VLAN (virtuální sítě) – struktura, princip činnosti, intranet, extranet, VPN

VLAN (virtuální sítě LAN)

Umožňují komunikaci v rámci internetu tak, jako by šlo o jedinou síť LAN, nebo slouží v rámci sítí LAN k virtuálnímu dělení sítě na podsítě. Často podstatně zlepšují chod sítě, její správu a také služby; vytvářejí logické skupiny v rámci komunikačního systému (sítě); brání šíření nepotřebných informací do částí sítě, kde nejsou takové informace potřebné nebo žádoucí; umožňují kontrolovat informace jdoucí z/do logických skupin a automatické sledování stěhování strojů, klientů, vytváření a rušení skupin apod.

VLAN sítě jsou realizovány nad sdílenou strukturou, tj. nejsou dedikovány žádné vlastní fyzické spoje pro jednotlivé virtuální části = stanice nejsou vázány na fyzické umístění. Jsou seskupovány do celku podle potřeby.

Problém rozšíření VLAN je v nejednotnosti hardwaru (uživatel je často vázán na jednoho výrobce) + mají velké náklady na administrativu).

Každá virtuální síť v rámci sítě LAN odpovídá broadcast doméně.

Výhody VLAN

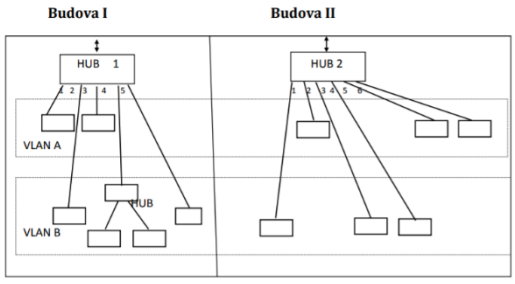
Omezení všesměrového vysílání (všesměrové vysílání od serverů a konc. stanic ve VLANech je přenášeno jen na porty switche, které jsou připojené ke stanicím patřícím do stejné VLAN); vyšší výkon; menší zpoždění.

Dělení VLAN

Typ rozpoznávání členství ve VLAN se vybírá podle toho, co je v daném případě nejvhodnější.

Podle portů

Síť je tvořena bez ohledu na umístění v budovách, rozlišení je prováděno podle čísel portů na příslušných switchích nebo hubech. Byla-li by tato situace řešena bez VLAN, v každé budově by musel být switch, který by byl napojený na společný switch pro každou podsíť (složitější zapojení a finanční náročnost). Ušetříme počet zařízení. Jde o nejužívanější řešení, protože je přehledné.



Bez vytvořených VLAN by musel být pro každou VLAN v každé budově samostatný switch. Tyto switche by byly napojeny na společný switch (pro každou podsíť) a ty na router. Celá struktura sítě by tedy byla složitější a hlavně finančně náročnější.

Podle stanic

Příslušnost do konkrétní VLAN je dána kombinací port + MAC adresa + síťový protokol. Toto je na switchích pevně (staticky) nastaveno.

Podle fyzických adres (dynamická VLAN)

Příslušnost do VLAN není závislá na portu, je dána pouze kombinací MAC adresy a síťového protokolu. Rámce se do VLAN zařadí podle zdrojové MAC adresy. Je nutné vést 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.

Podle třetí vrstvy ISO-OSI

Členství se rozpoznává podle adresy třetí vrstvy. Síť je rozdělená na podsítě. Adresy nemají směrovací funkci, jde pouze o adresy podsítě nejde o adresu pro směrování ven, slouží jen pro vnitřní účely. Uživatelé se mohou fyzicky přemisťovat.

Pakety jsou zapouzdřovány (*encapsulation*), v zapouzdřeném paketu se nachází mj. IP adresa VLAN, která tak není použita pro směrování do Internetu. *Decapsulation* provádí router, aby mohl paket poslat do příslušné VLAN.

Umožňuje rozdělení podle protokolů a nevyžaduje značení rámců podle příslušnosti. Nevýhodou je větší zpoždění způsobené testováním adres 3. vrstvy a náročná konfigurace.

Překryvný model

Paket včetně IP je zabalen do paketu 3. vrstvy obsahující v hlavičce novou IP adresu, zbytek bývá zašifrován. Takto vytvořené tunely spojují koncové zákazníky, celá síť se tváří jako jedna podsíť.

Peer-to-peer model

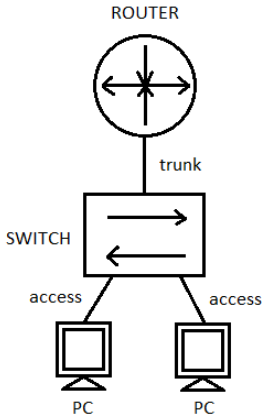
IP je rozšířena o 64bitový prefix, který je pro každého klienta jedinečný. Tato technologie využívá MPLS. Jsou pak vytvářeny speciální routovací tabulky – na hraničních směrovacích – pomocí směrovacího protokolu BGP. Každý paket je vybaven značkou, která zajistí transport na další hraniční router.

Podle multicastu

Tedy podle skupinového adresování. Používá se pro cílené směrování pro vysílání nebo příjem (např. televizního vysílání, videokonferencí atp.).

Trunk porty a access porty

Na routeru je pro všechny sítě jeidný výstup – nutné nakonfigurovat jeden interface (číslo portu + IP adresa) a subinterfaces (číslo podsítě + číslo VLAN, pro kterou platí).



Trunk port

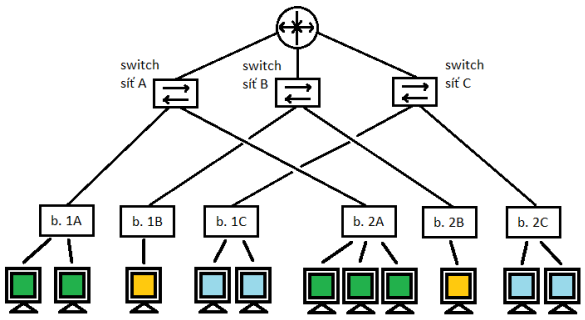
Port, po kterém tečou data do/ze všech VLANů.

Access port

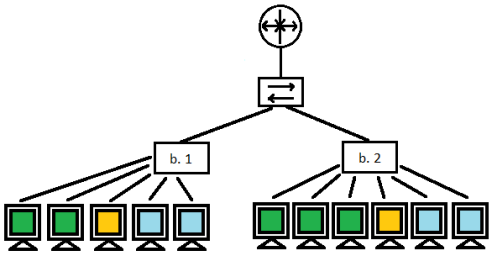
Port, na němž je VLAN (na každém access portu může být jen jedna – pro každou VLAN je jiná podsíť – každý počítač může být v jiné podsíti).

Porovnání sítě bez VLAN a s VLAN

Bez VLAN



S VLAN



Porovnání

V síti s VLANy není každá podsíť tvořena svým switchem, nýbrž právě virtuálně. Je ponechán pouze jeden switch, který se stará o *rozhazování* paketů do příslušných VLANů. Na switchi v každé budově je vytvořena VLAN A, VLAN B a VLAN C a tyto switche jsou s horním switchem propojeny trunkovým spojením. Switche musejí podporovat VLAN.

Pro rozlišení příslušnosti k jednotlivým VLAN přidává první switch každému paketu příznak – ten označí, ze které podsítě přišel. Ani hromadné korespondenci není dovoleno dostat se k počítačům z VLAN, do níž tato korespondence nepatří. Hromadná korespondence funguje jen u počítačů ve stejné VLAN.

Mají-li spolu komunikovat počítače z VLAN 1 (zelené), paket přijde na switch v b. 1 a odtamtud je poslán na příslušný počítač – protože jsou ve stejné podsíti.

Mají-li spolu komunikovat počítače ze dvou různých VLANů (např. zelený s modrým), paket dorazí na switch v b. 1 (který přidá příznak) a poté putuje na první switch, který jej předá routeru (ten upraví příznak) a paket putuje zpět přes první switch na switch budovy 1 nebo 2 a následně na příslušný počítač.

U routeru jsou vytvořeny virtuální porty s různými IP adresami podle různých VLAN. Tyto IP adresy slouží jen pro vnitřní potřebu.

Konfigurace virtuálních sítí

Spočívá zejména v konfiguraci switchů a routerů a určení trunkových spojení. U routeru se vytváří virtuální porty s různými adresami podle různých VLAN.

Manuální

Správce provádí jak počáteční nastavení, tak všechny změny manuálně. Umožňuje vysoký stupeň kontroly a je často pro menší sítě jednodušší.

Poloautomatická

Správce má možnost volby automatické nebo ruční konfigurace, automaticky lze provést počáteční konfiguraci nebo její změny, případně obojí.

Automatická

Spojení do skupin se provádí dynamicky automaticky podle aplikací a uživatelské identifikace.

Standardy VLAN

IEEE 802.10 podle CISCO – využívá standardu pro bezpečnost sítí, kde nahrazuje bezpečnostní hlavičku proměnné délky informací o příslušnosti k VLAN. Jedna hlavička je tedy využita pro dva účely. Řešení je pomalé, obtížnější a dražší.

IEEE 802.1Q – nový schválený standard. Známý také jako *VLAN Tagging* nebo *Dot1q*.

VPN – virtuální privátní síť

Většinou jde o vnitřní soukromou síť, která pro komunikaci používá veřejnost nebo jinou sdílenou datovou síť. Provoz této sítě je bezpečně oddělen od ostatních uživatelů. VPN je (logicky a z pohledu uživatele) samostatnou podsítí veřejné sítě (má samostatný adresový prostor), technicky a provozně je však její součástí. Přístup k uzlům mimo VPN je prováděn přes bránu.

VPN využívá protokol IPsec[1] a používá se nejčastěji tam, kde není nutné stálé připojení (připojení vzdáleného pracovníka, připojení obchodního partnera do vnitřního systému firmy atp.).

VPN se vytváří **a)** na výstupním routeru, na firewallu (nejvíce výhodné), **b)** na speciálním serveru v síti LAN (nevýhoda: větší provoz na vnitřní síti – komunikace k serveru a od něj) nebo **c)** přímo na stanici (nevýhoda: všechno musí projít přes NAT). Tam, kde je VPN vytvořen se upravují data pro vysílání.

Není garantována šířka pásma ani doba odezvy.

Úprava dat

Stanice data nejprve zašifruje, postupně se přidávají jednotlivé hlavičky. Na routeru/speciálním serveru/na stanici se data podruhé zapouzdří (encapsulation). Vznikne tak celý paket včetně hlavičky a adres. Vytvoří se nové hlavičky odpovídající normám VPN. Odesílatel je poslední router, příjemce je první router.

Použití VPN a bezpečnost

VPN se používá zejména pro bezpečný přenos přes nezabezpečenou síť (zhruba stejně bezpečné jako přes vlastní LAN). Každá VPN musí obsahovat tři bezpečnostní prvky: zapouzdření, šifrovanou autentizaci a šifrování dat.

[1] IPsec – bezpečnostní rozšíření protokolu IP; založeno na autentizaci a šifrování každého IP datagramu

Intranet

Část sítě využívající stejné technologie jako Internet, na rozdíl od něj jde však o síť privátní – vnitřní systém firmy, obecně nedostupný zvenčí. Využívání je omezeno na malou skupinu uživatelů.

Extranet

Extranet je soustava intranet sítí propojených přes Internet. Po technické stránce je založen na technologiích Internetu. Využívá přenosových infrastruktur a celkově služeb Internetu. Sleduje se vnější cíl → pro prezentaci firmy (např. obchodování; dodavatelé a distributoři; sdílení informací s VIP klientem; obecně pro sdílení informací s určitou skupinou lidí).

Jako zabezpečení jsou většinou na vstupech použity firewally.

Úkolem extranetů je tedy zpřístupnění lokální sítě globálním uživatelům a klientům LAN a dále umožnit přístup k informacím Internetu. Lokální sítě se zprůhlední.

Tunneling

Používanější způsob. Dvoubodové spojení přes rozsáhlou síť. Spojení musí podporovat všechny aktivní prvky. Tunneling se realizuje na druhé a třetí vrstvě ISO-OSI.

Druhá vrstva – sítě ATM
Třetí vrstva – sítě VPN pracující na IP protokolu

Využívá protokoly PPTP[2] a IPsec v režimu tunneling a dále protokolů L2F[3] nebo L2TP[4]. Možné také použít mechanismus GRE[5]. Existuje několik typů tunelování:

Side-to-side

Používá se pro stálá spojení (např. připojení poboček k centrále), realizováno na přístupovém bodu (firewall, směrovač, server) – přístupový bod slouží jako VPN gateway – tím se naváže VPN spojení

Remote access VPN

Např. pro vzdálený přístup individuálních klientů, každý klient musí mít speciální software (VPN klienta – program pro zadání hesla). Tunely se vytváří dynamicky před každým spojením, bezpečnost je žešena pomocí tzv. *AAA*:

autorizace	kontrola oprávnění uživatele k přístupu
autentizace	ověření uživatele zkontrolováním hesla
accounting	zaznamenání úspěšného/neúspěšného spojení

[2] PPTP – Point-to-Point Tunneling Protocol; od Microsoftu; funguje jen na TCP/IP; prolomeno (červenec 2012), nelze již považovat za bezpečné
[3] L2F – Layer 2 Forwarding; vyvinulo CISCO
[4] L2TP – Layer 2 Tunneling Protocol; jde o kombinaci PPTP a L2F, považováno za to nejlepší z PPTP a L2F; tunel L2TP se realizuje mezi přístupovým koncentrátorem jako klientem a síťovým serverem
[5] GRE – Generic Routing Encapsulation; libovolný OS; routery zapouzdří data přidáním GRE záhlaví a cílové adresy na konci tunelu; podporuje dvoubodové tunely

Význam extranetu

Snadné propojení s Internetem, levné propojení vzdálených soukromých sítí nebo segmentů sítě. Dále pak zavedení ověřené struktury Internetu do podnikových sítí, jedná se především o jednoduchou distribuci a prezentaci dat s možností omezení přístupu; vypracované GUI s velkými možnostmi; kompatibilitu s různými platformami jak po HW stránce, tak po SW stránce; snadný upgrade a zavádění nových technologií; snadné programování a vyvíjení aplikací (stránek, přístupů); poskytování novinek, zpráv; snadná konfigurace a obsluha.

Šifrování VLAN a VPN

Pomocí veřejného klíče

Asymetrické šifrování (vlastní privátní klíč + veřejný klíč příjemce) → přesun přes nezabezpečenou cestu → dekódování (vlastní privátní klíč + odesílatelův veřejný klíč).

Pomocí tajného klíče

Symetrické šifrování (jediný tajný klíč – k šifrování i k dešifrování, nutné ho zabezpečit proti neoprávněnému použití).

Příklad průběhu komunikace VPN

Předpokládejme, že se jedná o VPN založenou na routerech propojující dvě sítě. Síť 1 s IP 10.1.1.0/16 (brána: vnitřní IP adresa 10.1.1.254 a vnější IP adresa do Internetu: 250.121.13.12) a síť 2 s IP 10.1.2.0/16 (brána: vnitřní IP adresa 10.1.2.254 a vnější adresa: 110.121.112.34). Komunikace mezi sítěmi (počítači 10.1.1.99 a 10.1.2.22) bude vypadat takto:

1. vysílací počítač 10.1.1.99 vyhledá v routovací tabulce, že počítač 10.1.2.22 je nepřímo přístupný přes bránu
2. pošle paket na bránu 10.1.1.254
3. router IPsec 10.1.1.254 přečte obě IP adresy paketu a spustí nadefinovanou bezpečnostní asociaci na směrovač 110.121.112.34 druhé sítě
4. směrovač první sítě pošle na směrovač druhé sítě požadavek o domluvu IKE – Internet Key Exchange
5. oba směrovače se domluví na sadě šifrovacích a autentizačních klíčů
6. směrovač IPsec zašifruje paket a zapouzdří ho do jiného paketu
7. směrovač IPsec přes rozhraní 250.121.13.12 zašla zapouzdřený paket na rozhraní 110.121.112.34 druhého IPsec směrovače
8. po doručení tento router přečte zapouzdřený IP paket a dešifruje vložený IP paket
9. je-li vše OK, zašle pouze vložený paket na jeho IP destination adresu 10.1.2.22 přes své rozhraní 10.1.2.254
10. cílový počítač paket přečte