VLAN, podniková síť

Joseph Soukup – P4

Koncepce VLAN

- Logicky nezávislá síť v rámci jednoho nebo několika zařízení
- Obvykle bývá realizována na zařízeních zvaných přepínač, jehož porty se rozdělí na několik logicky samostatných částí
- Jde o dělení sítě už na 2. úrovni vrstvy ISO/OSI, v porovnání s podsítěmi na 3. vrstvě
- Skupina zařízení VLAN může komunikovat, jako kdyby byly připojeny na stejný kabel
- Unicast, broadcast jsou vysílány na konkrétní VLAN
- Zvyšuje výkon sítě oddělením velkých částí od malých

Výhody

- VLAN umožňuje realizaci přístupové a bezpečnostní politiky podle specifických skupin uživatelů, oddělení skupin, kteří mají např. citlivá data
- Každému portu přepínače může být přidělen pouze jedna VLAN
- Snížení nákladů za další switche apod.
- Lepší výkon -> dělení na 2. vrstvě do několik pracovních skupin
- Snížení broadcastů – vytvoření více, ale menších broadcastových domén -> snížení provozu
- Zjednodušená správa k přesunu zařízení do jiné sítě stačí překonfigurovat zařízení do VLANy, tedy správce konfiguruje SW (zařazení do VLAN) a ne HW (fyzické přepojení)
- Identifikace sítě pro konkrétní např. pracovní segment -> název
- 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 (zabezpečený 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

Typy VLAN

Podle portu

- Port switche je ručně a napevno zařazen (nakonfigurován) do určité VLANy
- Pokud do portu připojíme další switch, tak všechny zařízení připojená k němu budou v jedné VLANě

Podle MAC adresy

- Rámce (port) se zařadí do VLANy podle zdrojové MAC adresy -> MAC tabulky
- Dynamické zařazení, takže pokud přepojíme zařízení do jiného portu, automaticky se zařadí do správné VLANy

Podle protokolu = podle informace z 3. vrstvy

- Podle protokolu přenášeného paketu
- Zařazujeme podle IP adresy či rozsahu

Podle autentizace

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

Access VLAN

- Toto je defaultní mód switch portu
- Pokud je port v přístupovém módu, měli bychom jej zařadit do správné VLANy
- Může být členem pouze jedné VLANy, ve výchozím stavu jsou všechny porty ve VLAN 1

Trunk VLAN

- Trunk mode slouží primárně k tomu, abychom více switchů propojili mezi sebou a komunikace zůstala ve správné VLANě
- Point-to-point mezi dvěma síťovými zařízeními

IEEE802.1Q

- 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 switchy (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**

Native VLAN

- Spojený s protokolem 802.1q
- Nastavuje se na trunk portu
- Provoz, který je zařazen do native VLAN se při přenosu netaguje (zůstává nezměněn) a příchozí provoz, který není tagovaný se zařazuje do native VLAN

Management VLAN

- Management VLAN se používá pro správu switche a ze vzdálených míst pomocí protokolů, jako jsou Telnet, SSH, SNMP, syslog atd.
- Obvykle je management VLAN VLAN 1, ale můžeme použít jakoukoliv VLANu jako management VLAN
- Cisco doporučuje nepoužívat jako management VLAN VLAN 1 a nepoužívat ani VLAN, která přenáší uživatelská data
- Je nutné nastavit IP adresu a výchozí bránu pro management VLAN

Voice VLAN

- Voice VLAN povoluje access portům provádět IP hlasový provoz z IP telefonu
- Pro VoIP (IP telefonie) má Cisco řadu zjednodušení

- Jedním z nich je konfigurace, kdy je do portu připojen Cisco telefon (který obsahuje malý 3portový switch) a za ním je připojen PC
- Na portu nastavíme access VLAN, do ní spadá komunikace PC, a také voice VLAN (někde označována jako auxiliary VLAN – má i více použití), do které se zařadí komunikace telefonu
- Aby vše fungovalo, jak má, tak musíme použít Cisco IP telefon a na portu musí být povoleno CDP
- Ve skutečnosti vše funguje tak, že se na portu nastaví trunk, access VLAN se stane native VLAN (tedy netagované) a komunikace telefonu použije 802.1q

VTP

- VLAN Trunking Protocol
- Zajišťuje přenášení čísel a názvů virtuálních LAN mezi přepínači zařazených do jedné domény
- VTP spravuje přidávání, mazání a přejmenování VLAN uvnitř VTP domény
- VTP doména je tvořena jedním nebo více síťovými zařízeními, která mají nastaveno stejné jméno domény (volitelně i heslo) a jsou propojený pomocí trunku
- Princip je takový, že každý switch ve VTP doméně má nastaven jeden ze tří módů
    - Server – spravuje seznam všech VLAN, má jej uložen v NVRAM, může vytvářet i mazat VLANy, přijímá a odesílá advertisements přes trunky ve VTP doméně, jedná se o defaultní mód
    - Klient – přijímá konfiguraci ze serveru, udržuje lokální kopii všech VLAN, kterou nelze měnit a nemá ji uloženou v NVRAM, přijímá a odesílá advertisements
    - Transparentní – neúčastní se VTP, pracuje samostatně, může vytvářet i mazat VLANy, ale změny jsou lokální, přijímá advertisements a ve verzi 2 je i přeposílá, je to jediný mód, kde můžeme vytvářet Extended a Private VLANy, VTP a VLAN konfigurace je uložena v NVRAM
- 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

DTP

- Dynamic Trunk Protocol
- Slouží pro automatické vyjednávání, zda je daný port trunk
- Z bezpečnostního hlediska se doporučuje nepoužívat, protože by některá stanice mohla vyjednat, že se jedná o trunk a pak zachytávat veškerou komunikaci
- Konfigurace DTP se provádí na každém portu
    - Pokud nastavíme port napevno do přístupového módu (access), tak není ovlivněn DTP protokolem
    - Pokud jej nastavíme napevno do trunk módu, tak se opět jeho mód nemůže změnit, ale on vyjednává pomocí DTP, aby se linka (druhá strana) přepnula do trunku
    - Pokud je port v trunk módu, tak můžeme nastavit, aby negenerovala DTP rámce (a vůbec nepoužíval DTP)

Bezpečnost, metoda odstraňování závad, typické chyby při nasazení

- VLAN dokáže nezávisle na nastavení ostatních aktivních prvků, stanic a aplikací naprosto izolovat jednotlivé účastníky sítě mezi sebou
- Většinou jde o povolení přístupu na společná zařízení všem klientům sítě (servery, routery pro přístup do internetu a tiskové servery) a zároveň izolaci vlastních pracovních stanic v rámci pracovních skupin

Switch Spoofing

- Útočníkova stanice vydává za switch a získává data z trunku, kde je přenášeno množství VLAN (nebo všechny)
- Může se jednat o zneužití protokolu DTP, kdy stanice vyjedná na svém portu trunk

Double Tagging

- Odesílá rámce s přidanými dvěma 802.1q tagy
- Switch přijme rámec, první tag je do jeho správné VLANy, odstraní se, ale rámec se dále nekontroluje a zpracovává switchem, jako by byl první VLANě
- Pokud máme trunk port, kde je nativní VLAN nastavena stejná, jako měl port uživatele
- Tak se rámec odesílá netagované, jenže on již tag má a ten směruje do jiné VLANy
- Druhý switch odstraní druhý tag a rámec již putuje novou VLANou