Cisco IOS 3 - nastavení interface/portu - access, trunk, port security

Vložil/a Samuraj [1], 17 Září, 2007 - 15:20

- Networks & Protocols [2]

V pokračování popisu operačního systému Cisco Switchů se věnuji asi nejpoužívanější oblasti, nastavování parametrů pro porty a interfacy. Od základních vlastností, přes používání VLAN, nastavení IP adresy až po zabezpečení portu pomocí Port security. Popis je pouze stručný a v závěru se nachází praktické příklady.

Značení portů

Rozhranní na switchi - interfaces, jsou hlavně fyzické porty a VLANy. Vedle toho však existuje celá řada dalších, např. sériová linka (serial), konzole (console), asynchronní linka (TTY), síťový terminál (VTY) - telnet.

Fyzické porty switche se označují (adresují) typem, dnes hlavně fastEthernet (stačí f) a gigabitEthernet (stačí g), a číslem portu. Číslo portu je řetězec, který má tvar podle typu switche. Nejčastější je {slot}/{port} nebo {stack}/{slot}/{port}. Běžné (nemodulární) switche jsou brány, jako by byli ve slotu 0, takže příklad adresace (třeba pro switch C2690) je f0/1 a je jím označen fastEthernetový (10/100Mbit/s) port číslo 1. Stohovatelné switche, jako je třeba C3750, adresujeme například g1/0/1, což označuje gigabitový port, který je na prvním switchi ve stacku (nebo samostatně), slot 0 a port 1.

Konfigurace portů

Výběr portu

Když chceme konfigurovat nějaký interface/port, tak se z privilegovaného módu přepneme do konfigurace daného portu. Pro zjednodušení můžeme konfigurovat i více portů naráz.

```
SWITCH(config)#interface f0/5                // p?epneme se na kofiguraci portu 5
SWITCH(config)#interface range f0/1-5,g0/1  // vybereme porty 1 až 5 (fast) a 1
(gigabit)
```

Stav portu, vypínání

Port může být v několika stavech (mohli bychom dělit fyzicky stav portu a stav linky):

* vypnutý - down/disabled - nejde přes něj žádná komunikace
* vypnutý chybou - error-disabled - nejde přes něj žádná komunikace, informuje o chybě
* zapnutý nespojený - notconnect - fyzicky nepřipojený, po zapojení komunikuje
* zapnutý spojený - up/connected - funkční a komunikující

Pro přepínání stavu mezi vypnutým a zapnutým slouží příkazy

```
SWITCH(config-if)#shutdown    // vypnutí portu
SWITCH(config-if)#no shutdown // zapnutí portu
```

Pokud je port v error-disabled stavu, kam se může dostat díky chybě v spanning tree nebo port

security, je třeba jej nejprve vypnout a pak teprve zapnout. Uvádí se, že ve výchozím stavu jsou interface vypnuté (shutdown), ale není to pravda úplně vždy. Doporučuji nepoužívané porty vypínat (nejlépe globálně při úvodní konfiguraci) a při konfiguraci portu jej vždy zapnout.

Základní vlastnosti portu

Pro port můžeme nastavovat obecné vlastnosti jako je duplex, rychlost, popis, MDIX a další.

```
SWITCH(config-if)#duplex full
SWITCH(config-if)#speed 100
SWITCH(config-if)#description 3.14
SWITCH(config-if)#mdix auto
```

Switchport

Parametry, které se týkají charakteristik přepínání, jsou pod příkazem switchport. Port může pracovat ve třech módech:

* access - typicky pro PC, přijímá netagované pakety (bez určení VLANy) a zařazuje je do jedné VLANy
* trunk - jiný switch či aktivní prvek, komunikace je tagována a přenáší se vybrané VLANy
* dynamic - vyjednává o stavu portu

```
SWITCH(config-if)#switchport mode access
```

Access mode

Pokud je port v přístupovém módu, měli bychom jej zařadit do správné VLANy. Ve výchozím stavu jsou všechny porty ve VLAN 1.

```
SWITCH(config-if)#switchport access vlan 100
```

Trunk mode

Trunk mode slouží primárně k tomu, abychom více switchů propojili mezi sebou a komunikace zůstala ve správné VLANě. Pokud bychom switche propojili access portem, tak by se přenášela pouze komunikace ve VLANě, ve které by byl nastaven daný port a na druhém switchi by byl paket ve VLANě tohoto portu.

Pokud je port v trunk módu, je bodů pro konfiguraci více. U vyšších modelů switchů (obecně L3 switchů a výše) volíme metodu, kterou se k paketům dopňuje informace o zařazení do VLANy. K dispozici máme

* IEEE 802.1q - standardizovaná metoda, kterou podporují všechny switche. Funguje na principu tzv. tagování, do hlavičky paketu přidá 4B informaci (2B - 0x8100 = je to 802.1q/802.1p, 2B - priorita + číslo VLANy) a přepočítá CRC. Používá se také pro QoS.
* Cisco ISL - Cisco proprietární metoda, kterou podporují pouze vyšší řady switchů. Vezme celý původní paket a zabalí jej (encapsulate) jako obsah nového paketu. Přidává tedy 30B k obsahu.

SWITCH(config-if)#switchport trunk encapsulation dot1q

Následně musíme určit, které VLANy chceme, aby se přenášeli v daném trunku. Zadáním čísla VLANy (nebo čísel oddělených čárkou) provedem nastavení a předchozí hodnoty se smažou. Můžeme využít také pomocná klíčová slova add, remove, all, none, except.

```
SWITCH(config-if)#switchport trunk allowed vlan 100,200
```

```
SWITCH(config-if)#switchport trunk allowed vlan add 300
```

Souvisejícím údajem je nastavení nativní VLANy, ta slouží k přenosu paketů, které nebyly zařazeny do žádné VLANy. Jinak řečeno, pokud do portu, který je nakonfigurován jako trunk, připojíme normální stanici (která nepodporuje trunk), tak bude komunikovat v této VLANě. Ve výchozím nastavení je to VLAN 1. Důležité je, aby na obou stranách trunku byla nastavena stejná nativní VLANa.

```
SWITCH(config-if)#switchport trunk native vlan 1
```

Port security

Port security je jednoduchá a zajímavá metoda zabezpečení přístupu do sítě. Na portu, kde je nastavena, kontroluje, zda pakety přichází z povolené MAC adresy. Pokud tedy uživatel připojí do zásuvky jiné zařízení, nebude moci komunikovat.

Pro nastavení Port security musí být port ve statickém módu (ne dynamic). Zapnutí port security pro daný port:

```
SWITCH(config-if)#switchport port-security
```

Můžeme nastavit kolik MAC adres pro port (nebo VLANu) je povoleno (například pokud je do portu připojen switch), maximum je 132.

```
SWITCH(config-if)#switchport port-security maximum 1
```

Pokud nezadáme žádné povolené MAC adresy, tak se používají adresy dynamicky (dočasně se ukládají pro aktuální komunikaci až do maxima). Nebo můžeme MAC adresy zadat ručně jako statické adresy. U dynamických adres můžeme nastavit, aby se tyto adresy ukládaly jako statické.

```
SWITCH(config-if)#switchport port-security mac-address 0018.DEDA.2990 // pevná adresa
SWITCH(config-if)#switchport port-security mac-address sticky         // ukládat
dynamické adresy
```

Dále volíme, co se děje při porušení pravidel, tedy pokud přijde komunikace z MAC adresy, která není povolena (a dosáhlo se maxima). Možnosti jsou:

* protect - nepovolená komunikace je zahazována, povolené MAC adresy stále komunikují
* restrict - pošle informativní SNMP trap
* shutdown - port se zablokuje, přepne do stavu Error-disabled (připomínám, že pro opětovné zapnutí je třeba jej nejprve vypnout)

```
SWITCH(config-if)#switchport port-security violation shutdown
```

Pozn.: K porušení pravidel dojde také v případě, kdy je MAC adresa zadaná pro určitý port a tato adresa se objeví na jiném portu tohoto switche.

Pokud se port přepne do Error-disabled stavu, tak je třeba zásah administrátora, aby jej opět zapnul. Je však možno nastavit i automatické znovuzapnutí portu po určité době:

```
SWITCH(config)# errdisable recovery cause psecure-violation
SWITCH(config)# errdisable recovery interval 60              // ?as v sekundách, 60
- 86400
```

Pokud chceme, aby se MAC adresy pro port po určité době automaticky smazaly, můžeme použít klíčové slovo aging v řadě variant. Například pokud chceme, aby dynamické adresy měly platnost 10 minut:

```
SWITCH(config-if)#switchport port-security aging time 10
```

Ve výchozím stavu po zapnutí Port security, je povolena jedna MAC adresa, která se používá dynamicky, tedy první zařízení, které začne komunikovat. Pokud se pokusí komunikovat další

zařízení, dojde k zablokování portu.

Hlavní příkazy pro zobrazení informací o Port security jsou

```
SWITCH#show port-security                  // info pro všechny interface
SWITCH#show port-security address          // tabulka MAC adres a související info
SWITCH#show port-security interface f0/1  // detailní info pro ur?itý interface
```

Protected port

Mezi porty, které jsou nastaveny jako Protected se neposílá žádná komunikace na Layer 2 (broadcast, multicast, unicast), pouze komunikace na Layer 3 (tedy s IP adresou).

```
SWITCH(config-if)#switchport protected
```

Spanning-tree

Protokol SPT - Spanning Tree Protocol slouží k zabránění vzniku smyček v síti, například u redundantní topologie nebo při chybném propojení switchů. Jedná se o standardizovaný protokol IEEE 802.1d, ke kterému existuje řada vylepšených verzí. Funguje na principu nalezení nejkratší cesty v ohodnoceném grafu a nepotřebné porty zablokuje. Nebudu se zde hlouběji zabývat SPT, pouze zmíním jedno nastavení pro port, jelikož SPT i bez konfigurace běží a je výhodnější jej nechat spuštěný.

Pokud je k danému portu switche připojeno zařízení jako server či pracovní stanice a tudíž na tomto portu nemůže vzniknout smyčka, tak můžeme tento port nastavit do módu portfast, který zabrání úvodnímu blokování portu.

```
SWITCH(config-if)#spanning-tree portfast
```

Nastavení IP adresy a brány

Některým interfacům můžeme nastavit IP adresu, hlavně se jedná o VLANy. Tato adresa slouží primárně ke komunikaci se switchem, ale také pro další služby, jako je routování nebo DHCP server. Zjednodušeně můžeme říct, že nastavujeme adresu switchi. Pokud nepoužíváme VLANy, tak ji musíme nastavit na VLANu 1. V opačném případě je vhodné mít speciální VLANu pro správu a zde nastavit IP adresu.

Adresu můžeme nastavit napevno nebo ji nechat přiřazovat DHCP serverem. Pokud nastavujeme adresu napevno, musíme ji zadat spolu s maskou sítě, v které je tato adresa platná (to je z důvodu dalších služeb).

```
SWITCH(config)#interface vlan 1
SWITCH(config-if)#ip address 192.168.190.2 255.255.255.0
```

V některých případech potřebujeme nastavit adresu brány (gateway address). Pokud budeme se switchem komunikovat pouze z lokálního subnetu, tak to není třeba. V opačném případě musíme adresu nastavit, aby switch věděl kam posílat odpovědi. Brána se nastavuje pro celý switch.

```
SWITCH(config)#ip default-gateway 192.168.190.1
```

Na závěr - ukládání konfigurace

Důležité upozornění. Na závěr konfigurace je třeba provedené změny uložit do startup konfigurace, abychom o ně při restartu nepřišli.

```
SWITCH#copy running-config startup-config       // uložit
```

```
Destination filename [startup-config]?       // dotaz na jméno, stiskn?te ENTER
Building configuration...
[OK]
```

Příklady nastavení

Nastavení portu pro uživatele

```
SWITCH>enable                                // p?epnutí do privilegovaného módu
SWITCH#configure terminal                    // p?epnutí do konfigurace
SWITCH(config)#interface f0/1                // konfigurace daného portu switche
SWITCH(config-if)#shutdown                   // doporu?eno nejprve vypnout port, m?l
již být vypnutý
SWITCH(config-if)#switchport mode access     // port do p?ístupového módu
SWITCH(config-if)#switchport access vlan 100 // za?adit do pat?i?né VLANy
SWITCH(config-if)#description 3.14           // popis portu
SWITCH(config-if)#spanning-tree portfast     // do zásuvky je zapojen po?íta?, rychlý
náb?h
SWITCH(config-if)#no shutdown                // zapnutí portu
SWITCH(config-if)#exit                       // o úrove? zp?t
SWITCH(config)#exit                          // o úrove? zp?t
SWITCH#copy running-config startup-config       // uložit
Destination filename [startup-config]?       // dotaz na jméno, stiskn?te ENTER
Building configuration...
[OK]
```

Zrušení nastavení portu

Tímto postupem se vrátí zpět úvodní konfigurace portu. V řadě případů stačí port zablokovat (shutdown) a ostatní hodnoty nechat nastavené.

```
SWITCH>enable                                // p?epnutí do privilegovaného módu
SWITCH#configure terminal                    // p?epnutí do konfigurace
SWITCH(config)#interface f0/1                // konfigurace daného portu switche
SWITCH(config-if)#shutdown                   // vypnutí portu
SWITCH(config-if)#no switchport mode access  // zrušení  p?ístupového módu
SWITCH(config-if)#switchport access vlan 1   // za?adit do defaultní VLAN
SWITCH(config-if)#no description             // zrušit popis portu
SWITCH(config-if)#no spanning-tree portfast  // zrušení portfastu
SWITCH(config-if)#exit                       // o úrove? zp?t
SWITCH(config)#exit                          // o úrove? zp?t
SWITCH#copy running-config startup-config       // uložit
Destination filename [startup-config]?       // dotaz na jméno, stiskn?te ENTER
Building configuration...
[OK]
```

pozn. redakce: nebo také SWITCH(config)#default interface ...

Nastavení portu pro propojení mezi switchi - trunk

```
SWITCH>enable                                // p?epnutí do privilegovaného módu
SWITCH#configure terminal                    // p?epnutí do konfigurace
SWITCH(config)#interface g1/0/25             // konfigurace daného portu switche
SWITCH(config-if)#shutdown                   // doporu?eno nejprve vypnout port, m?l
již být vypnutý
SWITCH(config-if)#switchport trunk encapsulation dot1q   // nastavení metody
```

```
dopl?ování informací o VLAN, norma 802.1q, nastavuje se pouze na vyšších modelech
switch?
SWITCH(config-if)#switchport trunk allowed vlan 2-200    // které VLANy se p?enáší
SWITCH(config-if)#switchport trunk native vlan 1         // rámce bez VLANy se
p?enáší p?es trunk v Native VLAN
SWITCH(config-if)#switchport mode trunk    // port do TRUNK módu
SWITCH(config-if)#switchport nonegotiate   // nevyjednává se trunk protokolem DTP
SWITCH(config-if)#description 3.14         // popis portu
SWITCH(config-if)#no shutdown              // zapnutí portu
SWITCH(config-if)#exit                     // o úrove? zp?t
SWITCH(config)#exit                        // o úrove? zp?t
SWITCH#copy running-config startup-config       // ložit
Destination filename [startup-config]?     // dotaz na jméno, stiskn?te ENTER
Building configuration...
[OK]
```

Stejnou konfiguraci je třeba provést na druhé straně, tedy na druhém switchi a portu, kterým jsou propojeny.

Nastavení Port Security

```
SWITCH>enable                                          // p?epnutí do
privilegovaného módu
SWITCH#configure terminal                              // p?epnutí do konfigurace
SWITCH(config)#interface f0/5                          // konfigurace daného portu
switche
SWITCH(config-if)#switchport port-security             // zapneme port security
SWITCH(config-if)#switchport port-security maximum 1     // po?et MAC adres
SWITCH(config-if)#switchport port-security violation shutdown // p?i porušení
zablokovat port
SWITCH(config-if)#switchport port-security mac-address sticky // napevno uložit
dynamickou MAC adresu
SWITCH(config-if)#exit                                 // o úrove? zp?t
SWITCH(config)#exit                                    // o úrove? zp?t
SWITCH#copy running-config startup-config                        // uložit
Destination filename [startup-config]?                 //  dotaz na jméno,
stiskn?te ENTER
Building configuration...
[OK]
```

Samuraj, http://www.samuraj-cz.com/ [3]

URL článku:
https://www.security-portal.cz/clanky/cisco-ios-3-nastaven%C3%AD-interfaceportu-access-trunk-port-security

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/