Cisco IOS 7 - konfigurace VLAN, VTP

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) a VLAN Trunking Protocol (VTP).

O teorii, možnostech a výhodách VLAN jsem psal v článku VLAN - Virtual Local Area Network. 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 DTP.

VLANy	popis
0 a 4095	reservované pro systémové použití
1	defaultní VLAN, standardně obsahuje všechny porty, nedá se smazat
2-1001	bežný rozsah pro ethernetové VLANy
1002-1005	speciální defaultní VLANy pro Token Ring a FDDI, nedají se smazat
1006-4094	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                          // vytvoření/přepnutí 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
```

Změny se uloží při opuštění konfigurace.

```
SWITCH(config-vlan)#exit                        // o úroveň 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                        // přepnutí 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
```

Výše uvedené informace nejsou přesné. Správnější je 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. SVI vytvoříme prvním přístupem do něj a můžeme jej vytvořit i

pro neexistující VLANu. SVI pracuje na 3. vrstvě ISO/OSI modelu.

```
SWITCH(config)#interface vlan 15        // vytvoření 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.

```
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               // přepnutí do konfigurace portu
SWITCH(config-if)#switchport mode access    // nastavení portu do přístupového módu
SWITCH(config-if)#switchport access vlan 10  // zařazení do VLANy 10
```

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.

```
SWITCH(config)#interface f0/1                              // přepnutí na správný port
SWITCH(config-if)#shutdown                                // doporučeno  nejprve vypnout port
SWITCH(config-if)#switchport trunk encapsulation dot1q    // zvolím metodu označování
SWITCH(config-if)#switchport trunk allowed vlan 2-200     // které VLANy se přenáší
SWITCH(config-if)#switchport trunk native vlan 10         // určení nativní VLAN
SWITCH(config-if)#switchport mode trunk                   // nastavení portu do TRUNK modu
SWITCH(config-if)#switchport nonegotiate                  // nevyjednává se trunk protokolem DT
SWITCH(config-if)#no shutdown                             // nahození portu
```

> ***Pozn.:*** *Stejnou konfiguraci je třeba provést na druhé straně.*

Dynamic Trunk Protocol (DTP)

Dynamic Trunk Protocol (DTP) slouží pro vyjednávání, zda je daný port trunk. Z bezpečnostního hlediska se doporučuje tuto možnost 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 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 přijde žádost, tak se přepne do
SWITCH(config-if)#switchport mode dynamic desirable // posílá žádosti o vytvoření 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                          // stručné info o VLAN a zařazení portů
SWITCH#show interface vlan 10             // informace o SVI
SWITCH#show running-config vlan           // informace o VLAN z běžící  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 VLANech 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 a jsou propojeny pomocí trunku.

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

- **server** - může vytvářet a mazat VLANy, rozesílá informace ve VTP doméně
- **klient** - pouze přijímá konfiguraci ze serveru, udržuje lokální kopii, kterou nelze měnit
- **transparentní** - ignoruje VTP, pracuje samostatně, může vytvářet i mazat VLANy, ale změny jsou lokální, může přeposílat VTP advertisements

Server pak rozesílá (přes trunky) ***VTP advertisements*** každých 5 minut nebo při změně v konfiguraci. Server udržuje konfigurační ***revizní číslo*** (configuration revision number), které při každé změně zvýší o jedna. Klient pak při synchronizaci porovnává svoje a přijaté číslo.

Nejprve musíme 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
```

Dále nastavujeme heslo, které musí být na všech switchích v doméně shodné. Heslo není uloženo v running-config. Není povinné heslo nastavovat.

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

A jako poslední nastavíme, v jakém módu switch operuje

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

Existuje i několik dalších nastavení, například nastavení verze VTP (1 nebo 2), kdy všechny switche v doméně musí mít stejnou verzi.

Můžeme také povolit ***pruning***. V tom případě se rozesílají VTP rámce pouze do trunků, kde to má význam. Tedy pro ty VLANy, které jsou v trunku konfigurovány. Bez pruningu se posílá informace po všech truncích.

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

Informace o VTP zjistíme pomocí příkazů

```
SWITCH#show vtp status          // základní info o běhu VTP na switchi
SWITCH#show vtp counters        // statistika VTP přenosů
```