VLAN - Virtual Local Area Network

VLAN neboli virtuální lokální síť je v dnešní době běžná technologie, která přináší řadu výhod. Myslím, že všechny střední a větší firmy technologii VLAN používá a i pro malé firmy může být zajímavá. VLANy slouží k logickému členění sítě bez vazby na členění fyzické. V článku se pokouším popsat vše potřebné k pochopení toho, co to VLAN je, jaké jsou výhody a způsoby nasazení.

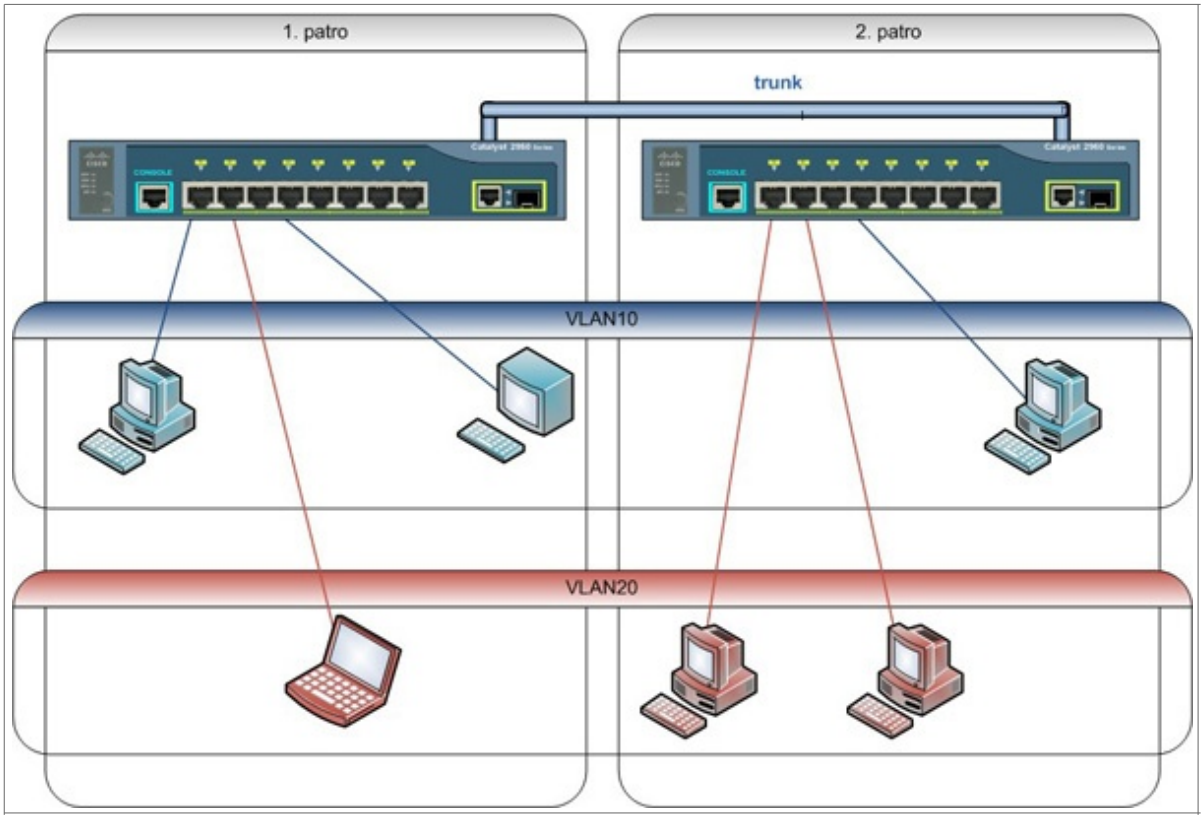
Co je to VLAN

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

Jednoduše řečeno pomocí VLAN můžeme dosáhnout stejného efektu, jako když máme skupinu 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 můžeme takovéto dvě sítě vytvořit na jednom (nebo několika propojených) switchi.

V praxi samozřejmě často potřebujeme komunikaci mezi těmito sítěmi. S VLAN můžeme 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.

Níže uvádím klasický obrázek, který se používá pro vysvětlení VLAN. 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.



Pro podrobné pochopení VLAN je třeba rozumět základům sítí a jejich segmentování (dělení na subnety - podsítě).

LAN

Počítačová síť vznikne ve chvíli, kdy dva (někdy se říká minimálně tři) nebo více počítačů propojíme dohromady pomocí telekomunikačního systému za účelem sdílení zdrojů. V praxi je dnes nejrozšířenější síť založena na technologii ***ethernetu*** a používá protokol ***TCP/IP***. Sítě se dále dělí podle řady parametrů na LAN, WAN, WLAN, MAN apod. V tuto chvíli nás zajímá ***lokální počítačová síť*** - LAN, která se vyznačuje tím, že počítače jsou propojeny na menším geografickém území (tedy v rámci firmy, budovy, místnosti, atp.).

Subnet

TCP/IP protokol používá pro adresování zařízení ***IP adresy***. Těchto adres je určitý rozsah, který se pro praktické použití 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.

Oddělení sítí

Jak jsem uvedl výše, pokud použijeme různé subnety, tak spolu zařízení nemohou komunikovat. Není to však úplně pravda, rozhodně nedojde k oddělení těchto zařízení. Pokud jsou totiž připojena na stejné médium, propojena do stejného hubu (pracuje na 1. vrstvě OSI) nebo switche (pracuje na 2. vrstvě OSI. Tak komunikace dorazí z jednoho zařízení na druhé, i když jsou v jiném subnetu. Zařízení však bude tuto komunikaci ignorovat. Je to proto, že hub (posílá všude) ani switch (používá MAC adresy) se nedívá na IP adresy procházející komunikace. Proto se dá tato komunikace zachytávat a odposlouchávat.

Kdežto použitím VLAN dojde k tomu, že komunikace se posílá pouze na porty, které jsou zařazeny do stejné VLANy. Záleží tedy sice na softwaru switche, ale dá se říct, že se jedná o fyzické oddělení. Existují nějaké metody útoky na VLAN (proniknutí do jiné VLAN), ale při dobře nastavené síti by mělo být vše bezpečné.

Subnety a VLANy

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

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.)

Původní důvody již dnes často nejsou aktuální nebo se z praxe změnily názory. Jak se používají VLANy dnes, jinak řečeno, jaký je jejich hlavní přínos, uvádím v další kapitole.

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, 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 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 se zařazuje komunikace do VLAN

Přiřazení do VLANy se nastavuje typicky na **switchi** (pouze v nějakých speciálních případech přichází označená komunikace přes trunk z jiného zařízení). Na switchích, které podporují VLANy, 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 VLANy 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 ***VLANy***. Veškerá komunikace, která přichází přes tento port, spadá do zadané VLANy. To znamená, že pokud do portu připojíme 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.

2. podle MAC adresy

Pakety (port) se zařadí do VLANy podle ***zdrojové MAC adresy***. Musíme tedy spravovat tabulku se seznamem MAC adres pro každé zařízení spolu s VLANou. Výhodou je, že se jedná o dynamické zařazení, takže pokud přepojíme zařízení do jiného portu, automaticky se zařadí do správné VLANy. Switch musí vyhledávat v tabulce MAC adres.

Jsou zde dvě možnosti, jak tato metoda může fungovat. Buď se podle MAC adresy prvního paketu nastaví zařazení portu do VLANy a toto nastavení zůstane, dokud se port nevypne. Nebo se každý paket zařazuje samostatně do VLANy podle MAC adresy. Toto řešení je velmi náročné na výkon.

Cisco má řešení zvané ***VLAN Membership Policy Server*** (VMPS), pro které je třeba speciální server, který spravuje tabulky MAC adres. Navíc se při této metodě zařazuje port do VLANy, takže pokud je do něj připojeno více zařízení (max. 20), musí být všechny ve stejné VLAN.

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 VLANy. Je to primárně bezpečnostní metoda, které řídí přístup do sítě (NAC), ale po rozšíření slouží i pro VLANy. Je to zajímavá metoda proto, že je velmi univerzální. Nezáleží ani na fyzickém zařízení ani na místě zapojení. RADIUS server, který ověřuje identitu uživatele, obsahuje také mapovaní uživatelů na VLANy a tuto informaci zašle po úspěšné autentizaci. U této metody je možné nastavení, že v případě, kdy není uživatel autentizován, tak je zařazen do speciální hostovské VLANy.

U Cisco switchů může být port single-host, kdy je možno připojit pouze jedno zařízení nebo multiple-host, kdy sice může být do portu připojeno více zařízení, ale ve chvíli, kdy se první autentizuje, tak je port autentizovaný (a zařazený do VLANy) a komunikovat mohou všechna zařízení.

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 VLANách 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. Cisco vytvořilo svoji metodu ISL, která zapouzdřuje celý paket, ale funguje pouze na Cisco zařízeních. Také můžeme propojit dva *access porty* na dvou switchích, zařadit je do stejné VLANy a přeneseme potřebné informace. To je ale velmi nepraktické.

Naštěstí vznikl standard **IEEE 802.1q**, který využívá značkování paketů. 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***.

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 paket, jeho hlavičku rozšíříme o 4B informací, z nichž první je značka, že se jedná o protokol 802.1q (hodnota 0x8100). Dále následuje priorita dle protokolu 802.1p, příznak, zda je MAC adresa v kanonickém tvaru a poslední je číslo VLANy.

Protože se změnili data, je třeba přepočítat kontrolní součet na konci paketu.

Originální paket

6B	6B	2B	64 až 1500B	4B
cílová adresa (DA)	zdrojová adresa (SA)	typ nebo délka	data	kontrolní součet (FCS)

Upravený paket pomocí 802.1q

6B	6B	4B	2B	64 až 1500B	4B
cílová adresa (DA)	zdrojová adresa (SA)	802.1q tag	typ nebo délka	data	kontrolní součet (FCS)

Tvar 802.1q tagu

2B	3b	1b	12b
0x8100	priorita (802.1p)	Canonical Format Indicator (CFI)	VLAN ID
Tag Protocol ID (TPID) 2B	Tag Control Information (TCI) 2B		

Native VLAN je termín spojený s protokolem 802.1q. Nastavuje se na ***trunk portu***, u Cisco prvků musíme nativní VLANu vždy nastavit a to shodně na obou stranách trunku, ale můžeme nastavit, aby se informace tagovali. Provoz, který je zařazen do native VLAN se při přenosu netaguje (zůstává nezměněn). Často se jako native VLAN nastavuje management VLAN. Důsledkem také je, že pokud se na trunk port dostane nějaký paket, který nemá tag, tak je zařazen do nativní VLANy.

Cisco ISL encapsulation

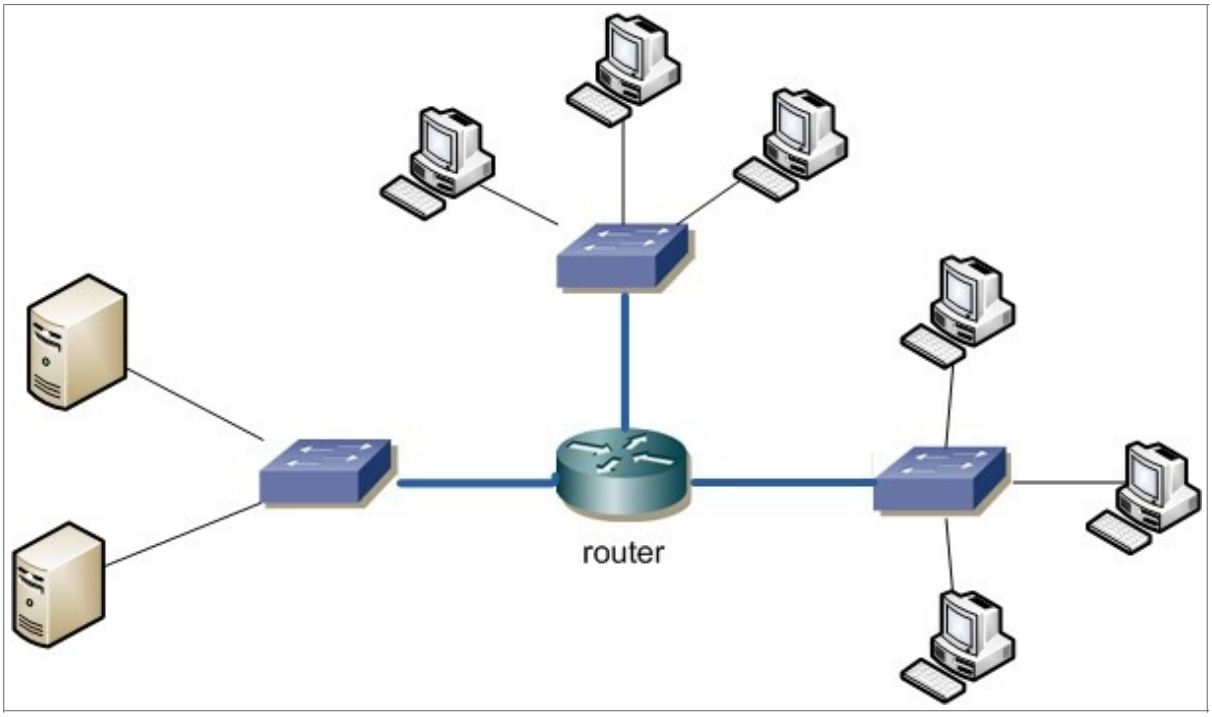
ISL znamená ***Inter-Switch Link***, tedy spoj mezi switchi. Cisco vytvořilo svůj protokol ještě v době, kdy neexistoval standard. ISL má výhodu, že funguje nejen pro protokol IP, ale i pro jiné. Stejně jako 802.1q podporuje prioritizaci.

Bohužel se jedná o proprietární metodu, kterou používá pouze Cisco a v dnešní době ji nalezneme pouze na switchích vyšší řady (třeba Catalyst 3750). Princip funkce je takový, že se celý paket zabalí (encapsulate) do nové hlavičky a kontrolního součtu. Z toho plyne nevýhoda, že se více zvětšuje komunikace, každý paket je o 30B větší.

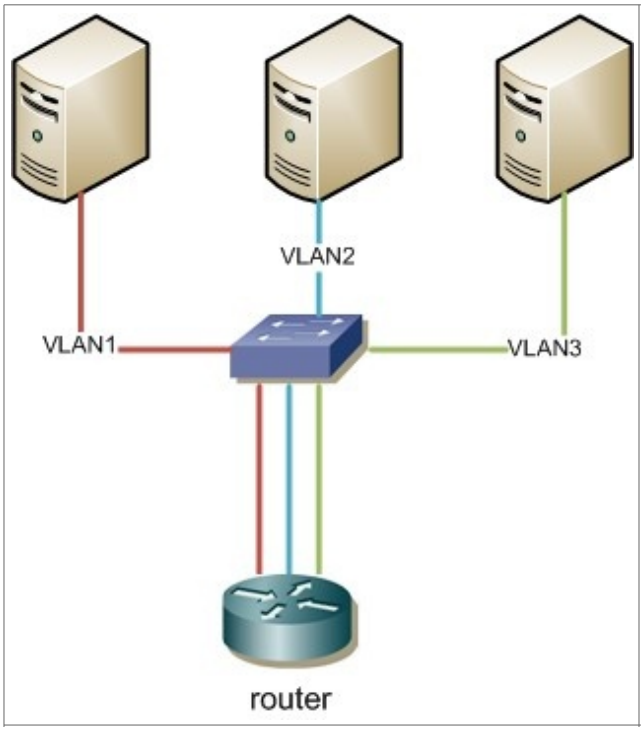
26B		4B
ISL header	encapsulation frame (originální rámec)	kontrolní součet (FCS)

Routing mezi VLANy

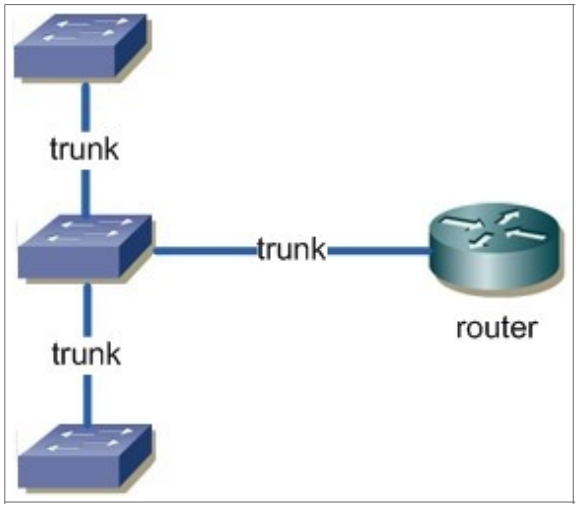
Tradiční routing vypadá tak, že máme několik oddělených sítí a chceme mezi nimi umožnit nějakou komunikaci. Následující obrázek představuje tři samostatné switche propojené pomocí routeru. Může se jednat například o firemní servery a dvě oddělení, které k nim chceme připojit, ale nechceme, aby mohla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

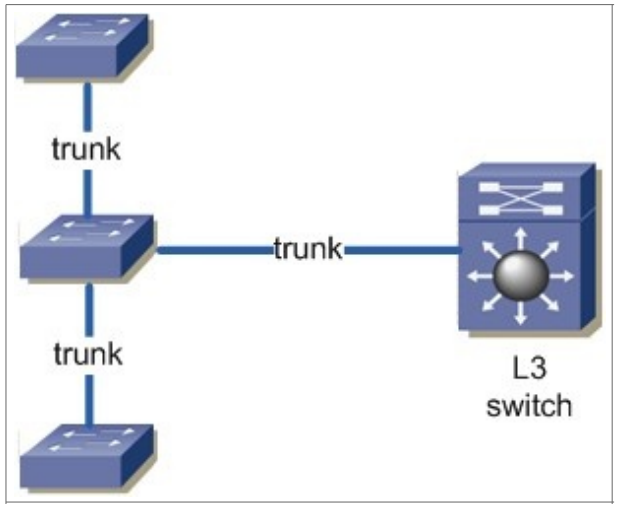


Pokud využíváme VLANy, můžeme se k nim chovat stejně jako k normálním podsítím. Na switchi můžeme jednotlivé VLANy, které chceme routovat, vyvést do samostatných access portů a ty připojit k routeru.



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.





U Cisco L3 switchů provedeme inter-VLAN routing jednoduše tak, že zapneme routování a na ty VLANy, které mají mezi sebou routovat, nastavíme IP adresu.