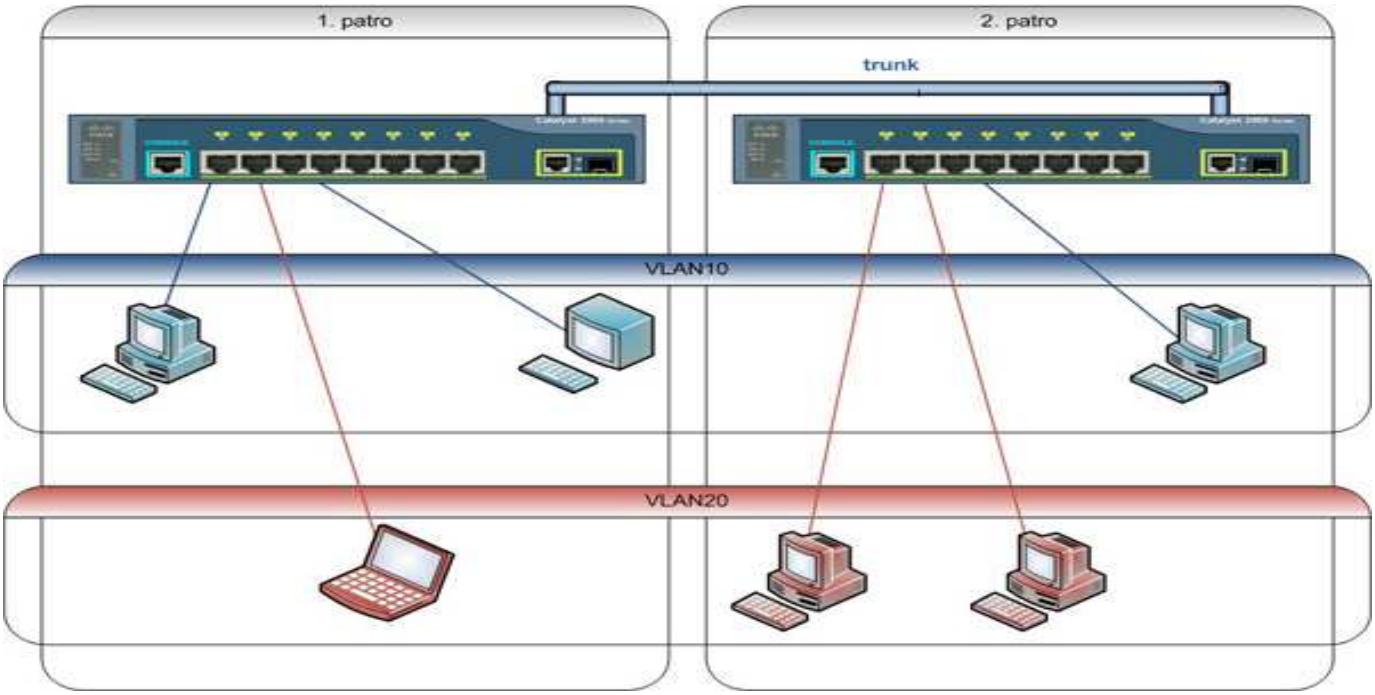
Virtální lokální sítě (VLAN)

Virtuální LAN slouží k logickému rozdělení sítě nezávisle na fyzickém uspořádání. Lze tedy LAN síť segmentovat na menší sítě uvnitř fyzické struktury původní sítě. Druhým důležitým pojmem, který bude více vysvětlen později, je trunk. Jako trunk označujeme port, který je zařazen do více VLAN.

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 je často potřeba komunikace i 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.

Na následujícím **obrázku 1** lze vysvětlit princip 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.

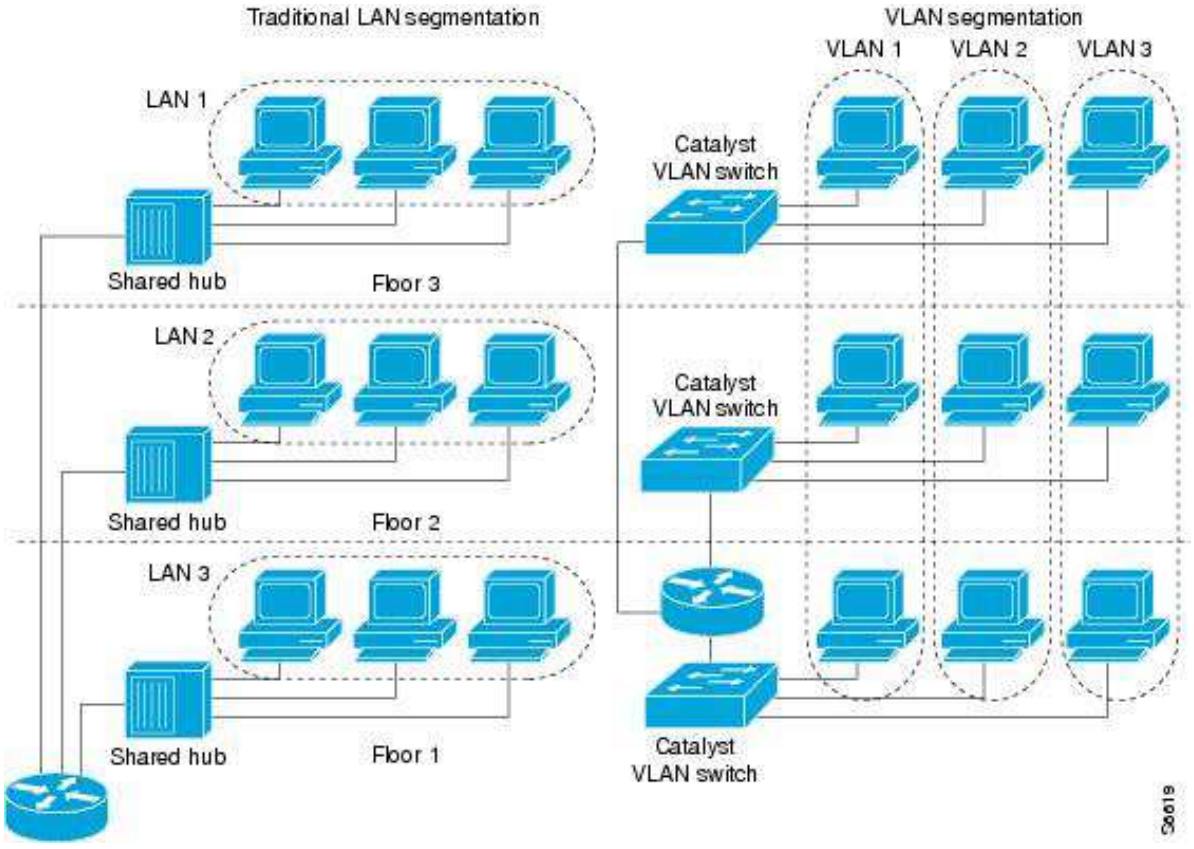


Pro pochopení VLAN je třeba rozumět základům sítí a jejich segmentování (dělení na subnety - podsítě).

Oddělení sítí

Jak bylo již uvedeno, pokud použijeme různé subnety, tak spolu zařízení nemohou komunikovat. Není to však úplně pravda. Nedojde k oddělení těchto zařízení, pokud jsou připojena na stejné médium (linku) prostřednictvím stejného hubu (pracuje na 1. vrstvě OSI) a 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 všesměrově) ani switch (používá MAC adresy) se nedívá na IP adresy procházející komunikace. Proto se dá tato komunikace zachytávat a odposlouchávat. Pokud tedy chceme mít oddělené sítě, tak musíme použít oddělené linky, což komplikuje technickou realizaci.

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



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.

Proč vznikly VLAN

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 broadcast domén v síti, které začaly být problémem již před několika lety,
- zmenšení kolizních domén v době, kdy se ještě používaly huby (switche byly novinkou).

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, 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. (například IP telefonie, komunikace mezi AP v centrálně řízeném prostředí, management apod.).
- HW náročnost- 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).

Například pro IP telefonii, kde je použití VLAN naprosto běžné (a často i nutné), nám stačí jediná zásuvka, kam přivedeme VLAN pro telefonii i VLAN s přístupem do sítě a v telefonu se komunikace rozdělí. Navíc VLAN můžeme vázat s QoS pro zaručení kvality komunikace (obsazení pásma).

Jak se zařazuje komunikace do 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.

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 VLAN, 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

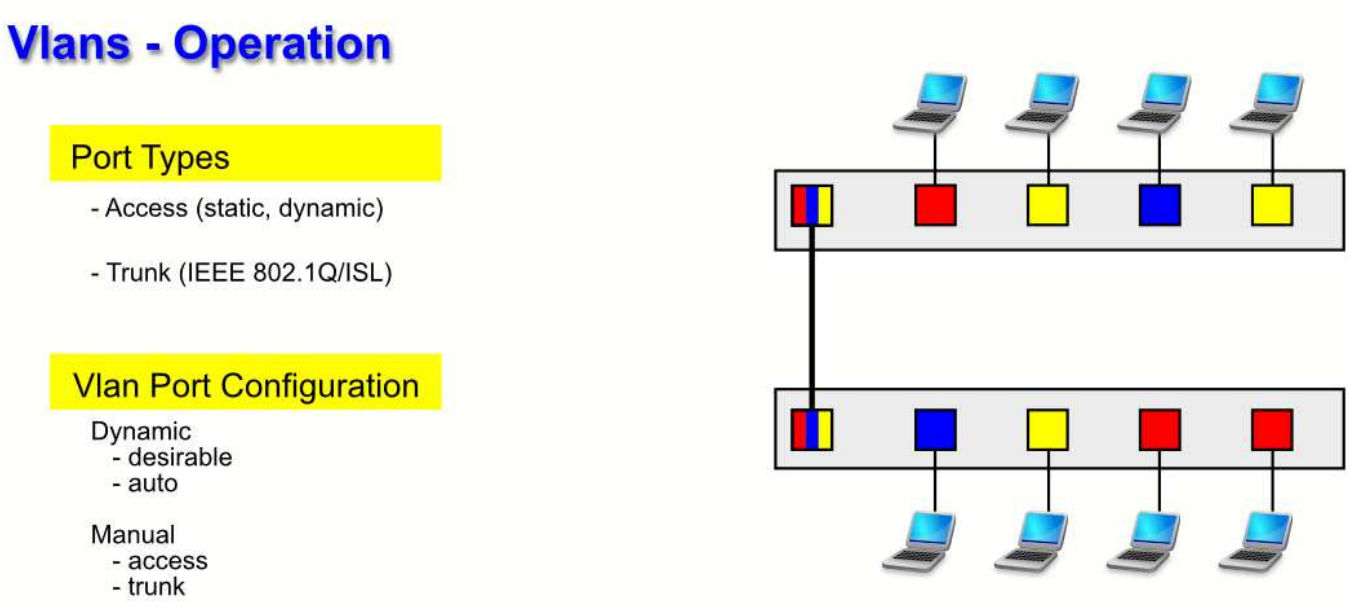
Ověří se uživatel nebo zařízení pomocí protokolu IEEE 802.1x a podle informací se automaticky umístí do VLAN. Je to primárně bezpečnostní metoda, které řídí přístup do sítě (NAC), ale po rozšíření slouží i pro VLAN. Je to zajímavá metoda proto, že je velmi univerzální.

Nezáleží ani na fyzickém zařízení ani na místě zapojení. RADIUS server, který ověřuje identitu uživatele, obsahuje také mapovaní uživatelů na VLAN 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 VLAN.

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 VLAN) a komunikovat mohou všechna zařízení.

Jak funguje komunikace v rámci VLAN

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, jak bylo řečeno výše (možnosti 2,3,4). 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. 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 rámec, ale funguje pouze na Cisco zařízeních. Také můžeme propojit dva access porty na dvou switchích, zařadit je do stejné VLAN a přeneseme potřebné informace. To je ale velmi nepraktické. 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.

Spoji dvou trunk portů se říká trunk nebo **trunk link**.