

Monitorovanie prevádzky

Na Cisco prepínačoch





Monitorovanie prevádzky

- Mnohokrát je potrebné odchytiť si komunikáciu prebiehajúcu na niektorých portoch
- Cisco má na toto účely funkciu
 - SPAN
 - Local SPAN
 - VLAN SPAN
 - RSPAN
 - (Remote) Switched Port ANalyzer
- Pointa:
 - Definuje sa tzv. monitorovacia relácia (session)
 - Táto relácia hovorí,
 - Čo sa odchyťáva (port alebo celá VLAN)
 - zdroj
 - Kam sa odchytené dáta posielajú (iný port alebo iná VLAN)
 - Cieľ
- **Odchyťávanie sieťovej komunikácie na prepínačoch Cisco Catalyst**
 - <http://nil.uniza.sk/sk/>



Vytvorenie local SPAN

- SPAN je relácia, v ktorej sa prevádzka z lokálnych portov alebo VLAN odosiela na zvolený lokálny port

```
Switch(config)# monitor session 1 source interface Fa0/1  
Switch(config)# monitor session 1 destination interface Gi0/1
```

- Cieľový port nie je viac použiteľný pre bežnú komunikáciu (vstupujúce rámce zahadzuje)
 - Je možné dovoliť spracovať aj bežné vstupujúce rámce príkazom

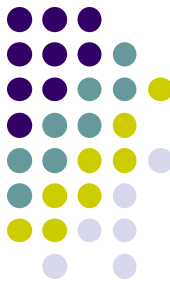
```
Switch(config)# monitor session 1 dest int Gi0/1 ingress vlan 1
```

- Aby bolo možné vidieť aj Layer2 obslužné protokoly (CDP, DTP, VTP, STP, PAgP, LACP, ...) a aby rámce odchádzali s pôvodným VLAN tagom, je potrebné výstupný port nakonfigurovať príkazom

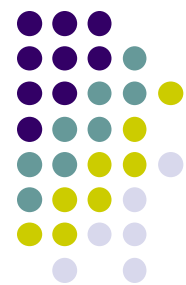
```
Switch(config)# monitor session 1 dest int Gi0/1 encap replicate
```

- Bez tohto príkazu zachytené rámce budú všetky „untagged“ a servisné protokoly nebudú odchyťované

Overenie local SPAN



```
switch(config)# end
switch# show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports        :
Both                : Fa3/1
Destination Ports   : Gi0/1
Encapsulation       : Native
Ingress             : Disable
```

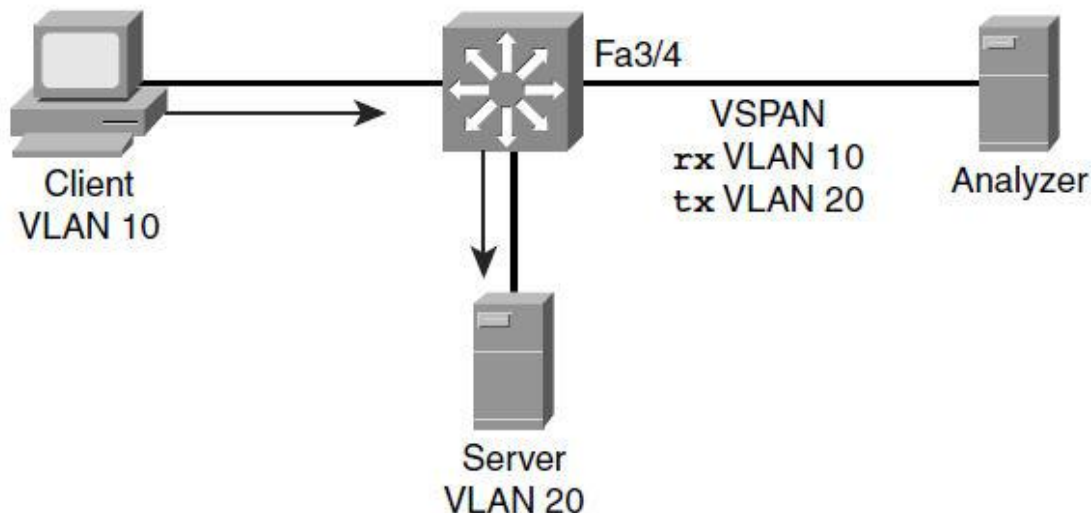


Pravidlá pre local SPAN

- Ako zdrojový a cieľový port môžu byť použité prepínané aj smerované porty
- Daný port môže byť použitý ako cieľový len pre jednu SPAN reláciu
- Port nemôže byť použitý ako cieľový ak je nakonfigurovaný ako zdrojový
- Port channel rozhranie (EtherChannel) môže byť zdrojom ale nie cieľovým portom pre SPAN
- Zdrojové porty môžu byť v rôznych VLAN
- Cieľový port neparticipuje v STP
 - Nepripájať na iný prepínač aby nevznikla slučka!

VLAN SPAN

- Vhodné ak chceme monitorovať tok medzi jednou a druhou VLAN



• Príklad

- Diagnostika toku medzi serverom vo VLAN 20 a klientom vo VLAN 10

```
Switch(config)# monitor session 1 source vlan 10 rx
Switch(config)# monitor session 1 source vlan 20 tx
Switch(config)# monitor session 1 destination interface FastEthernet 3 /4
Switch # show monitor session 1
Session 1
-----
Type                               : Local Session
Source VLANs                       :
    RX Only   : 10
    TX Only   : 20
Destination Ports : Fa3/4
Encapsulation    : Native
Ingress          : Disabled
```

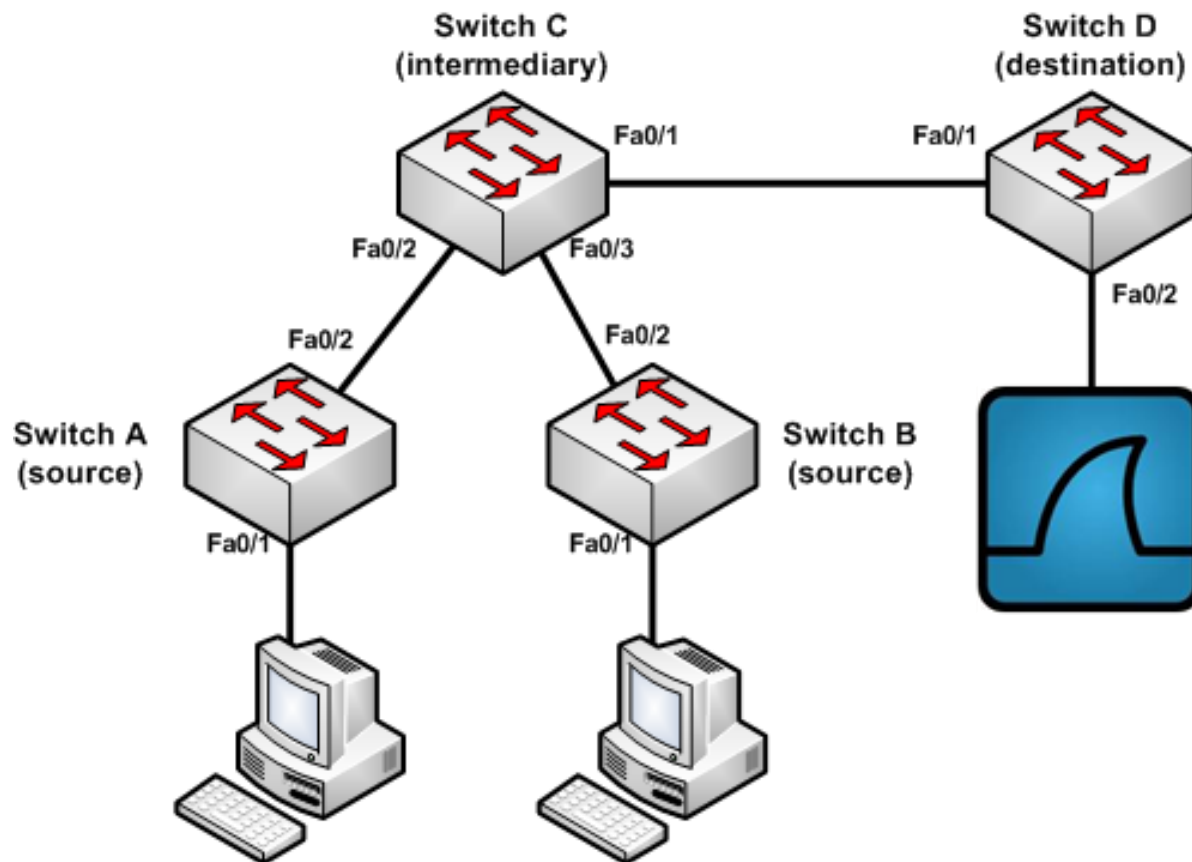


Pravidlá pre VSPAN

- VSPAN sessions, with both ingress and egress options configured, forward duplicate packets from the source port only if the packets get switched in the same VLAN.
- One copy of the packet is from the ingress traffic on the ingress port, and the other copy of the packet is from the egress traffic on the egress port.
- VSPAN monitors only traffic that leaves or enters Layer 2 ports in the VLAN:
 - Routed traffic that enters a monitored VLAN is not captured if the SPAN session is configured with that VLAN as an ingress source because traffic never appears as ingress traffic entering a Layer 2 port in the VLAN.
 - Traffic that is routed out of a monitored VLAN, which is configured as an egress source in a SPAN session, is not captured because the traffic never appears as egress traffic leaving a Layer 2 port in that VLAN.

Monitoring s RSPAN

- Remote SPAN (RSPAN) je veľmi podobné klasickému SPAN
- Ale podporuje situáciu, kde zdrojový port, zdrojová VLAN a cieľový port môžu byť na rôznych prepínačoch



Vytvorenie RSPAN



- RSPAN je dvojica relácií
 - Na zdrojovom switchi sa zachytáva prevádzka na lokálnych portoch alebo VLAN a odosiela sa do špeciálnej RSPAN VLAN
 - Na cieľovom switchi sa zachytená prevádzka z RSPAN VLAN odosiela na zvolený lokálny port
 - RSPAN VLAN je vyhradená len na účely RSPAN

```
Source(config)# vlan 999
Source(config-vlan)# remote-span
Source(config-vlan)# exit
Source(config)# monitor session 1 source interface Fa0/1
Source(config)# monitor session 1 source vlan 123
Source(config)# monitor session 1 destination remote vlan 999
```

```
Dest(config)# vlan 999
Dest(config-vlan)# remote-span
Dest(config-vlan)# exit
Dest(config)# monitor session 1 source remote vlan 999
Dest(config)# monitor session 1 destination interface Gi0/1
```



OTÁZKY?