dostat na různá místa, navíc nechceme, aby nám ovlivňoval běžný provoz. Příkladem je například IP telefonie, komunikace mezi AP v centrálně řízeném prostředí, management (zabezpečení správcovského přístupu k zařízením). Například pro IP telefonii, kde je použití VLAN naprosto běžné, nám stačí jediná zásuvka, kam přivedeme VLAN pro telefonii i VLAN s přístupem do sítě a v telefonu se komunikace rozdělí. Navíc VLANy můžeme použít spolu s QoSem pro zaručení kvality komunikace (obsazení pásma).
* **Snížení HW -** samozřejmě se nám nesnižuje potřebný počet portů (až na speciální případy jako IP telefonie), ale tím, že mohou být různé podsítě na stejném switchi, jej můžeme lépe využít (například pro propojení tří zařízení nepotřebujeme speciální switch, který má minimálně 8 portů).

# Jak funguje komunikace v rámci VLAN

V praxi máme dvě situace, kdy se při komunikaci řeší příslušnost k VLANě. Je to při komunikaci v rámci jednoho switche nebo při komunikaci mezi několika switchi.

## VLANy na jednom switchi

Při komunikaci ve VLAN v rámci *jednoho switche* je to jednoduché. Switch si v operační paměti udržuje informace, do které VLANy patří daná komunikace (port), a v rámci switche povoluje pouze správné směrování. V tomto případě máme jednotlivé porty zařazeny do jedné VLANy a to buď staticky, nebo dynamicky, jak bylo řečeno výše (možnosti 2,3,4). Cisco těmto portům říká *access port* (přístupový port).

## VLANy mezi více switchi

Složitější situace nastává, když chceme, aby se informace o *zařazení do VLANy* neztratila při přechodu na jiný switch, tedy abychom v celé naší síti mohli využít stejné VLANy a nezáleželo, do kterého switche je zařízení připojeno. Navíc chceme, aby tato metoda fungovala i mezi switchi různých výrobců. To byl ze začátku problém a používali se různé metody. Například, když zařazujeme komunikaci podle MAC adresy, tak můžeme tabulku přiřazení mít na všech switchích.

Naštěstí vznikl standard **IEEE 802.1q**, který využívá značkování rámců. Označuje se komunikace jen ve chvíli, kdy je to třeba. Takže dokud probíhá v rámci jednoho switche a připojených zařízení, tak se nic nepřidává. Teprve, když chceme poslat komunikaci dalšímu switchi (či podobnému zařízení), tak ji označíme. Odchozí komunikace se taguje na portu, kterému se říká *trunk port*. Tento port přenáší více (vybraných) VLAN a aby je mohl odlišit, tak je označuje. Spoji dvou trunk portů se říká **trunk** nebo *trunk link*.  
**Trunk = Spojení dvou switchů**; přes tuto linku běhají pakety VLANu (Pokuď se ze SW1 posílá packet na SW2).

# IEEE 802.1q tagging

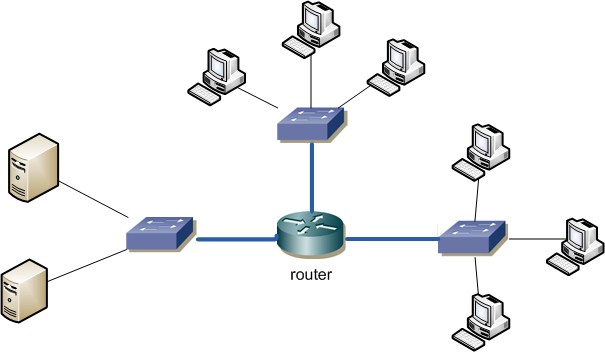
Protokolu **IEEE 802.1q** se říká také *trunking protokol* nebo *dot1q* *tagging*. Jedná se o standardizovanou metodu, kterou podporují všechny moderní switche s podporou VLAN. Funguje na principu tzv. tagování. Vezmeme originální rámec, jeho hlavičku rozšíříme o 4B informací, z nichž první je značka, že se jedná o protokol 802.1q. Dále následuje priorita dle protokolu 802.1p, příznak, zda je MAC adresa v kanonickém tvaru a poslední je číslo VLANy.

## Trunk port

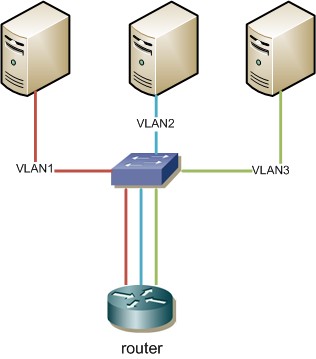
Trunk je propojení, které slouží ke komunikaci mezi více VLAN sítěmi současně. Jedná se tedy o přenos rámců ze zařízení, které je ve VLAN síti na jednom přepínači, do zařízení patřícího do stejné sítě na druhém přepínači. Rámec však pro tento přenos musí obsahovat zmínku o síti VLAN, což žádný z protokolů nad 2.vrstvou ani žádný z ethernetových protokolů nepodporuje. Proto byly vytvořeny protokoly ISL (InterSwitch Link), jenž je přímo protokolem firmy Cisco a 802.1Q, vyvinutý organizací IEEE, které tuto úlohu plní.

# Routing mezi VLANy

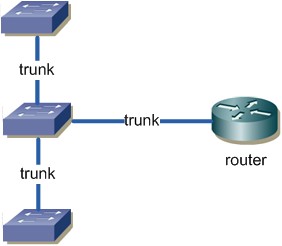
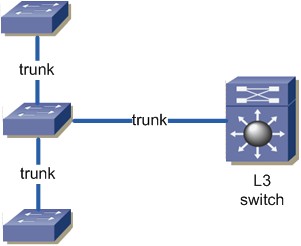
Tradiční routing vypadá tak, že máme několik oddělených sítí a chceme mezi nimi umožnit nějakou komunikaci. Následující obrázek představuje tři samostatné switche propojené pomocí routeru. Může se jednat například o firemní servery a dvě oddělení, které k nim chceme připojit, ale nechceme, aby mohla komunikovat mezi sebou.



Pokud využíváme VLAN, můžeme se k nim chovat stejně jako k normálním podsítím. Na switchi můžeme jednotlivé VLANy, které chceme routovat, vyvést do samostatných access portů a ty připojit k routeru.



To je však zbytečné plýtvání a výhodnější je použít mezi routrem a switchem trunk. Také můžeme místo klasického routeru využít L3 switch, který je rychlejší.

# Access control list

ACL (access control list, seznam pro řízení přístupu) je v oblasti [počítačové bezpečnosti](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_bezpe%C4%8Dnost) seznam oprávnění připojený k nějakému objektu (např. [souboru](https://cs.wikipedia.org/wiki/Soubor)). Seznam určuje, kdo nebo co má povolení přistupovat k objektu a jaké operace s ním může provádět. V typickém ACL specifikuje každý záznam v seznamu uživatele a operaci.   
Například: Záznam v ACL [Pepa, smazat] pro soubor XYZ dává uživateli Pepa právo smazat soubor XYZ.

U bezpečnostního modelu používajícího ACL tak systém před provedením každé operace prohledá ACL a nalezne v něm odpovídající záznam, podle kterého se rozhodne, zda operace smí být provedena.

Na aktivních prvcích Cisco jsou ACL vlastností IOSu. Můžeme je používat na několika místech, ale nejčastější použití je pro řízení (omezování) síťového provozu, tedy pro filtrování paketů.

Mezi typické představitele paketových filtrů patří např. tzv. [ACL](https://cs.wikipedia.org/wiki/Access_control_list) (Access Control Lists) ve starších verzích operačního systému [IOS](https://cs.wikipedia.org/wiki/Cisco_IOS)

## ACL slouží hlavně

* jako základní síťová bezpečnost k blokování nebo povolení (routovaného) provozu
* ke kontrole šířky pásma
* Policy Based Routing
* vynucení síťových politik
* identifikaci nebo klasifikaci provozu (pro QoS, NAT, apod.)

## Stručná charakteristika a vlastnosti

* ACL je sekvenční (řazený) seznam pravidel **permit** (povolit) a **deny** (zakázat), těmto pravidlům se říká **ACE**(Access Control Entries).
* ACL můžeme identifikovat **číslem** nebo **jménem** (pojmenované ACL).
* Nová pravidla se přidávají vždy na konec seznamu.
* Používá se pravidlo **first-fit**. Seznam se prochází od začátku ke konci, a pokud dojde ke shodě, tak se dále neprochází.
* Každý neprázdný seznam má na konci **defaultní pravidlo**, které zakazuje vše (deny any). Prázdný seznam povoluje vše.
* Je dobré umísťovat více specifická pravidla na začátek a obecná (subnety apod) na konec.
* Pokud se v ACL vyhodnotí deny, tak se odešle ICMP host nedosažitelný (unreachable).
* Filtrování (používání ACL) zpomaluje zařízení (stojí výpočetní výkon).
* Odchozí pravidla (outbound filters) neovlivňují provoz, který pochází lokálně z routeru (filtrují pouze procházející provoz).

## Typy ACL

Nejpoužívanější je dělení ACL na dva typy

* **standard ACL** - starší a jednodušší verze ACL s méně možnostmi konfigurace

**Příklad:**Následující ACL s číslem 5 povoluje přístup subnetu 10.5.1.0/24 mimo adresy 10.5.1.10, všechny ostatní adresy jsou zakázány.

SWITCH(config)#**access-list 5 deny host 10.5.1.10**

SWITCH(config)#**access-list 5 permit 10.5.1.10 0.0.0.255**

SWITCH(config)#**access-list 5 deny any**

* **extended ACL** - novější a složitější ACL s více možnostmi

**Příklad:**

ACL číslo 105 povoluje přístup na server 10.5.1.10 odkudkoliv, ale pouze na port 80 (tedy http) a ping.

SWITCH(config)#**access-list 105 permit tcp any host 10.5.1.10 eq 80**

SWITCH(config)#**access-list 105 permit icmp any any echo**

SWITCH(config)#**access-list 105 permit icmp any any echo-reply**

SWITCH(config)#**access-list 105 deny ip any any**

# ACL a VLAN Map

*VLAN mapy* slouží k řízení (omezování a povolování) provozu v rámci VLAN. Pomocí *VLAN map* se kontroluje veškerý provoz, který vstupuje do VLAN (třeba přes port nebo z jiné VLAN) a může být zakončený ve stejné VLAN nebo jiné. Takže se pomocí něj kontroluje, jak *routovaný provoz* (L3, na který se jinak používá Router ACL), tak i *bridgovaný - switchovaný provoz* (L2, pro který máme Port ACL). Provoz může být kontrolovaný na základě *IP* nebo *MAC adres*.

VLAN Map je podobná funkce ACL.