



Ako negociovať trunk?

Protokol DTP



EURÓPSKA ÚNIA

Európsky sociálny fond
Európsky fond regionálneho rozvoja



OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE



MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Na pripomenutie ...

Skúsme si zodpovedať nasledujúce otázky:

- Čo je to virtuálna sieť VLAN?
- Aké režimy portu prepínača poznáme?
- Aký je medzi nimi rozdiel?
- Ako umožníme prenos viacerých VLAN cez jednu linku medzi prepínačmi?



Obsah

Prečo použiť DTP?

Základy DTP

DTP režimy

Aktivita 7.1

Problémy DTP

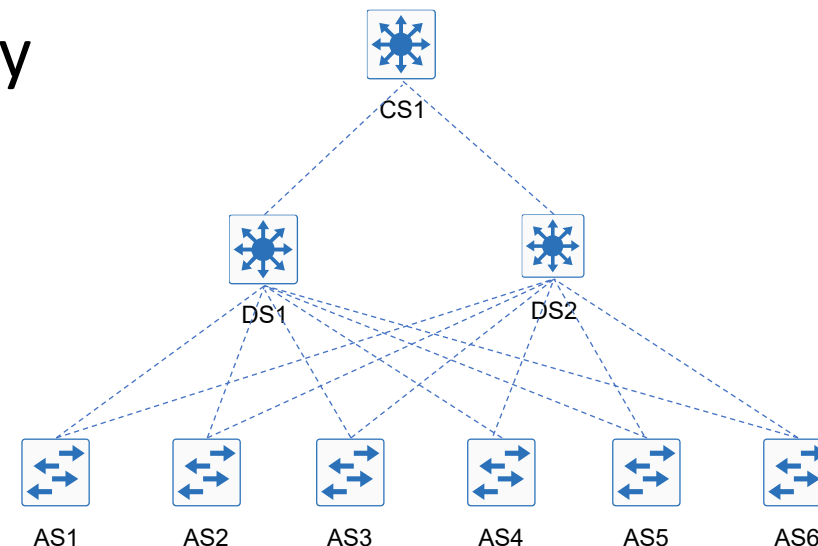
Vypnutie DTP

Aktivita 7.2



Prečo použiť DTP?

- Distribučná a jadrová vrstva hierarchického modelu zvyčajne nemajú prístupové porty (porty fungujú v režime trunk).
- Pri manuálnom vytváraní trunk liniek je potrebné sa pripojiť na všetkých 9 prepínačov a zmeniť režim príslušných portov



- Pri použití DTP postačuje sa pripojiť na DS1 a DS2 a zmeniť režim ich portov, režim portov ostatných prepínačov nastaví protokol DTP.

Základy DTP

- DTP (angl. Dynamic trunking protocol) riadi negociáciu trunk režimu na portoch danej linky (ak príslušné porty podporujú DTP).
- DTP funguje len na Cisco zariadeniach, pri vytváraní trunk linky so zariadením od iného výrobcu, je potrebné vypnúť DTP.

DTP režimy	Dynamic auto	Dynamic desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Obmedzená konektivita
Access	Access	Access	Obmedzená konektivita	Access

DTP režim dynamic auto

```
Switch(config-if)# switchport mode dynamic auto
```

- Umožňuje dynamicky zmeniť režim portu.
- Prispôsobí sa, ale **neiniciuje** vytvorenie trunk linky.
- Port sa prepne do režimu trunk, ak príslušný port susedného prepínača na danej linke je nastavený ako trunk alebo dynamic desirable.

DTP režim dynamic desirable

```
Switch(config-if)# switchport mode dynamic desirable
```

- Umožňuje dynamicky zmeniť režim portu.
- Prispôsobí sa, pričom **iniciuje** vytvorenie trunk linky.
- Port sa prepne do režimu trunk, ak príslušný port susedného prepínača na danej linke je nastavený ako trunk, dynamic desirable alebo dynamic auto.

DTP režim access

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

- Staticky nastaví prístupový režim portu.
- Oznamuje, že **odmieta** vytvorenie trunk linky.
- Port bude v prístupovom režime bez ohľadu na konfiguráciu príslušného portu susedného prepínača na danej linke.

DTP režim trunk

```
Switch(config-if)# switchport mode trunk
```

- Staticky prepne port do režimu trunk.
- **Iniciuje** nastavenie trunk režimu aj u suseda.
- Port bude v režime trunk bez ohľadu na konfiguráciu príslušného portu susedného prepínača na danej linke.

Overenie DTP režimu

```
Switch# show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking
  Encapsulation: dot1q
Operational Trunking Encapsulation:
  native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1
  (default)
Voice VLAN: none
Administrative private-vlan host-
  association: none
Administrative private-vlan mapping:
  none
Administrative private-vlan trunk
```

```
  native VLAN: none
Administrative private-vlan trunk
  encapsulation: dot1q
Administrative private-vlan trunk
  normal VLANs: none
Administrative private-vlan trunk
  private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Overenie DTP režimu

```
Switch# show dtp interface f0/1
```

```
DTP information for FastEthernet0/1:
```

```
TOS/TAS/TNS: TRUNK/ON/TRUNK
```

```
TOT/TAT/TNT: 802.1Q/802.1Q/802.1Q
```

```
Neighbor address 1: 0CD996D23F81
```

```
Neighbor address 2: 000000000000
```

```
Hello timer expiration (sec/state):  
12/RUNNING
```

```
Access timer expiration (sec/state):  
never/STOPPED
```

```
Negotiation timer expiration  
(sec/state): never/STOPPED
```

```
Multidrop timer expiration (sec/state):  
never/STOPPED
```

```
FSM state: S6:TRUNK
```

```
# times multi & trunk 0
```

```
Enabled: yes
```

```
In STP: no
```

```
Statistics
```

```
-----
```

```
640 packets received (640 good)
```

```
0 packets dropped
```

```
0 nonegotiate, 0 bad version, 0  
domain mismatches,
```

```
0 bad TLVs, 0 bad TAS, 0 bad TAT, 0  
bad TOT, 0 other
```

```
646 packets output (646 good)
```

```
640 native, 6 software encap isl, 0  
isl hardware native
```

```
0 output errors
```

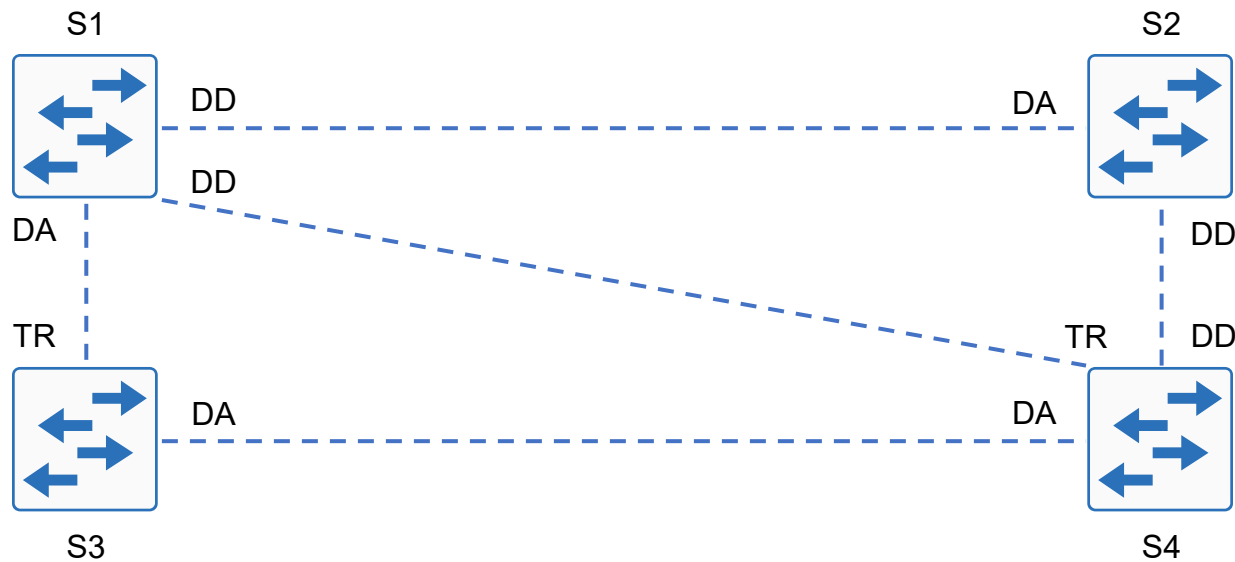
```
0 trunk timeouts
```

```
1 link ups, last link up on Mon Mar 01  
1993, 00:00:56
```

```
0 link downs
```

Aktivita 7.1: Negociácia trunk režimu

Ktorá kombinácia DTP režimov na portoch medzi prepínačmi zabezpečí vytvorenie trunk linky?



Legenda

TR – trunk
DA – dynamic auto
DD – dynamic desirable

Pre zadanie úlohy vid'
m07-a01-zadanie.pdf

?

Problémy DTP

- Predvolený dynamický režim na prepínačoch môže byť zneužitý na zmätenie prepínača (angl. switch spoofing attack).
- Útočník môže na pôvodne prístupovom porte zaslať DTP správu a dohodnúť vytvorenie trunk linky.
- Útočník získa prístup do všetkých VLAN povolených na trunk linke.



- **Odporúčané je používať statické režimy a vypnúť DTP.**
- **Nepoužívané porty administratívne vypnúť.**

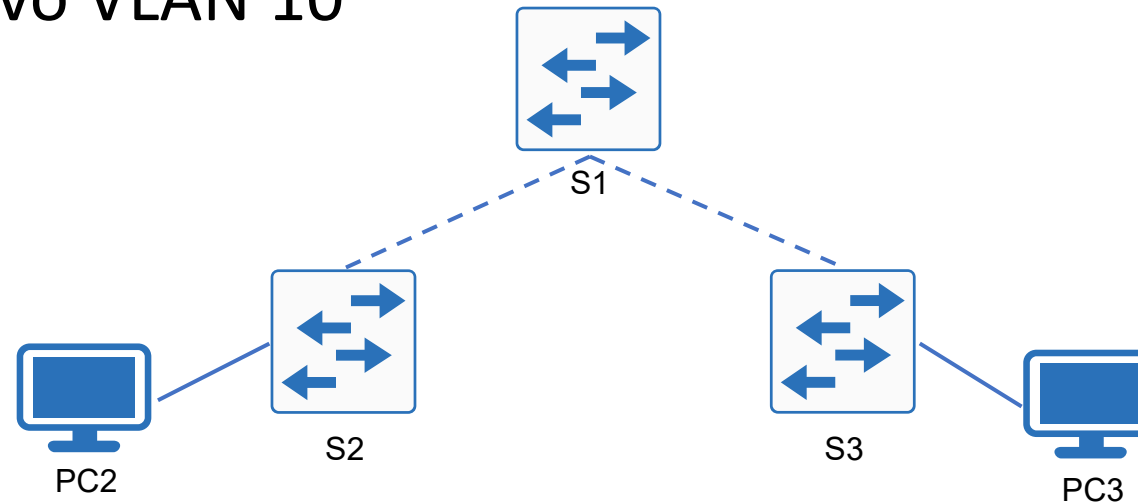
Vypnutie DTP

```
Switch(config-if)# switchport nonegotiate
```

- Port prestane generovať a spracovávať DTP správy.
- Príkaz je možné použiť len ak nie je nastavený dynamický DTP režim.
- Po vypnutí DTP je na vytvorenie trunk linky potrebné prepnúť obidva porty danej linky manuálne do statického trunk režimu.

Aktivita 7.2: Základná konfigurácia DTP

- Vytvorte trunk linky medzi prepínačmi pomocou DTP
- Prepínače komunikujú vo VLAN 99
- Počítače komunikujú vo VLAN 10



Pre zadanie úlohy vid'.
m07-a02-zadanie.pdf



