Cisco IOS 10 - Rapid Spanning Tree Protocol

Vložil/a Samuraj [1], 17 Leden, 2013 - 11:08

- Networks & Protocols [2]

Tento článek přímo navazuje na předchozí díl, kde byl popsán obecně STP protokol a konfigurace PVSTP. V tomto díle je mnohem stručnější popis, hlavně zaměřený na konfiguraci, dvou novějších verzí STP, tedy RSTP a MSTP. Popisuje také moje praktické zkušenosti s přechodem na RSTP. A je zde malá zmínka o Flex Link.

Rapid Spanning Tree Protocol (RSTP)

Maximální čas, kdy konverguje STP je 50s (v praxi můžeme dosáhnout nižších hodnot, ale tak okolo 30s), což je pro praktické situace příliš vysoká hodnota. Proto byl vymyšlen upravený algoritmus zvaný ***Rapid Spanning Tree Protocol*** (RSTP), který má čas konvergence v praxi kolem 1 či 2s. RSTP byl původně definován jako rozšíření normou IEEE 802.1w, ale v roce 2004 byl zařazen do normy IEEE 802.1d.

Základní princip je podobný klasickému STP, ale je upraven pro rychlejší konvergenci při změně topologii. Má integrován ekvivalent Cisco funkcí *PortFast*, *UplinkFast* a *BackboneFast*.

Pozn.: RSTP je zpětně kompatibilní s klasickým STP. Ale pokud detekuje nějaký BPDU rámec z STP, tak se přepne do tohoto módu.

Změny oproti STP

- drobná změna formátu BPDU (používá se verze 2)
- všechny switche generují BPDU a posílají je na všechny porty každý hello time (místo přeposílání Root BPDU)
- posílají se Agreement / Proposal BPDU
- pro linky se definuje jejich typ (point-to-point, edge, shared), takže některé mohou rychle přejít do stavu *forwarding*
- změnily se role/typy portů, jsou čtyři (root, designated, alternate, backup)
- stavy portů (discarding, learning, forwarding)

Typy portů/linek

- **point-to-point**, tedy spoj bod-bod, připojení dalšího switche, linka musí být full duplex
- **edge**, koncový/hraniční port (PortFast), je do něj připojeno koncové zařízení (jako PC či tiskárna)
- **shared**, sdílená linka, například hub, linka je half duplex

Edge porty definujeme pomocí funkce *PortFast*. ***Point-to-point*** a ***shared*** konfigurujeme pomocí *link-type*. Výchozí stav pro full duplex linky je ***P2P.*** Pro P2P musíme zaručit, aby byla linka ve full duplex módu.

Role portů

- **Root Port** - nejlepší BPDU na switchi
- **Designated Port** - nejlepší BPDU na segmentu
- **Alternate Port** - blokovaný, alternativní cesta k rootu (záloha root)
- **Backup Port** - blokovaný, redundantní cesta k segmentu (záloha designated)

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

BPDU

velikost [B]	položka
2	protokol ID
2	verze protokolu
2	typ BPDU
1	příznaky
8	root BID
4	cena cesty k rootu
8	odesílatelovo BID
2	ID portu, který posílá BPDU
2	Message Age
2	Maximum Age
2	Hello Time
2	Forward Delay
1	Verison 1 length

Pozn.: Switch, na kterém běží klasický STP, zahazuje BPDU z RSTP.

Všechny switche posílají BPDU každý hello time, u STP se přeposílají/modifikují BPDU přijaté na Root Portu. Message Age slouží jako počítadlo hopů, po vyčerpání je rámec zahozen.

Agreement / proposal

Nabídka a souhlas. Switche posílají nabídku sousedovi, pokud má soused větší BID, tak odpoví souhlasem a oba přenastaví stav (root a designed).

Konfigurace RSTP na Cisco IOSu

Na Cisco switchích běží upravená verze RSTP protokolu označovaná jako ***Rapid PVSTP+*** (používá se zkratka RPVSTP či PVRSTP či rapid-PVSTP), kdy pro každou VLANu běží samostatná instance STP.

Běžný, a asi jediný možný, postup konfigurace spočívá v tom, že se nejprve nakonfiguruje ***PVSTP+*** (ten běží defaultně) a pak se přejde do módu ***RPVSTP+***. Přechod může být postupný (asi nedokážeme nakonfigurovat všechny switche najednou), protože RSTP je zpětně kompatibilní s STP. Je důležité pamatovat na to, že při přechodu dojde k výpadkům spojení.

V rapid-PVST neexistují funkce ***UplinkFast*** a ***BackboneFast***, pokud se přepneme do RSTP, tak se tyto funkce nepoužijí, přesto se doporučuje je vypnout.

```
SWITCH(config)#no spanning-tree uplinkfast
SWITCH(config)#no spanning-tree backbonefast
```

Pro přechod z PVST módu do rapid PVST stačí jediný příkaz.

SWITCH(config)#spanning-tree mode rapid-pvst

Určování typu linky se provádí na jednotlivých portech

```
SWITCH(config-if)#spanning-tree portfast                // mód portu edge
SWITCH(config-if)#spanning-tree portfast trunk          // pokud je port trunk a
chceme jej nastavit jako edge
SWITCH(config-if)#spanning-tree link-type point-to-point // mód portu P2P
SWITCH(config-if)#spanning-tree link-type shared        // mód shared
```

Po tom, co nastavíme všechny switche do RPVST, tak budou pracovat stále v módu PVST, protože migrační proces zjistí, že soused je v módu PVST a kvůli kompatibilitě se nepřepne. Switch nepozná,

že se již může přepnout do RPVST, musíme vyvolat znovu vyjednávání o protokolu. Následující příkaz restartuje migrační proces.

SWITCH#clear spanning-tree detected-protocols

Poznámky z praktického nasazení RSTP

Uvedu pár praktických poznámek, když jsem přecházel z ***PVSTP+*** na ***Rapid PVSTP+*** na asi 13 Cisco switchích. V této síti nejsou žádné úmyslné smyčky a STP se používá jednoduše, pokud by omylem vznikla smyčka.

Nejvíce mne zajímalo, jak vlastně bude probíhat celý přechod (kdy k němu dojde) a jaké budou výpadky. Přesné odpovědi jsem nikde na netu nenašel (ani v Cisco článku, který popisuje tuto migraci). Ve všech informacích se zdůrazňuje, že při přechodu dojde k výpadkům. A také se zdůrazňuje, že pokud switch v RSTP detekuje BPDU z STP, tak se přepne do STP (myslím Cisco verze) a již se nedokáže přepnout zpět do RSTP. Pro přepnutí pak musíme využít výše uvedený příkaz. Proto mě nebylo jasné, když postupně přepnu switche do RSTP, jak vyvolat nové vyjednávání na všech najednou. No v praxi to vypadalo následně.

Na začátku jsem měl na všech switchích koncové porty nakonfigurované pomocí PortFast. Překonfiguraci switchů jsem začal na ***access switchích*** (ne od jádra, jak se doporučuje u MST). Většina portů neměla ani žádný výpadek a zůstala stále ve stavu ***forwarding***. ***Edge porty*** byly nakonfigurovány, většina ostatních (tam, kde jsou další Cisco switche) se automaticky nastavila do ***P2P***. Pokud jsem se podíval pomocí show spanning-tree, tak byly označeny **P2P Peer(STP)**, to znamená, že sousední switch je v ***STP módu***. Pouze pár portů prošlo stavy od ***blocking***, ale velmi rychle. Na těchto portech byl většinou nějaký malý switch (a občas se port nastavil do Shared).

Po tom, co jsem nakonfiguroval všechny *access switche*, jsem přešel na ***core switch***. Přepnutí proběhlo obdobně jako ostatní switche. Ale následně již všechny ***P2P porty*** byly označeny pouze jako **P2P**, takže by měly pracovat v **RSTP** módu. Ještě jsem zkusil sledovat nějakou komunikaci pomocí debug spanning-tree bpdu a show logging a zde jsem viděl, že se posílají ***RSTP BPDU***, takže asi vše automaticky přešlo do **RSTP módu**.

Pokud někdo víte, jak se pozná, jestli switch pracuje opravdu v RSTP (a ne v RSTP přepnutém do STP), či jiné podrobnosti, tak uvítám info.

Multiple Spanning Tree Protocol (MSTP)

MSTP vznikl jako rozšíření RSTP a byl definován v IEEE 802.1s, ale v roce 2003 byl sloučen do normy IEEE 802.1q, která popisuje VLANy (MSTP s VLANy přímo souvisí). Jako základ používá ***RSTP***, ale navíc dovoluje seskupovat VLANy do ***spanning-tree instancí*** (takže pro každou skupinu běží samostatná instance STP). Díky tomu dovoluje využít více cest a provádět jednoduchý *load balancing* (rozdělování zátěže, ale statické). Standardně dovoluje MSTP vytvořit až 65 různých rozdílných logických topologií (instancí).

Cisco PVSTP má vždy jednu STP instanci pro jednu VLAN, tedy čím více VLAN, tím více STP instancí a tím větší zatížení switche. Klasické STP (či RSTP) má oproti tomu pouze jednu STP instanci pro všechny VLANy, což znamená menší HW náročnost, ale existuje pouze jedna virtuální topologie a nemůžeme tedy rozdělit zátěž pro různé VLANy různou cestou.

Důležitým termínem u MSTP je ***MST region***. Ten je tvořen skupinou switchů, které mají stejnou konfiguraci (stejně mapované instance na VLANy). Jednotlivé regiony nebo switche bez MSTP jsou dohromady propojeny klasickým STP. Takže, aby se switch stal součástí regionu (a tedy se účastnil MSTP), tak musí mít stejnou konfiguraci jako ostatní (to znamená stejné jméno regionu, číslo revize a mapování VLAN na instance).

MST instance představuje mapování VLAN do skupin (jak bylo zmíněno dříve). V jednom regionu můžeme vytvořit řadu instancí (čísla 0 až 4094, ale maximálně 65 instancí) se skupinami VLAN.

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

Defaultně jsou všechny VLANy zařazeny do instance 0 (MST00).

Při přechodu na MSTP nebo změně zařazení VLAN do MST instance dojde k reinicializaci a tudíž krátkému výpadku spojení. Převod z PVST na MST by se měl provádět od jádra (centrálního prvku) a postupovat dolů.

Konfigurace MSTP na Cisco IOSu

Pro přepnutí MST stačí jeden příkaz. Defaultně jsou všechny VLANy v jedné instanci (číslo 0). Lepší je nejprve provést konfiguraci instancí a pak teprve přepnou switch.

SWITCH(config)#spanning-tree mode mst

Konfigurace regionu a instancí se provádí v MST konfiguračním módu.

```
SWITCH(config)#spanning-tree mst configuration // p?epnutí do módu
SWITCH(config-mst)#show                          // informace o regionech
SWITCH(config-mst)#name region1                  // pojmenování konfigurace/regionu
SWITCH(config-mst)#revision 10                 // revizní ?íslo konfigurace
SWITCH(config-mst)#instance 1 vlan 100, 150    // vytvo?ení instance a za?azení VLAN,
využijeme poml?ku a ?árku
```

Další řada (ladících) parametrů se nastavuje pro celý switch nebo port.

```
SWITCH(config)#spanning-tree mst 0 root primary          // nastaví switch jako root
pro danou instanci
SWITCH(config)#spanning-tree mst 0 priority 32768        // nastaví prioritu switche
pro danou instanci
SWITCH(config)#spanning-tree mst hello-time 1       // nastaví hello time
SWITCH(config-if)#spanning-tree mst 0 port-priority 64   // nastaví prioritu portu
```

Zobrazení informací o MST.

SWITCH#show spanning-tree mst

Flex Link

Jenom stručně se zmíním o zajímavé funkci ***Flex Link***, která nesouvisí s STP. Jedná se pouze o jednoduchou funkci, kdy mám dvě linky a jedna je definována jako záložní. Komunikace jde normálně pouze po primární lince, ale ve chvíli, kdy tato vypadne, se přepne na záložní linku. Výhodou je, že čas přepnutí je do 50ms.

Konfiguruje se na primárním interfacu (může to být port nebo EtherChannel) a určujeme jeho záložní.

SWITCH(config-if)#switchport backup interface f0/2

Pro zobrazení informací o Flex Linku můžeme použít.

SWITCH#show interface switchport backup

Zajímavé odkazy

- Spanning tree protocol [3] - popis STP na Wikipedii
- Cisco - Understanding Rapid Spanning Tree Protocol (802.1w) [4] - pěkný popis funkce RSTP
- Understanding Multiple Spanning Tree Protocol (802.1s) [5] - pěkný popis funkce MSTP

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

- Configuring STP Features [6] - popis příkazů
- Configuring STP [7] - vysvětlení a popis příkazů STP, speciálně pro Catalyst 2960
- Configuring STP [8] - vysvětlení a popis příkazů STP, speciálně pro Catalyst 3750
- Spanning Tree from PVST+ to Rapid-PVST Migration Configuration Example [9]
- Configuration example to migrate Spanning Tree from PVST+ to MST [10]
- Configuring Flex Links [11]

URL článku: https://security-portal.cz/clanky/cisco-ios-10-rapid-spanning-tree-protocol

Odkazy:
[1] https://security-portal.cz/users/samuraj
[2] https://security-portal.cz/category/tagy/networks-protocols
[3] http://en.wikipedia.org/wiki/Multiple_Spanning_Tree_Protocol
[4] http://www.cisco.com/warp/public/473/146.html
[5] http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfc.shtml
[6] http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080160a5c.html
[7] http://www.cisco.com/en/US/products/ps6406/products_configuration_guide_chapter09186a00805a762d.html
[8] http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_sec/configuration/guide/swstp.html
[9] http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a00807b0670.shtml
[10] http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a00807b075f.shtml
[11] http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_sec/configuration/guide/swflink.html

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