Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky

Projekt do SPS

Otestování speciálních vlastností přepínači Cisco Catalyst:

- *port security*
- *protected port*
- *broadcast storm control*
- *Flexlink*
- *private VLAN*
- *Unidirectional Link Detection (UDLD)*

Tomáš Jílek – JIL022
Lukáš Kašpar – KAS167
Ladislav Rozsíval – ROZ089

Security port

Prvním pojmem, kterým jsme se v projektu zabývali, byl port security. Security portů se užívá k blokování vstupu na jednotlivých portech přepínače.. K blokování portu přepínače dojde, pokud se o přístup na daný port pokusí jiná než povolená MAC adresa. Na každém portu přepínače lze nastavit jedna výchozí MAC adresa. Kromě této adresy má přepínač ještě paměť pro uložení dalších MAC adres, které lze rozdělit mezi porty podle potřeby (počet adres závisí na typu přepínače). Tyto adresy mohou být přiděleny například jednomu portu, anebo rozloženy po celém přepínači.

Postup při nastavování adres portům

Nejprve si alokujeme pro daný port požadovaný počet MAC adres, následně přiřadíme portu jednotlivé MAC adresy. To můžeme provést buď manuálně nebo nechat port ať se naučí MAC adresy dynamicky z připojených zařízení. Případně některé nastavit manuálně a zbytek nechat naučit automaticky. Pokud port „spadne“, tak se dynamicky naučené MAC adresy vymažou. Port na přepínači může být nastaven ve třech režimech: shutdown, protect, restrict mode (viz. tabulka nastavení).

Port Security se Sticky MAC Addresses je novější verze port security. Má mnoho stejných výhod jako port security se statickými MAC adresami ale Sticky MAC adresy mohou být naučeny dynamicky a po odpojení linky si udrží dynamicky naučené bezpečné MAC adresy v startup-config souboru. Security port se tak nemusí dynamicky učit znova bezpečné MAC adresy.

Na novějších přepínačím se můžeme setkat se tzv. port security se Sticky. Jehož výhoda spočívá v tom, že si jednotlivé MAC adresy, které byly dynamicky naučené, stále udržuje v paměti.

Výchozí nastavení portů

Vlastnost	Výchozí nastavení
Port security	Zakázáno
Maximum number of secure MAC addresses	1
Violation mode	Vypnuto
Sticky address learning	Zakázáno
Port security aging	Zakázáno (0)

Nastavení portu security

	Příkaz	Význam
Step 1	**configure terminal**	Privilegovaný režim
Step 2	**interface** *interface-id*	Konfigurace rozhraní
Step 3	**switchport mode access**	Nastavení módu jako access
Step 4	**switchport port-security**	Přepnutí portu do security
Step 5	**switchport port-security maximum** *value*	Nastavení počtu MAC, kterým povolíme přístup na port.
Step 6	**switchport port-security violation** {**protect** | **restrict** | **shutdown**}	Pokud na port přistupuje jiná než povolená MAC adresa, pak lze nastavit jedna z těchto možností : **protect** Pokud počet povolených adres dosáhne nastaveného limitu, všechny pakety s neznámou adresou jsou zahazovány. **restrict** stejný jako protect, avšak navíc je oznámeno, že o přístup se pokusila nepovolená MAC adresa, zpráva zapsána do syslogu. **shutdown** V tomto modu port security způsobuje, že pokud se o přístup pokusí nepovolená MAC adresa, port se přepne do chybového stavu a vypne se LED dioda portu.
Step 7	**switchport port-security mac-address** *mac-address*	Tento příkaz slouží pro statické nastavení povolené MAC adresy na daném portu. Příkaz opakujte pro každou požadovanou MAC adresu. Pokud zadáte méně než maximum zbytek do maxima se naučí dynamicky.
Step 8	**switchport port-security mac-address sticky**	Povolení port security se Sticky
Step 9	**end**	Návrat
Step 10	**show port-security**	Ověření konfigurace

Příklad

Příklad jak nastavit max. 50 adres se Sticky

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
```

```
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end
```

Příklad jak nastavit jednu statickou MAC adresu a zbytek se naučí dynamicky

```
Switch# configure terminal
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address 00:E0:4C:73:14
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end
```

Zhodnocení

Port security byl odzkoušen na přepínači Cisco 2950 v módu shutdown. Test byl proveden tak, že jsme připojili 2 PC k přepínači na port 1 a 2. Port 1 jsme přepnuli do security módu s povolenou MAC adresou prvního PC. Dostupnost PC byla prověřena echo zprávami. Po přepojení prvního PC do portu 2 a druhého PC do portu 1, echo zprávy už neměli odezvu, protože MAC adresa druhého PC nebyla povolena pro port 1.

UDLD - Unidirectional Link Detection

UDLD protokol pracující na druhé vrstvě spolupracuje s mechanismy první vrstvy, které slouží k fyzickému zjištění stavu linky. Jedná se o detekci jednosměrných spojení a následné odpojení portu. Jednosměrné spojení znamená, že jedna strana přijímá a nemůže vysílat, a druhá strana naopak. Pokud je tedy provoz pouze jednosměrný, tak je port odpojen úplně. Možnost konfigurace UDLD je buď globální, pro celý přepínač, anebo pro jednotlivé porty. Konfigurace pro jednotlivé porty má vyšší prioritu než konfigurace globální.

Výchozí nastavení UDLD

Vlastnost	Výchozí nastavení	Význam
UDLD global enable state	Zakázáno	Globální stav UDLD
UDLD per-interface enable state for fiber-optic media	Zakázáno pro optická vlákna	Stav UDLD
UDLD per-interface enable state for twisted-pair (copper) media	Zakázáno pro Ethernet 10/100 a 1000BASE-TX rozhraní	Stav UDLD
UDLD aggressive mode	Zakázáno	Stav UDLD v agresivním módu

Nastavení UDLD

	Příkaz	Význam
Step 1	**configure terminal**	Privilegovaný režim
Step 2	**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*}	Specifikace módu UDLD: • **aggressive -** povolení UDLD v agresivním režimu pro všechny optické vlákna. • **enable -** povolení UDLD v normálním režimu pro všechna optická vlákna.UDLD ve výchozím nastavení je zakázán. • **message time** *message-timer-interval* **-** Rozsah posílání zpráv je možno nastavit od 7 do 90 sekund. Pozn. Toto nastavení platí pouze pro optická vlákna. Pro další rozhraní je nutno použít konfiguraci na rozhraní.
Step 3	**end**	Návrat
Step 4	**show udld**	Ověření konfigurace

Povolení UDLD na rozhraní

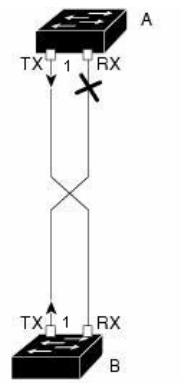
	Příkaz	Význam
Step 1	**configure terminal**	Privilegovaný režim
Step 2	**interface** *interface-id*	Konfigurace rozhraní
Step 3	**udld port** [**aggressive**]	S použitím volitelného parametru **agressive** aktivujeme na daném portu agresivní mód. Bez tohoto parametru je port v modu **enable**. **aggressive** - aktivuje UDLD v agresivním módu na daném rozhraní. Ve výchozím nastavení je UDLD vypnuté.
Step 4	**end**	Návrat
Step 5	**show udld** *interface-id*	Ověření konfigurace

Reset konfigurace nastavení UDLD

- reset všech rozhraní, které byly vypnuty UDLD

	Příkaz	Význam
Step 1	**udld reset**	Reset pro všechna rozhraní
Step 2	**show udld**	Ověření konfigurace

Příklad funkce



Když UDLD je v agresivním režimu, při detekci problému se zavře port. Pokud se nachází UDLD v normálním režimu, logická linka je považována za neurčitou a interface nebude zavřen.

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# udld port aggressive enable
Switch(config-if)# end
```

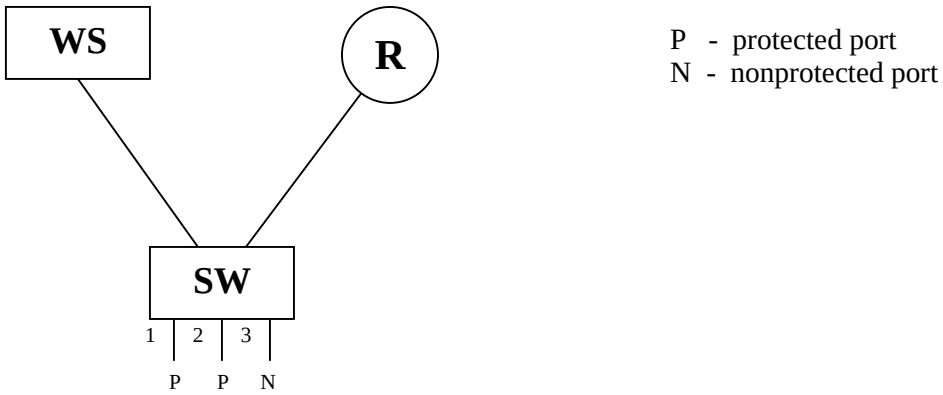
Protected port

Protected port – v překladu chráněný port, se užívá pokud chceme zabránit komunikaci mezi zařízeními připojenými do jednoho přepínače. Dva protected porty mezi sebou nemohou navzájem komunikovat. Komunikace je povolena jen mezi protected portem s neprotected portem. Kdyby jsme chtěli komunikovat dvěma protected porty mezi sebou, tak musí jít komunikace přes L3 zařízení. Jedná se tedy o omezení komunikace na druhé vrstvě.

Nastavení protected na rozhraní

	Příkaz	Význam
Step 1	**configure terminal**	Privilegovaný režim
Step 2	**interface** *interface-id*	Konfigurace rozhraní
Step 3	**switchport protected**	Nastavení port jako protecte port
Step 4	**end**	Návrat
Step 5	**show interfaces** *interface-id* **switchport**	Ověření nastavení

Příklad užití protected portů



Obr. 1

Na obrázku 1 jsou nastaveny porty jedna a dva jako protected a port tři nikoliv. Pokud budou chtít komunikovat port jedna s portem dva, tak komunikace neproběhne. Pokud bude komunikovat port tři s prvním nebo druhým portem, bude komunikace probíhat.

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport protected
Switch(config-if)# end
```

Zhodnocení

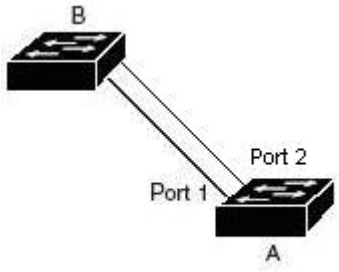
Výše uvedený příklad byl odzkoušen na přepínači Cisco 2950. Test byl proveden tak, že jsme připojili 3 PC k přepínači na porty 1, 2 a 3. Port 1 a 2 jsme nastavili jako protected porty. Dostupnost PC byla prověřena echo zprávami. Vše fungovalo tak jak bylo očekáváno, jelikož

komunikace probíhala pouze mezi portem 3 a některým ze zbylých dvou portů a komunikace mezi porty 1 a 2 nebyla možná.

Flex links

Flex linky – používají se pro redundantní připojení. Nejčastějším využitím je připojení k poskytovateli internetu, kde nahrazují spaning tree. Jedna linka je zálohou druhé. Když hlavní linka „spadne“, tak druhá se stane hlavní a veškery provoz jde přes ni. Až druhá linka opět naběhne, tak se stane záložní linkou pro hlavní linku. Jedna hlavní linka může mít pouze jednu linku záložní. Jedna záložní linka může být zálohou pro více hlavních linek.
Při pádu primární linky je přechod na záložní linku okamžitý, při testování podle uvedené architektury nebylo žádné zpoždění zaznamenáno.
Testování bylo provedeno na přepínači Cisco Catalyst 3560.

Příklad užití flex linků



obr. 2

Switche A,B jsou zapojeny podle topologie na obrázku 2. Porty 1 a 2 z A jsou připojeny ke switchi B. Port 1 je nakonfigurován jako primární linka. Port 2 je nakonfigurován jako její záložní linka. Protože porty 1 a 2 jsou nakonfigurovány jako Flex linky, pouze jeden port propouští provoz a druhý je v záložním režimu. V našem případě je to Port 1 a tedy provoz mezi A a B jde přes port jedna. Pokud rozpojíme linku z portu jedna, tak se zapne port 2 a provoz začne procházet přes něj. Pokud port 1 znovu zapojíme přejde do záložního režimu a provoz bude dál procházet port 2.

Nastavení flex link na rozhraní

	Příkaz	Význam
Step 1	**configure terminal**	Privilegovaný režim
Step 2	**interface** *interface-id*	Konfigurace rozhraní Layer 2 nebo port channel. Port-channel od 1 do 6.
Step 3	**switchport backup interface** *interface-id*	Konfigurace Layer 2 rozhraní (nebo port channel). Když linka je v forwarding traffic, nebo rozhraní pak je v módu standby.
Step 4	**end**	Návrat
Step 5	**show interface** [*interface-id*] **switchport backup**	Ověření konfigurace

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2
Switch(conf-if)# end
Switch# show interface switchport backup
```

Zhodnocení

Flex links byly odzkoušeny na dvou přepínačích Cisco 2950. Test byl proveden podle výše uvedeného příkladu. Na každý z přepínačů jsme připojili jedno PC a pustili mezi nimi echo zprávy. Komunikace bez problému probíhala. Odpojili jsme primární linku z portu 1 a provoz téměř okamžitě přešel na záložní linku a komunikace mezi PC probíhala dál bez problémově. Po zpětném připojení linky do portu 1 se tato linka opravdu nastavila jako záložní k lince z portu 2 a na komunikaci mezi PC to nemělo žádný vliv. Při odpojení a následném připojení linky z portu 2 se linky vrátili do původního nastavení. Vše fungovalo jak mělo a test proběhl úspěšně.

TSC - Traffic storm control

„Rámcová bouře“ nastane, když velké množství broadcast, unicast, nebo multicast paketů přichází na port. Přeposílání těchto paketů může způsobit zpomalení nebo celkovou nedostupnost sítě z důvodu přetížení přepínače. Storm control je konfigurována na switchi jako na celku, ale funguje na portové bázi. Ve výchozím nastavení je vypnuta. Strom control používá zvyšování a snižování hranic blokování a poté obnovení přeposílání paketů. Můžete také nastavit port tak, aby se odpojil při překročení nastavené hranice pro povolené zatížení portu.
Storm control používá kapacitu linky k změření provozu. Hranice jsou vyjádřené jako procento celkové šířky pásma, které může být použito k provozu broadcast, unicast, nebo multicast paketů.
Rostoucí hranice storm control je procento z celkové šířky pásma, od kterého je přeposílání blokováno. Klesající hranice je procento celkové kapacity linky, do které switch normálně přeposílá pakety. Obecně, vyšší hranice menší efektivní ochrana proti broadcast storm.

Nastavení traffic storm na rozhraní

	Příkaz	Význam
Step 1	**configure terminal**	Privilegovaný režim
Step 2	**interface** *interface-id*	Konfigurace rozhraní
Step 3	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **pps** *pps* [*pps-low*]}	For level - specifikuje rostoucí hranici pro broadcast, multicast nebo unicast provozu jako procento šířky pásma. Storm control nastane, když provoz dosáhne tuto hranici. For level-low - specifikuje rostoucí hladinu jako procento šířky pásma. Tato hodnota musí byt menší než rising supression hodnota. Normální přenos se restartuje, když traffic klesne pod tuto úroveň. For pps - specifikuje rostoucí hranici pro broadcast, multicast nebo unicast v paketech za sekundu. Storm control nastane, když provoz přesáhne tuto hranici. Tato volba je dostupná jen na non-LRE Catalyst 2950 switches běžících na Cisco IOS Release 12.1(14)EA1 a pozdějších. For pps low - specifikuje klesající hranici v paketech za sekundu které může byt mensi nebo rovno rostoucí prahová hladina. Normální přenos se restartuje, když traffic klesne pod tuto úroveň. Tato volba je dostupná pouze na

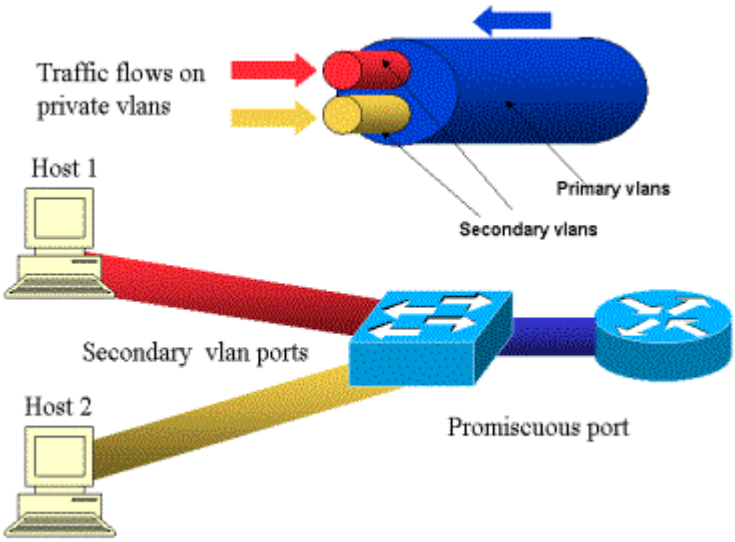
		non-LRE Catalyst 2950 switches Pro pps a pps low je rozsah od 0 do 4294967295.
Step 4	**storm-control action** {**shutdown** | **trap**}	Specifikuje akci, která se použije když nastane storm. Defaultní je odfiltrováni traficu a neposílaní. **shutdown** - error-disable stav portu během storm. **trap** - generováni SNMP trap když nastane storm.
Step 5	**end**	Návrat
Step 6	**show storm-control** [**interface**] [{**broadcast** | **history** | **multicast** | **unicast**}]	Ověření konfigurace

Příklad konfigurace traffic storm na portu 1

```
Switch # configure terminal
Switch (config)# interface fastethernet 0/1
Switch (config-if)# storm-control multicast level 70.5
Switch (config-if)# end
```

Private VLANs (PVLANs)

Privátní VLANy poskytují mechanismus ke kontrole, která zařízení smí vzájemně komunikovat uvnitř podsítě. Privátní VLANy používají oddělené (isolated) a společné (community) vedlejší VLANy ke kontrole s kým zařízení komunikuje.

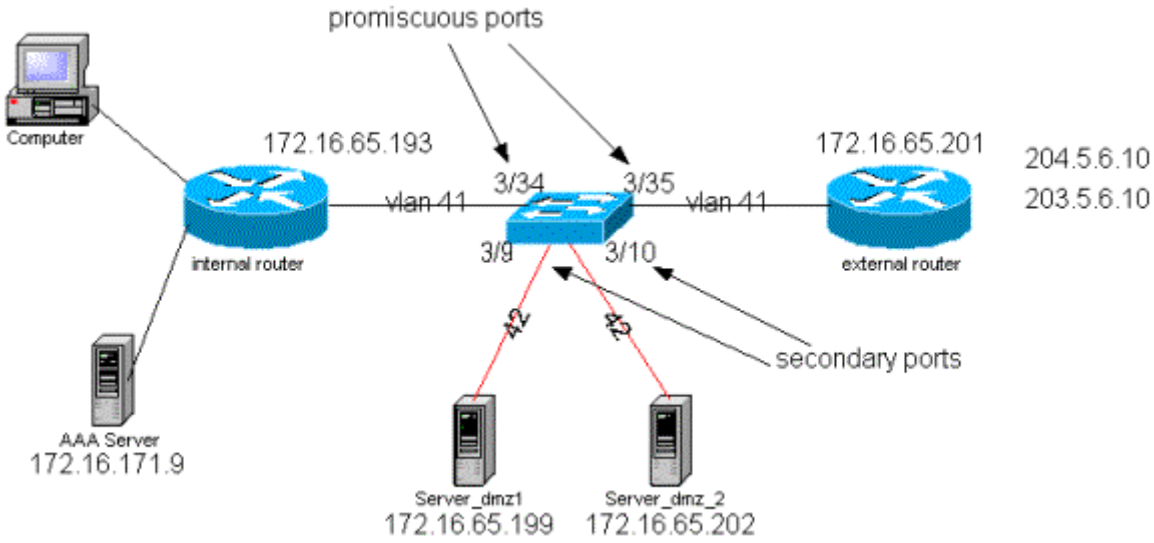


obr. 3

Jak je vidět z obrázku 3, tak vedlejší VLANy (červená a žlutá) jsou přiřazeny hlavním (modrá) VLANům a porty jsou přiřazeny k sekundárním VLANům. Porty v oddělených VLANech nemohou komunikovat s žádným zařízením ve VLAN, než promiscuous portem.
V PVLAN jsou promiscuous porty přiřazeny do primární VLAN, zatímco community a isolated porty patří do sekundární VLAN. PVLAN mohou mít jen jeden primární VLAN, ale několik sekundárních VLANů. Provoz, který přichází do switche z promiscuous portu může být switchem přeposlán do všech portů, které patří do stejné primární VLAN. Provoz, který přichází do switche z portu mapovaného do sekundární VLAN, může být přeposílán na promiscuous port nebo na port patřící do stejné společné (community) VLAN.

Switch port, který je součástí PVLAN může být konfigurován jedním ze tří způsobů:
- Promiscuous port – komunikuje s jakýmkoliv portem
- Isolated port – komunikuje pouze s promiscuous portem
- Community members – komunikuje s promiscuous portem a dalšími členy společné vedlejší VLAN

Tento způsob je jedním z nejužívanějších scénářů použití PVLAN:



obr. 4

V příkladě na obrázku číslo 4 předpokládáme, že DMZ servery budou přístupné uživatelům z venku a ze vnitř sítě, ale nebudou mezi sebou navzájem komunikovat. Ve stejném příkladu DMZ servery potřebují otevřít nějaký druh spojení na interního hostitele a současně vnitřní klient chce přistupovat na internet. Dobrý příklad je, že jeden ze serverů je web server, který potřebuje přistupovat k databázovému serveru uvnitř stejné sítě a zároveň být přístupný uživatelům zvenku.
Firewall na externím routeru je nastaven aby povoloval příchozí spojení na servery umístěné v DMZ, ale obvykle není nastaven žádný filtr na odchozí spojení. Protože DMZ servery nepotřebují spolu komunikovat navzájem, tak je doporučeno je izolovat na L2. Porty serveru (3/9 a 3/10) budou nastaveny jako izolované porty, zatímco porty připojené k routerům (3/34 a 3/35) budou nastaveny jako promiscuous porty. Definujeme primární VLANy (vlan41) pro routery a sekundární VLAN (42) pro DMZ servery připojené k nim.

Zhodnocení

Private Vlany nebyly odzkoušeny, protože dostupné switche je nepodporovaly.