Cisco IOS 7 - konfigurace VLAN, VTP

Vložil/a Samuraj [1], 13 Prosinec, 2010 - 16:17

- Networks & Protocols [2]

Další popis operačního systému Cisco IOS se tentokrát věnuje důležité, a v praxi potřebné, oblasti virtuálních lokálních sítí, tedy VLAN. Teorii jsem popsal v dřívějším článku, takže nyní se jedná o praktický popis konfigurace VLAN. Zmíněny jsou také protokoly Dynamic Trunk Protocol (DTP) pro automatické vyjednávání trunků a užitečný VLAN Trunking Protocol (VTP) pro konfiguraci VLAN na jednom místě a její automatickou distribuci na ostatní switche.

O teorii, možnostech a výhodách VLAN jsem psal v článku VLAN - Virtual Local Area Network [3]. Pár informací o konfiguraci VLAN, ve spojitosti se zařazováním portu do VLANy či trunku, jsem popsal již v článku Cisco IOS 3 - nastavení interface/portu - access, trunk, port securit. Nezmínil jsem však vlastní vytváření VLAN. V tomto článku je souhrnný popis konfigurace VLAN a věcí s tím souvisejících.

Čísla VLAN

VLANy se běžně identifikují pomocí čísla, takže máme například VLAN 10. Pro jednoduší zapamatování a orientaci se k nim ještě přiřazují jména.

Cisco switche by v posledních letech měly podporovat tyto číselné rozsahy pro VLANy. Starší zařízení nepodporují čísla nad 1005, navíc tyto VLANy nejsou přenášeny pomocí VTP a neukládají se do VLAN databáze.

VLANy	popis
0 a 4095	rezervované pro systémové použití
1	defaultní VLAN, standardně obsahuje všechny porty, nedá se smazat
2-1001	běžný rozsah pro ethernetové VLANy
1002-1005	speciální defaultní VLANy pro Token Ring a FDDI, nedají se smazat
1006-4094	Extended VLAN - rozšířené VLANy pro ethernet, nejsou vždy podporovány

Vytvoření a pojmenování VLANy

Konfigurace VLAN je (u některých typů switchů) udržována v běžící konfiguraci a v souboru vlan.dat.

Novou VLANu vytvoříme následujícím příkazem, pokud již VLANa existuje, tak se přepneme do její konfigurace.

```
SWITCH(config)#vlan 10                    // vytvo?ení/p?epnutí do VLAN 10
```

Nyní jsme v konfiguraci VLANy a můžeme nastavit několik parametrů, dobré je nastavit jméno VLANy pro snadnější orientaci.

```
SWITCH(config-vlan)#name net1             // pojmenování VLANy
```

Z vlastností, které můžeme nastavit pro celou VLANu, zmíním pouze změnu IP MTU (maximální velikost přenášených paketů - payload rámce), standardní je 1500B pro Ethernet (rámec má velikost 1518B).

```
SWITCH(config-vlan)#mtu 2000                // možné hodnoty 576 až 18190 (podle typu switche)
```

Změny se uloží při opuštění konfigurace.

```
SWITCH(config-vlan)#exit                    // o úrove? výš
```

Zrušit VLANu můžeme standardně. Při zrušení VLANy však nedojde k odstranění vazeb, které na ni existují (jako zařazení portů do VLANy).

```
SWITCH(config)#no vlan 10                   // smazání VLANy 10
```

Pozn.: VLANu vytvoříme také tím, když ji použijeme na určitém místě. Například pokud port zařadíme do neexistující VLANy, tak se tato vytvoří.
Nastavení IP adresy pro VLANu

VLANy jsou virtuální interfacy, proto s nimi můžeme provádět řadu operací jako s klasickým interfacem (portem). Jednou z možností je nastavení IP adresy, tím vlastně nastavíme adresu switche v dané VLANě.

```
SWITCH(config)#interface vlan 10                          // p?epnutí do konfigurace
SWITCH(config-if)#ip address 192.168.190.1 255.255.255.0  // nastavení IP adresy
SWITCH(config-if)#no shutdown                             // nahození interfacu
```

Switch Virtual Interface - SVI

Výše uvedená informace není přesná. Správně musíme říci, že pro každou VLANu můžeme vytvořit Switch Virtual Interface (SVI), což je ten zmiňovaný virtuální interface. VLANy a SVI však existují nezávisle na sobě, i když se provádí mapování (které může být maximálně 1:1) mezi SVI a VLANou. SVI vytvoříme prvním přístupem do něj a můžeme jej vytvořit i pro neexistující VLANu. SVI pracuje na 3. vrstvě ISO/OSI modelu a defaultně je vytvořen pro VLAN 1 (a nelze jej smazat). SVI potřebujeme, pokud chceme provádět inter VLAN routing (routovat provoz mezi VLANami) nebo umožnit IP konektivitu ke switchi (pro přístup na CLI přes telnet/SSH a podobné funkce).

```
SWITCH(config)#interface vlan 15        // vytvo?ení SVI
```

Pro smazání SVI použijeme

```
SWITCH(config)#no interface vlan 15     // smazání SVI
```

VLAN 1

Na switchích, které podporují VLANy, musí existovat alespoň jedna VLANa, protože každý port musí být do nějaké zařazen. Na Cisco zařízeních je to VLAN 1 a všechny porty, ve výchozím stavu, jsou do ní zařazeny.

Z bezpečnostního hlediska je dobré nepoužívat tuto defaultní VLAN 1, nebo ji použít pouze pro hostovský přístup, a pro vlastní síť vytvořit jiné VLANy.

VLAN 1 nelze smazat a nelze ji ani vypnout, což je možné u všech ostatních VLAN.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

```
SWITCH(config-vlan)#shutdown            // vypnutí VLANy
```

Přiřazení portu do VLANy

Standardně jsou všechny porty zařazeny do VLAN 1. Pokud chceme nakonfigurovat přístupový port s pevným zařazením do VLANy, postupujeme následovně.

```
SWITCH(config)#interface f0/1               // p?epnutí do konfigurace portu
SWITCH(config-if)#switchport mode access    // nastavení portu do p?ístupového módu
SWITCH(config-if)#switchport access vlan 10  // za?azení do VLANy 10
```

Voice VLAN

Pro VoIP (IP telefonie) má Cisco řadu zjednodušení. Jedním z nich je konfigurace, kdy je do portu připojen Cisco telefon (který obsahuje malý 3-portový switch) a za ním je připojeno 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 netagovaná) a komunikace telefonu použije 802.1q.

```
SWITCH(config-if)#switchport voice vlan 20   // za?azení hlasu do VLANy 20
```

Konfigurace Trunku

Aby se zachovala informace o zařazení do VLANy, a aby se přenášela data v různých VLANách mezi switchi, je třeba mezi nimi zřídit trunk. Ten se nastavuje na obou stranách, na portu, kterým jsou switche propojeny mezi sebou. Můžeme využít standard IEEE802.1q (tagování rámců) nebo Cisco proprietální ISL (zapouzdřování), které je podporováno pouze u vyšších Cisco switchů. Také je možné vyjmenovat VLANy, které se mohou trunkem přenášet, pokud příkaz neuvedeme, tak se přenáší všechny.

```
SWITCH(config)#interface f0/1                              // p?epnutí na správný port
SWITCH(config-if)#shutdown                                 // doporu?eno  nejprve
vypnout port
SWITCH(config-if)#switchport trunk encapsulation dot1q  // zvolím metodu rozlišování
VLAN
SWITCH(config-if)#switchport trunk allowed vlan 2-200   // které VLANy se p?enáší
SWITCH(config-if)#switchport trunk native vlan 10       // ur?ení nativní VLAN
SWITCH(config-if)#switchport mode trunk                 // nastavení portu do TRUNK
modu
SWITCH(config-if)#switchport nonegotiate                // nevyjednává se trunk
protokolem DTP
SWITCH(config-if)#no shutdown                           // nahození portu
```

Pozn.: Stejnou konfiguraci je třeba provést na druhé straně. Aby se ustanovil trunk, tak je třeba dodržet několik předpokladů. Musí se jednat o Point to Point linku, porty musí mít nastavenu stejnou rychlost (speed), duplex, metodu encapsulace a nativní VLANu (u ISL se může lišit).

Dynamic Trunk Protocol (DTP)

Dynamic Trunk Protocol (DTP) slouží pro automatické vyjednávání, zda je daný port trunk. Z bezpečnostního hlediska se doporučuje tuto možnost nepoužívat, protože by některá stanice mohla

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

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 negeneroval DTP rámce (a vůbec nepoužíval DTP).

SWITCH(config-if)#switchport nonegotiate

* Poslední možností je nastavení portu do dynamického módu, kdy aktivně využívá DTP.

```
SWITCH(config-if)#switchport mode dynamic auto      // pokud p?ijde žádost, tak se
p?epne do trunku
SWITCH(config-if)#switchport mode dynamic desirable // posílá žádosti o vytvo?ení
trunku
```

Nejvhodnější je nastavit přístupové porty napevno do módu access a trunk porty napevno do trunk módu s vypnutým vyjednáváním.

Pro zobrazení informací o DTP slouží příkazy:

```
SWITCH#show dtp
SWITCH#show dtp interface f0/1
```

Zobrazení informací o VLANach - show příkazy

```
SWITCH#show vlan                        // stru?né info o VLAN a za?azení port?
SWITCH#show vlan id 500                 // seznam port? ve VLAN 500 a MTU pro VLANu
SWITCH#show interface vlan 10           // informace o SVI
SWITCH#show running-config vlan         // informace o VLAN z b?žící  konfigurace
SWITCH#show interfaces f0/1 switchport  // informace o portu spolu s VLAN
SWITCH#show interfaces trunk            // info o truncích
```

VTP - VLAN Trunking Protocol

Většinou chceme, aby vytvořené VLANy existovaly v celé síti (nebo v určité části, ale ne pouze na jednom switchi). Pro přenášení dat v těchto VLANách mezi switchi se využívají trunky. Aby se však dalo s těmito VLANami pracovat, tak musí být vytvořeny na každém switchi. Při menším počtu switchů (a pokud chceme větší dohled), tyto VLANy na každém switchi nakonfigurujeme ručně (většinou to není tolik práce). Musíme však pamatovat při vytvoření nové VLANy ji opět všude nakonfigurovat.

Druhou možností je využití VLAN Trunking Protocol (VTP), což je L2 protokol, který slouží k přenášení informací o VLANách mezi switchi. 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 propojeny pomocí trunku.

Princip je takový, že každý switch ve VTP doméně má nastavený jeden ze tří módů

*** server** - spravuje seznam všech VLAN, má jej uložen v NVRAM, může vytvářet a 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 (ale nesynchronizuje svoje VLANy, ani je nezveřejňuje), je to jediný mód, kde můžeme vytvářet Extended a Private VLANy, VTP a VLAN konfigurace je uložena v NVRAM

Pozn.: Konfigurace VTP, pokud je v režimu server nebo klient, se nenachází v running config.

Server rozesílá (pouze přes trunky) VTP advertisements (oznámení) každých 5 minut nebo při změně v konfiguraci. Server udržuje konfigurační revizní číslo (configuration revision number), které při každé změně zvýší o jedna. Klient při synchronizaci porovnává svoje a přijaté číslo. VTP advertisements obsahuje management domain, revision number, verzi VTP, známé VLANy a jejich parametry. Advertisements jsou tří typů, Summary, Subset a Client Request.

Pozn.: Standardizovanou obdobou VTP je protokol Generic VLAN Registration Protocol - GVRP a jeho nástupce Multiple VLAN Registration Protocol - MVRP. Na Cisco zařízeních jej však příliš nenajdeme.

Konfigurace VTP

Pro konfiguraci musíme nejprve vytvořit VTP doménu, těch může existovat více a informace se předávají pouze v rámci domény.

Pozn.: VTP pakety neprochází přes router.

```
SWITCH(config)#vtp domain domena1
```

Volitelně můžeme nastavit heslo, které musí být na všech switchích v doméně shodné. Heslo není uloženo v running-config.

```
SWITCH(config)#vtp password heslo
```

Jako poslední nastavíme, v jakém módu switch operuje.

```
SWITCH(config)#vtp mode server     // možnosti server, client, transparent
```

Na dnešních Cisco switchích můžeme použít VTP ve dvou verzích (VTP 1 a 2). Verze 2 navíc podporuje Token Ring, VLAN consistency check, unrecognized TLV a v Transparent modu přeposílá advertisements. Defaultní je verze 1, nastavení můžeme změnit.

```
SWITCH(config)#vtp version 2
```

Informace o VTP zjistíme pomocí příkazů

```
SWITCH#show vtp status          // základní info o b?hu VTP na switchi
SWITCH#show vtp counters        // statistika VTP p?enos?
SWITCH#show vtp password        // zobrazí VTP heslo
```

VTP Pruning

Můžeme také povolit pruning. Konfiguruje se na VTP serveru a ovlivní celou doménu. Zabrání odesílání zbytečných paketů (broadcast, multicast, neznámé) na switche, kde není žádný port v dané VLANě a ani přes něj nevede funkční cesta dál.

```
SWITCH(config)#vtp pruning
```

VLAN 1 je pruning ineligible, to znamená, že se na ni pruning neuplatňuje, VLAN 2 až 1001 je standardně pruning eligible, ale můžeme změnit konfigurací.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

URL článku: https://www.security-portal.cz/clanky/cisco-ios-7-konfigurace-vlan-vtp

Odkazy:
[1] https://www.security-portal.cz/users/samuraj
[2] https://www.security-portal.cz/category/tagy/networks-protocols
[3] http://www.samuraj-cz.com/clanky/administrace/vlan-virtual-local-area-network/

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn