Obsah

Virtuální lokální sítě (VLAN)

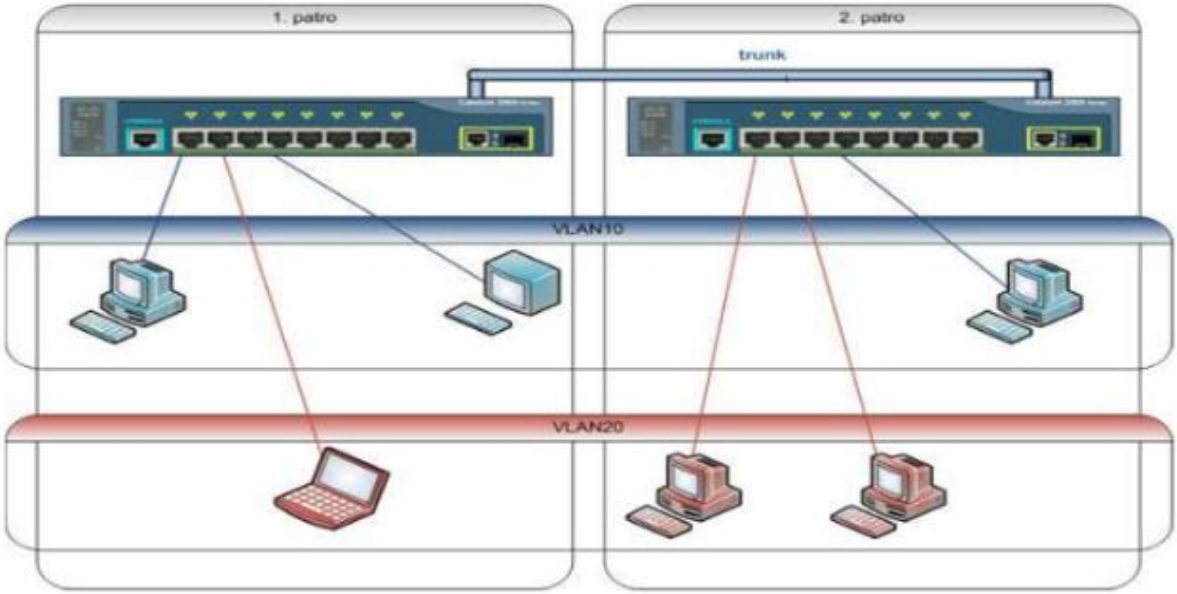
(Video vysvětlující VLAN)

- Slouží k logickému rozdělení sítě nezávisle na fyzickém uspořádání. Můžeme tedy naši síť segmentovat na menší sítě uvnitř fyzické struktury původní sítě.

Spoji dvou *trunk portů* se říká ***trunk*** nebo ***trunk link***.
trunk = port, který je zařazen do více VLAN

- Jednoduše řečeno pomocí VLAN můžeme dosáhnout stejného efektu, jako když máme skupinu zařízení připojených do *jednoho switche* a druhou skupinu do *jiného switche*. Jsou to dvě nezávislé sítě, které spolu nemohou komunikovat (jsou fyzicky odděleny).
    - Pomocí VLAN můžeme takovéto dvě sítě vytvořit na ***jednom switchi***.

- V praxi je často potřeba komunikace i mezi těmito sítěmi. S VLAN můžeme pracovat stejně jako s normálními sítěmi. Tedy použít mezi nimi **jakýkoliv způsob routování**.



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

Podsíť – subnet

- CP/IP protokol používá pro adresování zařízení IP adresy. Těchto adres je určitý rozsah, který se pro praktické použití (směrování, přidělování adres organizacím, broadcasty) dělí na menší hierarchické části, kterým se říká subnety (podsítě).
- Zařízení mohou přímo komunikovat pouze s dalšími zařízeními, která jsou ve stejném subnetu. Se zařízeními z jiných subnetů komunikují typicky přes jednu adresu – gateway (bránu), která provádí routování.

Subnety a VLAN

- Z výše uvedeného také plyne to, že pro různé VLAN bychom měli používat různé subnety. Pokud chceme mezi těmito VLAN routovat, tak je to nutné, stejně jako v případě, kdy chceme využít některé speciální funkce na switchi.

Komunikace VLAN

- Přiřazení do VLAN se nastavuje typicky na switchi (pouze v některých speciálních případech přichází označená komunikace přes *trunk* z jiného zařízení).
- Na switchích, které podporují VLAN, vždy existuje alespoň jedna VLAN. Jedná se o defaultní VLAN číslo 1, kterou není možno smazat či vypnout. Pokud nenastavíme jinak, tak jsou všechny porty (tedy veškerá komunikace) zařazeny do VLAN 1. Pro zařazení komunikace do VLAN existují čtyři základní metody, ale v praxi je nejvíce využívána možnost první – zařazení dle portu.

1. podle portu

- Port switche je *ručně a napevno zařazen* (*nakonfigurován*) do určité VLAN.
- Veškerá komunikace, která přichází přes tento port, spadá do zadané VLAN. To znamená, že pokud do portu připojíme další switch, tak všechny zařízení připojená k němu budou v jedné VLAN.
- 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.

2. podle MAC adresy

- Rámce(port) se zařadí do VLAN *podle zdrojové MAC adresy*.
- Musíme tedy spravovat tabulku se seznamem MAC adres pro každé zařízení spolu s VLAN.
- Výhodou je, že se jedná o *dynamické zařazení*, takže pokud přepojíme zařízení do jiného portu, automaticky se zařadí do správné VLAN (Switch musí vyhledávat v tabulce MAC adres).
- jsou zde dvě možnosti, jak tato metoda může fungovat:
  - Buď se podle MAC adresy prvního rámce nastaví zařazení portu do VLAN a toto nastavení zůstane, dokud se port nevypne.
  - Nebo se každý rámec zařazuje samostatně do VLAN podle MAC adresy. Toto řešení je velmi náročné na výkon.

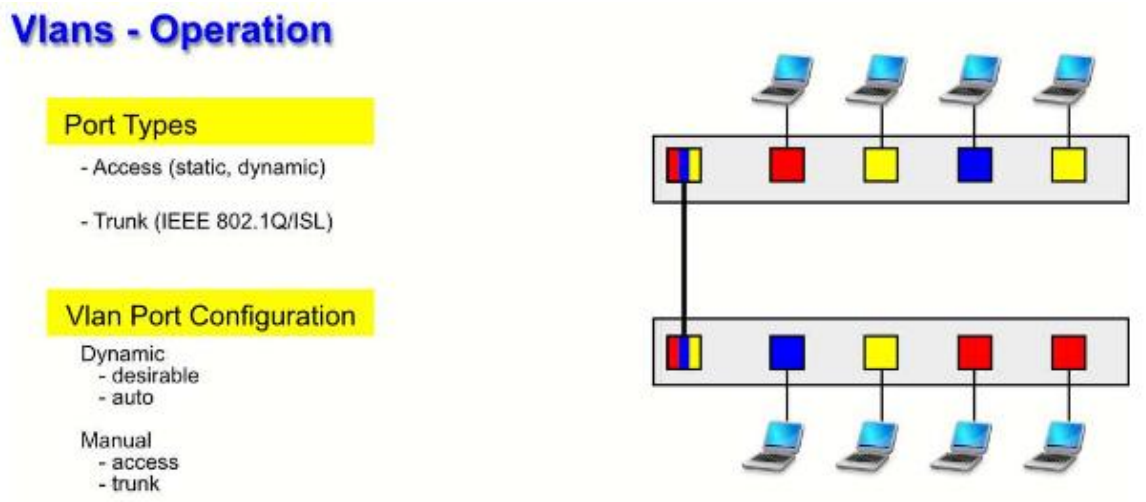
3. podle protokolu = podle informace z 3. vrstvy

- Tato metoda určuje zařazení podle protokolu přenášeného paketu.
- Například oddělíme IP provoz od AppleTalk. Nebo zařazujeme podle IP adresy či rozsahu.
- V praxi není příliš rozšířené.
- Zařízení musí mít napevno definovanou IP adresu a switch se musí dívat do třetí vrstvy (normálně funguje na druhé), znamená to zpomalení.

4. podle autentizace

- Ověří se uživatel nebo zařízení pomocí protokolu IEEE 802.1x a podle informací se automaticky umístí do VLAN.

- Je to primárně bezpečnostní metoda, které řídí přístup do sítě (NAC), ale po rozšíření slouží i pro VLAN.
- Obsahuje také mapovaní uživatelů na VLAN a tuto informaci zašle po úspěšné autentizaci.
- Je velmi univerzální.



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

VLAN na jednom switchi

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

VLAN mezi více switchi

- Složitější situace nastává, když chceme, aby se informace o zařazení do VLAN neztratila při přechodu na jiný switch, tedy abychom v celé naší síti mohli využít stejné VLAN a nezáleželo, do kterého switche je zařízení připojeno.
- Navíc chceme, aby tato metoda fungovala i mezi switchi různých výrobců.

  - Cisco vytvořilo svoji metodu **ISL**, která zapouzdřuje celý rámec, ale funguje pouze na Cisco zařízeních.

  - Proto 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.

Praktické výhody VLAN

1. snížení broadcastů
    - Hlavní výhodou VLAN je vytvoření více, ale menších, broadcastových domén.
    - Tedy zlepšení výkonu sítě snížením provozu (traffic).

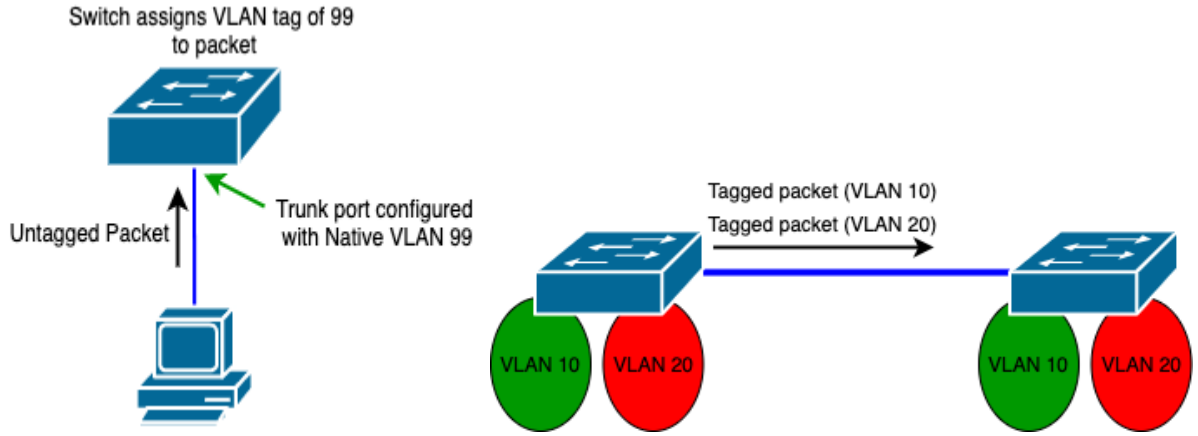
2. zjednodušená správa
    - K přesunu zařízení do jiné sítě stačí překonfigurovat zařazení do VLANy, tedy správce konfiguruje SW (zařazení do VLAN) a ne HW (fyzické přepojení).

3. 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.

4. 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]).

5. 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).

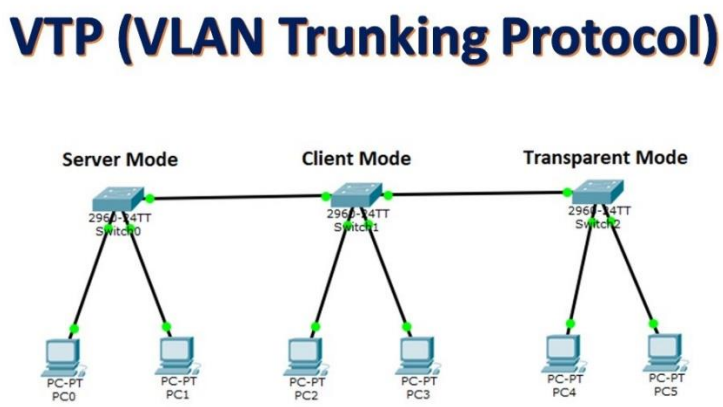
Nativní a tagované pakety

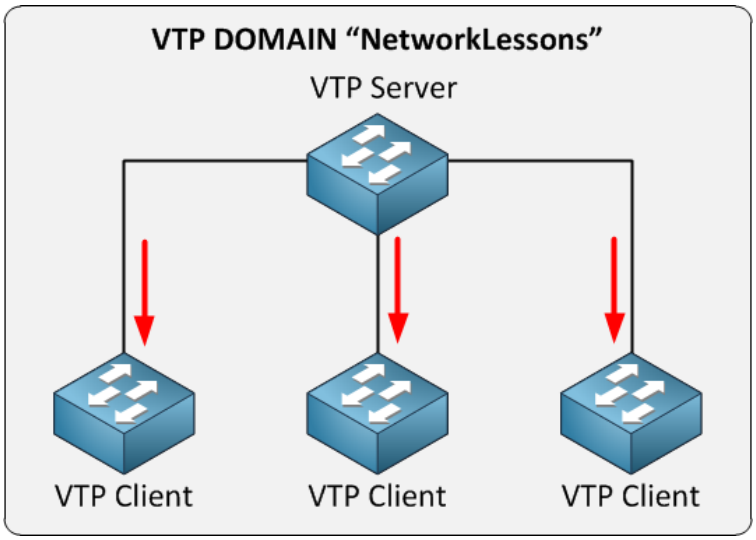


VLAN Trunking Protocol

(Video vysvětlující VTP)

- VLAN Trunking Protocol (VTP) je *proprietární síťový protokol společnosti Cisco*, který zajišťuje přenášení čísel a názvů virtuálních LAN (VLAN) mezi přepínači (switch) zařazených do jedné domény, což usnadňuje jejich správu.
- Protokol VTP je dostupný na většině Cisco přepínačích typu Catalyst.





- Při návrhu zvolí správce sítě ***jeden z přepínačů*** jako *server*, ostatní mohou typu *client* nebo *transparent*, a také zvolené přepínače přiřadí do domény, která je označena textovým řetězcem.
- Jakákoliv změna v nastavení VLAN na přepínači typu *server* (přidání, přejmenování, smazání), **je přenesena na ostatní přepínače ve stejné doméně** – přepínače typu *client* tyto změny použijí na svou tabulku VLAN v paměti.
- Přepínače typu *transparent* je jen rozešlou na další přepínače.
- U přepínačů *client* **nelze vytvářet VLAN, ani měnit existující**.

- ***synchronizace jednotlivých přepínačů:***
    - Je zabezpečena *číslem revize*, což je 32bitové číslo, které vytváří přepínač typu server.
    - Při vytvoření či změně názvu domény je nastaveno na nulu, o jedničku je zvětšen jakoukoliv změnou VLAN.

- Přepínače mezi sebou komunikují zasíláním tří druhů paketů na *multicastovou MAC adresu* 01-00-0C-CC-CC-CC:
    1. Summary advertisements
        - Tento paket je zasílán ve výchozím nastavením *každých pět minut* a obsahuje *jméno domény, číslo revize a čas poslední změny*.
        - Při obdržení této zprávy přepínač **zkontroluje**, zda paket obsahuje **stejný** *název domény* jako přepínač a také, zda *číslo revize je vyšší než číslo revize z poslední obdržené Summary advertisements*.
        - V takovémto případě odešle zpět paket *Advertisement requests*, jinak zprávu ignoruje.
        - Tyto zprávy je možno *zaheslovat*, pro správnou funkci je potřeba, aby na všech přepínačích v jedné doméně bylo nastaveno **stejné heslo**.

    2. Subset advertisements
        - Je odesílán směrem ze *serveru* na *klienta* v případě změn provedených v nastavení VLAN na serveru.
        - Obsahuje *název domény, číslo revize a informace o jedné nebo více VLAN* – číslo, stav (aktivní/neaktivní), jméno a velikost MTU (Maximum transmission unit).

    3. Advertisement requests
        - Paket přepínač zasílá, pokud byl *resetován, správce změnil doménové jméno nebo jako odpověď na paket Summary advertisements*, který obsahoval **vyšší číslo revize**.
        - Přepínač, který tuto zprávu obdrží, odešle zpět *Summary advertisements* následovaný *Subset advertisements*.

- Další funkcí protokolu je *VTP Pruning*, který zabrání zbytečnému odesílání všesměrových (broadcast) paketů z určité VLAN na přepínače, které *nemají* aktivní žádné zařízení na této VLAN.
- Tuto funkci je potřeba aktivovat pouze na přepínači typu *server*, na ostatní ve stejné doméně je toto nastavení přeneseno *automaticky.*

Směrování mezi VLANy

- Defaultně je switch v módu L2 switchování, pokud chceme použít L3 vlastnost IP routing, tak ji musíme zapnout.

SWITCH(config)#ip routing

- Nepotřebujeme použít žádný routovací protokol, protože veškeré routování se odehrává na jednom zařízení. Cisco IOS automaticky vkládá přímo připojené interfacy do routovací tabulky.
- Pokud je zapnuto routování, tak IOS routuje podle záznamů v routovací tabulce, což jsou statické routy a přímo připojené interfacy. To je výhoda inter-VLAN routingu, že pro základní funkcionalitu není třeba téměř žádná konfigurace.
- VLAN interfacy jsou na core switchi přímo připojené interfacy, mezi kterými se provádí routování automaticky.
- Musíme pouze pro VLANy, které chceme routovat, vytvořit VLAN interface a nastavit mu IP adresu. IP adresa je stejně nutná, protože se jedná o gateway (bránu) pro daný subnet.

Příklad:

- následující příklad vytváří VLAN interface pro VLAN 100, která má subnet 10.0.1.0/24 a chceme adresu gateway 10.0.1.1. VLAN 100 již máme vytvořenou:

```
- SWITCH(config)#interface vlan 100

- SWITCH(config-if)#ip address 10.0.1.1 255.255.255.0  // zadání
  IP adresy spolu s maskou, která určuje subnet

- SWITCH(config-if)#no shutdown                         // výchozí
  stav interface je vypnutý
```

- Ještě je vhodné nastavit default gateway, pokud chceme komunikovat třeba do internetu, aby router věděl, kam poslat provoz, který nepatří do žádné z jeho VLAN. Možností nastavení je několik, ale první možnost je pouze pro úplnost, tu nemůžeme použít!

```
SWITCH(config)#ip default-gateway 10.0.1.250          // mohu použít,
pouze pokud není zapnuto routování

SWITCH(config)#ip default-network 10.0.1.0            // nastaví
defaultní síť, při používání routování

SWITCH(config)#ip route 0.0.0.0 0.0.0.0 10.0.1.250    // nejčastější
metoda, vytvořím přímo záznam do routovací tabulky
```

Omezení routování a neroutované VLANy

- neroutovaná VLAN – chceme mít izolovanou VLAN, tady naprosto neroutovanou s ostatními VLANami, buď funguje jako uzavřená síť nebo ji dále propojujeme pomocí firewallu či jiné GW omezeně.

- routovaná VLAN – chceme, aby jedna VLAN mohla komunikovat pouze s některými dalšími, případně aby byla povolena pouze určitá komunikace.

Neroutovaná VLAN

- Vytvoříme izolovanou VLANu. Stačí, aby její VLAN interface neměl zadanou IP adresu (nemusí vůbec existovat či může být shutdown).
- Taková VLAN se neúčastní routovacího procesu.
- IP adresu potřebujeme mít na VLANě z několika důvodů, například když chceme v této VLANě přistupovat na switch (na jeho CLI nebo webové rozhranní) nebo když chceme využít přidělování IP adres z DHCP serveru na switchi (do této VLAN).

Omezeně routovaná VLAN pomocí ACL

- Pokud chceme, aby některá VLANa byla routována (mohla komunikovat) pouze s některými dalšími (a ne se všemi). Případně chceme ještě více specifikovat komunikaci mezi VLANami (nebo ji úplně zakázat).
- Můžeme použít Access Control List (ACL).
- Tyto ACL aplikujeme na VLAN interface na routeru (v našem případě core switchi), těmto ACL se říká Router ACL.

Příklady:

Vezmeme situaci, kde máme VLAN 100, VLAN 200 a přidáme ještě VLAN 300. Chceme, aby VLAN 100 komunikovala s VLAN 200 a VLAN 300, ale VLAN 300 komunikovala pouze s VLAN 100, stejně jako VLAN 200. Jinak řečeno plné routování, kde se VLAN 300 omezí pouze na komunikaci s VLAN 100.

```
SWITCH(config)#ip routing
SWITCH(config)#interface vlan 100
SWITCH(config-if)#ip address 10.0.1.1 255.255.255.0
SWITCH(config-if)#no shutdown
SWITCH(config)#interface vlan 200
SWITCH(config-if)#ip address 10.0.2.1 255.255.255.0
SWITCH(config-if)#no shutdown
SWITCH(config)#interface vlan 300
SWITCH(config-if)#ip address 10.0.3.1 255.255.255.0
SWITCH(config-if)#no shutdown
SWITCH(config)#ip access-list extended vlan300in
SWITCH(config-ext-nacl)#permit ip 10.0.3.0 0.0.0.255 10.0.1.0
0.0.0.255
SWITCH(config)#interface vlan 300
SWITCH(config-if)#ip access-group vlan300in in
```

Druhý příklad ukazuje možnost izolace jedné VLANy.

```
SWITCH(config)#ip access-list extended vlan300
SWITCH(config-ext-nacl)#deny ip any any
SWITCH(config)#interface vlan 300
SWITCH(config-if)#ip access-group vlan300 in
SWITCH(config-if)#ip access-group vlan300 out
```

VLAN:

- https://vcklan.cz/sesity/files/Maturita/Informatika/14-Zakladni%20nastaveni%20site%20TCPIP/File4.pdf
- https://docplayer.cz/5667460-Virtalni-lokalni-site-vlan.html

VTP:

- https://cs.wikipedia.org/wiki/VLAN_Trunking_Protocol

Směrování mezi VLANy:

- https://www.samuraj-cz.com/clanek/cisco-ios-18-inter-vlan-routing-a-acl-smerovani-mezi-vlany/