Module 2 – Virtual LAN

SWITCH Module 2 Defining VLANs

Virtuálne LAN (VLAN)

- Virtual LAN (VLAN)
  - VLAN sú samostatné, nezávislé broadcastové domény vytvárané iba logikou prepínača
  - VLAN umožňujú virtualizovať fyzické prepínané LAN siete
    - Bez VLAN tvorila jedna prepínaná infraštruktúra jednu prakticky nerozdeliteľnú sieť
    - Pri VLAN je prepínaná infraštruktúra zdieľaná medzi mnohé VLAN, no jednotlivé VLAN sú medzi sebou trvale oddelené
- Získame
  - Možnosť virtualizovať sieť
    - Nad jednou fyzickou infraštruktúrou vytvoriť množstvo logických
  - Oddelenie fyzickej (geografickej) topológie od logickej
  - Môžeme vytvárať LAN siete napr.
    - Podľa funkcií v organizácii, projektových tímov, aplikácií a pod.

Interná práca switcha s VLAN

- Implementovanie podpory VLAN z pohľadu logiky switcha je relatívne jednoduché
  - MAC tabuľka sa rozšíri o stĺpec VLAN
  - Riadok MAC tabuľky bude teda obsahovať informácie v tvare

    <VLAN> <MAC> <Port>
- Rámec vchádzajúci portom bude spracovaný podľa tohto postupu:
  - Ak je jeho MAC adresa neznáma, zaznačí sa do tabuľky aj vrátane VLAN, do ktorej patrí prístupový port, ktorým rámec vošiel
  - Príjemca sa bude hľadať len medzi tými riadkami MAC tabuľky, ktoré majú zhodné číslo VLAN ako port, ktorým rámec vošiel

Všeobecné výhody VLAN

- Jednoduché premiestňovanie pracovných staníc na LAN
- Jednoduché pridávanie staníc do LAN
- Jednoduchá zmena konfigurácie LAN
- Zvýšená bezpečnosť
  - Izolácia prevádzky na VLAN
  - Ľahká kontrola sieťovej prevádzky
    - Použitie smerovačov
  - Segmentácia siete
  - Redukcia propagácie broadcastov v sieti
- Šetrenie finančných prostriedkov na infraštruktúru

Typy VLAN – Cisco terminológia

- **Default VLAN**
  - Na Cisco Catalyst VLAN1
  - Default VLAN je večne živá – je nedotknuteľná
  - Všetky porty sú štandardne priradené do VLAN1
  - Viaceré obslužné protokoly komunikujú cez VLAN1
- **Native VLAN**
  - Špecifický pojem pre 802.1Q trunky
  - Dáta natívnej VLAN sú prenášané bez tagu
- **Management VLAN**
  - Má vytvorený a zapnutý „interface VLAN X“
  - Nemala by obsahovať user porty
  - Slúži pre účely vzdialeného manažmentu
- **Data VLAN**
  - Nesie používateľské dáta
- **Voice VLAN**
  - Oddelená pre VoIP
  - Niekedy „auxiliary VLAN“

Typy VLAN – podľa členstva portu

- **Statické**
  - Členstvo vo VLAN nastavuje administrátor manuálne
    - Priraďuje fyzický port prepínača do VLAN port po porte
    - Kým administrátor nezmení priradenie portu, port je členom danej VLAN
    - Každý port je členom nejakej VLAN
  - Známe aj ako port-based, port-centric
  - Výhodou je absolútna kontrola a deterministický dizajn, nevýhodou je vyššia administratívna náročnosť
- **Dynamické**
  - Dynamické určenie členstva na základe určitých kritérií, v okamihu keď sa host pripojí na port
    - Na základe:
      - **MAC adresy** pripojeného hosta (IP adresy, typ protokolu)
    - Vyžaduje sa **konfiguračný server** v sieti
      - Správne nakonfigurovaný VLAN Membership Policy Server (VMPS)
      - RADIUS spojený s 802.1X – otvorené riešenie

Spôsob návrhu VLAN

- VLAN poskytujú vynikajúcu flexibilitu
  - Nech sa používateľ vo firemnej sieti nachádza kdekoľvek, môže byť stále vo svojej VLAN
- Táto flexibilita však vedie k tomu, že VLAN sa rozprestiera nad celým campusom
  - Neprehľadné, zle udržiavateľné riešenie
- To viedlo k definovaniu dvoch základných paradigiem, ako sa VLAN vlastne majú vytvárať a ohraničovať
  - **End-to-End VLAN**
  - **Local VLAN**

End-to-End VLAN (Campuswide)

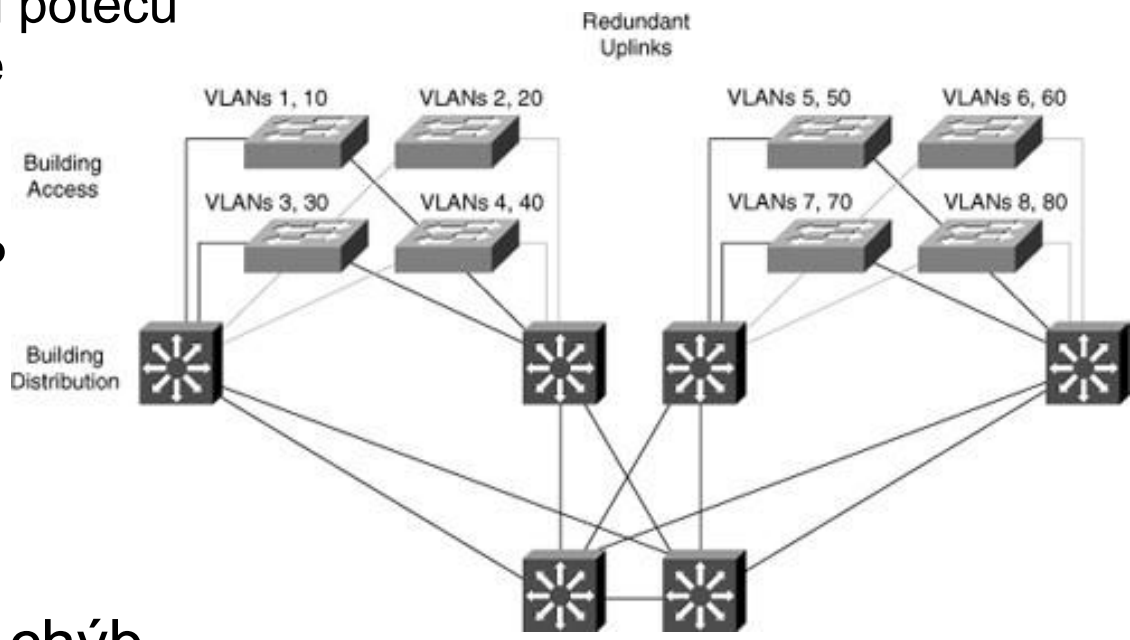
- Pôvodný koncept, ktorý odrážal pravidlo 80/20
  - Ktoré už dnes kvôli centralizácií serverov a Internetu neplatí
- VLAN sa rozprestierajú po celej sietí naprieč Access, Distro a Core vrstvou
  - Užívateľ v ľubovoľnej časti siete je stále v tej istej VLAN
- Užívatelia zgrupovaný skôr funkcionálne než geograficky
- **Výhody**
  - Extrémna flexibilita užívateľov
  - Prevádzka je prepínaná a nie smerovaná
  - Môžem definovať špeciálne VLAN podľa účelu (Voice, mcast, visitor)
- **Nevýhody**
  - Komplikovaný manažment (siete, užívateľov, tokov, STP, diagnostika)
    - VLAN definícia na všetkých prepínačoch
    - Broadcast a unknown cast ide naprieč Distro a Core vrstvou
    - Potencionálne pri L2 slučkách plytvanie zdrojov (BW a CPU) Distro a Core vrstvy
    - Vzhľadom na rozprestretie VLANy a užívateľov ťažšia diagnostika
  - Implementácia sa neodporúča, ak nie je na to dobrý dôvod

Local VLAN

- VLAN končí v rozvádzači (wiring closet)
  - Odráža skôr fyzické alebo geografické členenie siete
    - Preto nazývané aj geografické VLAN
  - Odráža pravidlo 20/80
    - Centralizácia serverov a internetového prístupu
- VLAN je ohraničená prístupovým a distribučným prepínačom v jednom rozvádzači
  - Distribučný prepínač pomocou L3 ***switchingu*** umožňuje prestup do inej VLAN
- Local VLANs sú v súčasnosti odporúčaný prístup
  - Menší rozsah VLAN znamená jej lepšiu spravovateľnosť, menšiu „failure domain“, jednoduchšie zabezpečenie redundancie atď.

Výhody Local VLAN

- Priamočiary dizajn
  - L2 a L3 cesty, ktorými potečú dáta, sú jednoduchšie
- Aktívna redundancia
  - (R)PVST alebo MSTP
  - IGP, FHRP
- Vysoká dostupnosť
  - Redundancia
- Ohraničenie výskytu chýb
  - Menšie skupiny používateľov
- Škálovateľný dizajn
  - Jednoducho rozšíriteľný



Rozdelenie rozsahov VLAN na Cisco Access prepínačoch

- **Normal Range VLANs**
  - VLANy sú identifikované VLAN ID 1 - 1005
  - ID od 1002 do 1005 sú rezervované pre Token Ring a FDDI VLAN
  - VLAN ID 1 a 1002 až 1005 sú automaticky vytvorené a *nemôžu byť zmazané*
  - Konfigurácia VLAN je uložená v databáze tvorenej súborom vlan.dat vo Flash pamäti
- **Extended Range VLANs**
  - VLAN ID je v rozsahu 1006 – 4094, typ iba Ethernet
  - Sú uložené v startup-config a ak je použitá VTPv3, aj vo vlan.dat
  - Konfigurovateľné
    - Vo VTP Transparent režime pri VTPv1 a v2
    - VTPv3 podporuje extended range VLANs v ľubovoľnom režime
- Cisco Cat2960 podporuje do 255 normálnych a rozšírených VLAN

Popdora VLAN v produktoch Cisco

Model	Max. No. of VLANs *	VLAN ID range
Catalyst 2940	4	1–1005
Catalyst 2950/2955	250	1–4094
Catalyst 2960	255	1–4094
Catalyst 2970/3550/3560/3750	1005	1–4094
Catalyst 2848G/2980G/4000/4500	4094	1–4094
Catalyst 6500	4094	1–4094

* Závisí aj od verzie IOS

VLAN ID rozsahy

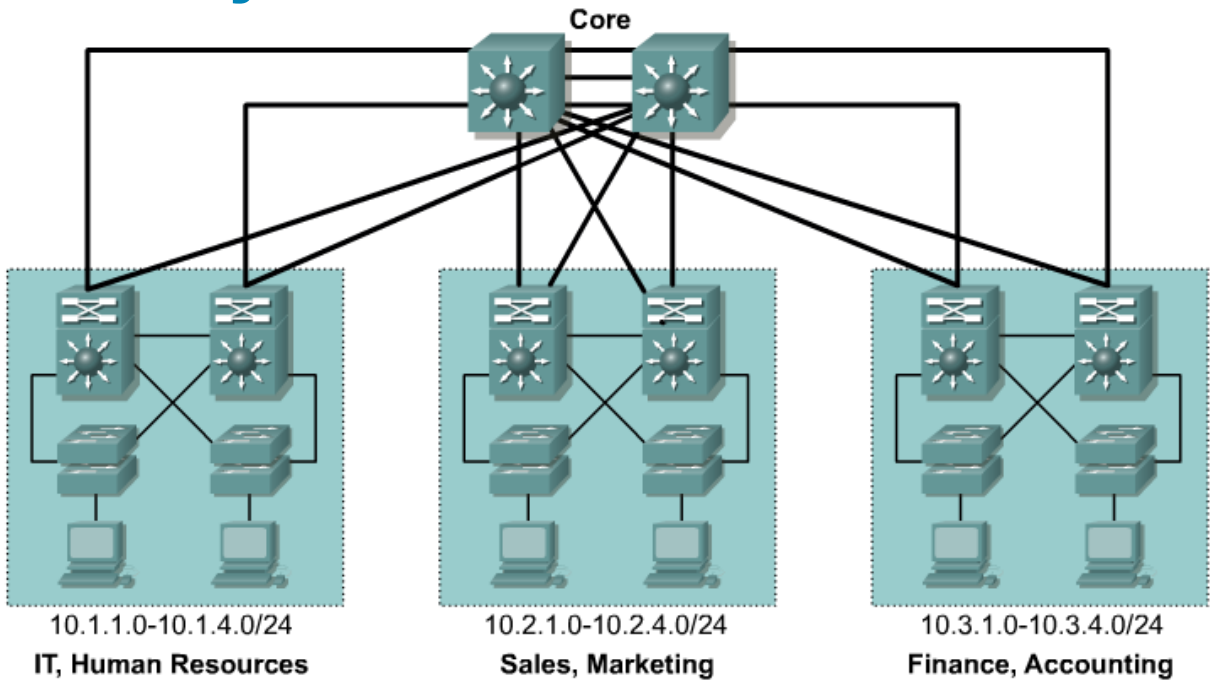
VLAN Ranges	Range	Use	VTP Propagated
0, 4095	Reserved	For system use only. VLANs cannot be seen or used.	—
1	Normal	Cisco default VLAN. This VLAN can be used but not modified or deleted.	Yes
2–1001	Normal	These VLANs can be created, used, and deleted.	Yes
1002–1005	Normal	Cisco defaults for FDDI and Token Ring. These cannot be deleted.	Yes
1006–4094	Extended	For Ethernet VLANs only. Layer 3 ports and some software features require internal VLANs. Internal VLANs are allocated from 1006 and up. You cannot use a VLAN that has been allocated for such use. To display the VLANs used internally, enter the **show vlan internal usage** command. Switches running Cisco Catalyst product series software do not support configuration of VLANs 1006-1024. If you configure VLANs 1006-1024, ensure that the VLANs do not extend to any switches running Cisco Catalyst product series software. You must enable the extended system ID to use extended-range VLANs.	No

VLAN – **Odporúčania pri návrhu VLAN**

Porozumej sieťovým tokom a službám

- Naplánuj/poznaj VLAN a ich účel
  - Dohľad a administrácia (CDP, SNMP, RMON)
  - IP telefónia
    - Signalizácia a hlasová prevádzka
    - Vytvorenie separátnych VLAN pre hlas, oddelenie od dát
    - Umiestnenie zariadení (zariadenie pre VoIP musia byť trvale dostupné)
  - IP multicast
    - Podpora potrebných protokolov (IGMP, PIM)
    - Kontrola nad multicast tokmi
    - Výber Rendezvous Point
  - Bežné dáta
  - „Scavenger“ dáta
    - Dáta prekračujúce istý kontrakt, napr. objem
    - Vlastná QoS trieda

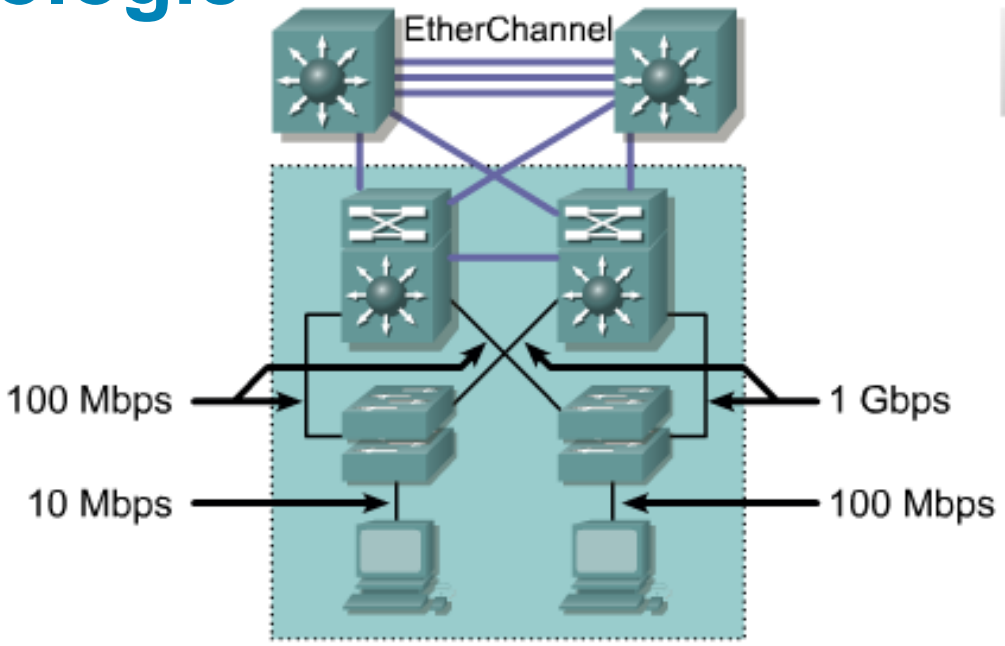
VLAN dizajn – adresovanie



- Alokuj IP adresný priestor v súvislých blokoch
  - Aby sa dala využiť „Route summarization“
- Alokuj jednu IP subnet per VLAN
  - Minimalizuješ chyby pri prideľovaní adries
- Daná VLAN by nemala prekračovať Core vrstvu
  - Eliminácia Bcast a Unknown cast
  - Urči/ujasni, kde ktoré VLAN budú definované

Odporúčané technológie

- Fast Ethernet
  - Koncové zariadenia k prístupovému switchu
- 1 GigaEthernet
  - Prepoj medzi access/distro
  - Prepoj medzi distro/core
  - Pripojenie serverov
- 10 GigaEthernet
  - Najmä v core vrstve
- Využitie EtherChannel



Zariadenia a prepoje

- Prepínače s primeraným výkonom, hustotou portov a ich typmi
- Zvážiť rast siete v budúcnosti
- Medzi access/distro prepínačmi dodržať agregáciu na úrovni menšej ako 20:1
- Medzi distro/core prepínačmi dodržať agregáciu na úrovni menšej ako 4:1

VLAN konfigurácia - príprava

Overenie základnej konfigurácie prepínača
show running-config

```
Switch>enable
Switch#show running-config
Building configuration...

Current configuration : 1215 bytes
!
version 12.2
service config
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Nejake_ine_meno
!
... Output omitted ...
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
```

Overenie základnej konfigurácie prepínača
show vlan

```
Switch#show vlan

VLAN  Name                                Status    Ports
----  ----------------------------------- --------- -------------------------
1     default                             active    Fa0/1, Fa0/2, Fa0/3,
                                                    Fa0/4, Fa0/5, Fa0/6,
                                                    Fa0/7, Fa0/8, Fa0/9,
                                                    Fa0/10, Fa0/11, Fa0/12,
                                                    Fa0/13, Fa0/14, Fa0/15,
                                                    Fa0/16, Fa0/17, Fa0/18,
                                                    Fa0/19, Fa0/20, Fa0/21,
                                                    Fa0/22, Fa0/23, Fa0/24
                                                    Gi0/1, Gi0/2
2     Nejaka_vlana                        active
1002  fddi-default                         act/unsup
1003  token-ring-default                   act/unsup
1004  fddinet-default                      act/unsup
1005  trnet-default                        act/unsup
... Output omitted ...
```

Overenie základnej konfigurácie prepínača
show flash

```
Switch#show flash
Directory of flash:/

    2  -rwx          616   Mar 1 1993 00:01:17 +00:00  vlan.dat
    7  drwx          192   Mar 1 1993 00:06:41 +00:00  c2960-
lanbase-mz.122-35.SE5

32514048 bytes total (24179200 bytes free)
```

Začiatok konfigurácie prepínača - zmazanie cudzej konfigurácie

- Pred začiatkom práce ak tam ostala cudzia konfigurácia môžeme vymazať nastavenia prepínača nasledujúcim spôsobom
  - Potrebné vymazať všetky VLAN informácie vymazaním VLAN databázy vlan.dat z Flash pamäte
    - `delete vlan.dat`
    - **POZOR: nerobiť `erase flash:`**
      - **Zmaže IOS!!!!!!!!**

```
Switch#show flash
Directory of flash:/

    2  -rwx          616   Mar 1 1993 00:01:17 +00:00  vlan.dat
    7  drwx          192   Mar 1 1993 00:06:41 +00:00  c2960-lanbase-
mz.122-35.SE5

32514048 bytes total (24179200 bytes free)
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#
```

Vymazanie prepínača pripojeného do väčšej živej siete

- Môže nastať situácia kedy zmazané VLAN (vlan.dat) sa nám neustále nanovo objavujú na prepínači (znovu naučením cez VTP)

```
Switch#conf t
Switch(config)#
Switch(config)#interface range FastEthernet 0/1 -24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range GigabitEthernet
0/1 -2
Switch(config-if-range)#shutdown
15:45:59: %LINK-5-CHANGED: Interface GigabitEthernet0/2,
changed state to administratively down
Switch(config-if-range)#exit
Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)#no vlan ID_VLANY
```

Implementácia statických VLAN

Postup pri vytváraní VLAN

- Postup:
  - Vytvorenie VLAN
  - Overenie VLAN konfigurácie
  - Priradenie portu/portov prepínača do VLAN
  - Overenie konfigurácie portov prepínača
  - Overenie funkčnosti VLAN
    - Overenie adresy KZ
    - ping
- Manažment prepínača
  - Vytvorenie a konfigurácia manažment VLAN
  - Parkovacia VLAN (inactive)
    - Priradenie nevyužitých portov

Vytvorenie VLAN – Globálny mód or VLAN konfiguračný mód

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name Uctaren
Switch(config-vlan)#vlan 3
Switch(config-vlan)#name Marketing
Switch(config-vlan)#end
Switch#
```

alebo

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name Uctaren
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name Marketing
Switch(config-vlan)#end
Switch#
```

Preferovaná cesta, zmeny hneď, konfigurácia normal aj extended range VLAN

Vytvorenie VLAN – VLAN database mód

```
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#vlan 2
VLAN 2 added:
    Name: VLAN0002
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#
```

- Zmeny sú aplikované až po príkaze **exit** alebo **apply**
- Len pre normal range VLANs
- V novších IOS nebude podporovaný

Zobrazenie aktuálnej VLAN konfigurácie

```
Switch#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------
1    default                             active    Fa0/1, Fa0/2 ,Fa0/3,
                                                   Fa0/4, Fa0/5, Fa0/6,
                                                   Fa0/7, Fa0/8, Fa0/9,
                                                   Fa0/10, Fa0/11, Fa0/12,
                                                   Fa0/13, Fa0/14, Fa0/15,
                                                   Fa0/16, Fa0/17, Fa0/18,
                                                   Fa0/19, Fa0/20, Fa0/21,
                                                   Fa0/22, Fa0/23, Fa0/24
                                                         Gi0/1, Gi0/2
2   Uctaren                              active
3   Marketing                            active
1002 fddi-default                          act/unsup
1003 token-ring-default                    act/unsup
1004 fddinet-default                       act/unsup
1005 trnet-default                         act/unsup
... Output omitted ...
```

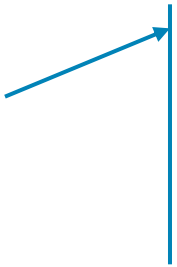
- Cisco prepínače defaultne majú len VLAN1 (typ Ethernet, MTU 1500B)
  Tzv. Manažment VLAN do ktorej sú asociované všetky fyzické porty

Priradenie portu prepínača do VLAN – access port (prístupový port)

- Koncový systém (KS) je pripojený na prepínaný port
- Priradenie KS je vytvorené asociovaním portu do jednej VLAN = **Access port**
- **Access port**
  - Asociovaný len s jednou VLAN.
  - Asociovaná VLAN musí existovať vo VLAN databáze.
  - KS zdieľa IP adresu (prefix) s inými KS v danej VLAN.
- **Asociovanie**
  - Statické asociovanie
    - Konfiguráciou
  - Dynamické asociovanie
    - Na základe MAC adresy KS pripojenej o na port
    - Musí existovať VLAN Membership Policy Server (VMPS) na určenie do ktorej VLAN treba KS zaradiť.

Priradenie portu prepínača do VLAN

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#end
Switch#show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
 1 default                             active    Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7,
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15,
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19,
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23,
                                                 Fa0/24, Gi0/1, Gi0/2
2 Uctaren                              active    Fa0/1
3 Marketing                            active    Fa0/2
```



Vytvorenie access portu a asociovanie portu s VLAN

Priradenie rozsahu portov prepínača do VLAN – overenie konfigurácie

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa 0/1 - 5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#end
Switch#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
1    default                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9,
                                                 Fa0/10, Fa0/11, Fa0/12,
                                                 Fa0/13, Fa0/14, Fa0/15,
                                                 Fa0/16, Fa0/17, Fa0/18,
                                                 Fa0/19, Fa0/20, Fa0/21,
                                                 Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
2 Uctaren                              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                                 Fa0/5
...
```

Iný postup vytvorenia VLAN a priradenia portu do VLAN

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
Switch(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
Switch#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
 1 default                             active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9,
                                                 Fa0/10, Fa0/11, Fa0/12,
                                                 Fa0/13, Fa0/14, Fa0/15,
                                                 Fa0/16, Fa0/17, Fa0/18,
                                                 Fa0/19, Fa0/20, Fa0/21,
                                                 Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
2 VLAN0002                             active    Fa0/1
```

VLAN bude mať default parametre

Overenie VLAN konfigurácie a priradenia portov

```
Switch#show vlan

Switch#show vlan brief

Switch#show vlan id ID_VLANY

Switch#show vlan name MENO_VLANY

Switch#show vlan summary

Switch#sh int INT SPEC switchport

Switch#sh run vlan
```

Overenie VLAN konfigurácie a priradenia portov

```
Switch#sh int fa 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 2 (VLAN0002)
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
Appliance trust: none
```

Zmazanie VLAN konfigurácie

```
! Erase vlan.dat - spominane
Switch#delete flash:vlan.dat

! Removes VLAN 5 from the VLAN database
Switch(config)#no vlan 5

! Vlan database mode
Switch#vlan database
Switch(vlan)#no vlan 5
Switch(vlan)#exit

! Removes port from VLAN 5 and reassigns it
! to the default VLAN (vlan1 ??)
Switch(config)#interface fastethernet 0/5
Switch(config-if)#no switchport access vlan 5
```

Defaultné nastavenie rozhrania

- Vrátenie default nastavenia na rozhranie

```
Switch(config)#default interface interface-id

Napr.

Switch(config)#default interface fa 0/1
```

- Vrátenie default nastavenia na viac rozhraniach naraz

```
Switch(config)# default interface range fa 0/1 - 24
```

Nepoužité porty do inactive VLAN

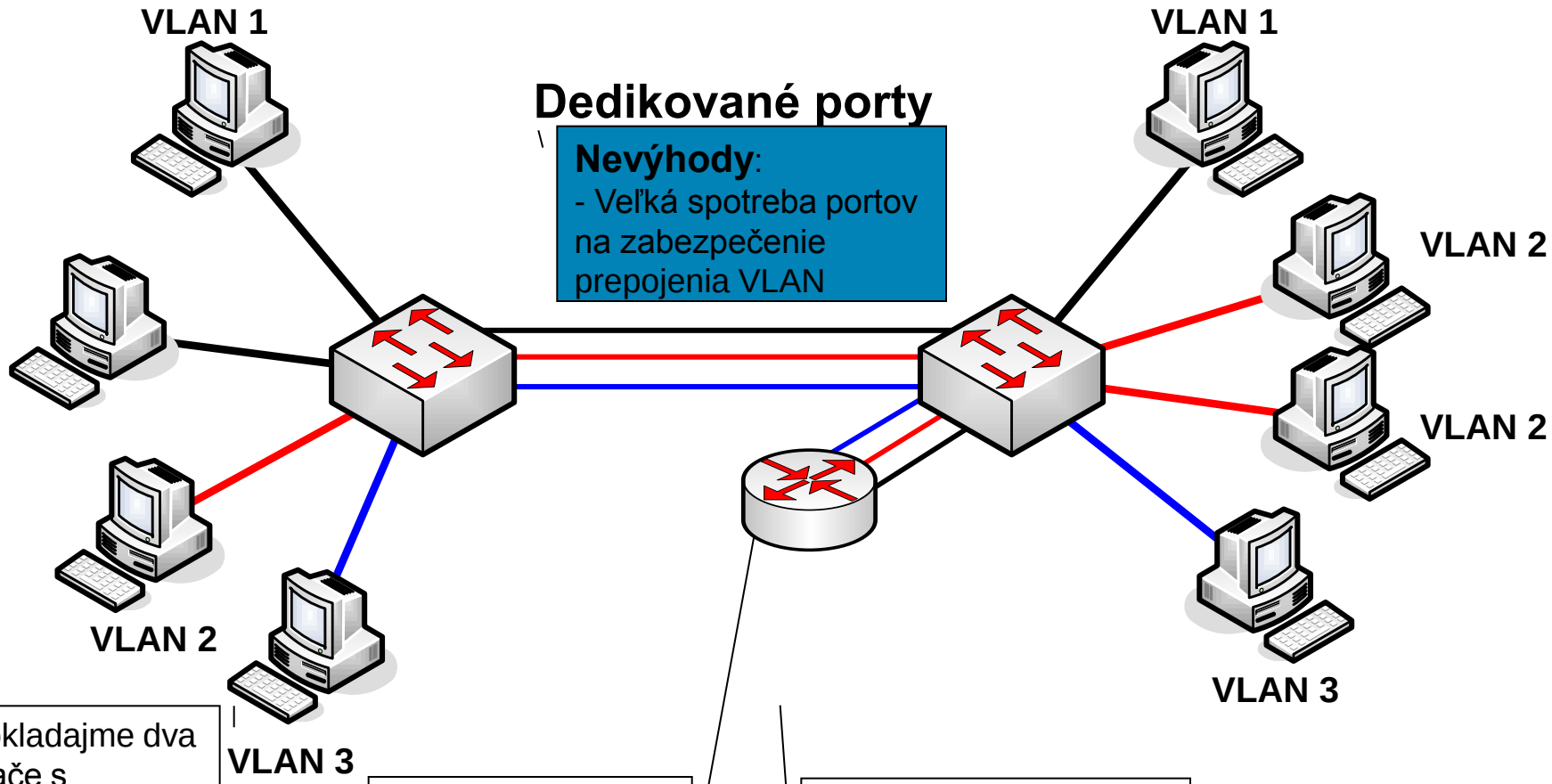
```
Switch(config)# vlan 99
Switch(config-vlan)# state suspend   ! Globalne cez VTP
Switch(config-vlan)# shutdown ! Lokálne
```

```
ALS1#ping 10.1.1.200

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
ALS1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.

ALS1(config)#int fa 0/1
ALS1(config-if)#switchport acc vlan 99
ALS1(config-if)#^Z
ALS1#ping 10.1.1.200

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.200, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
ALS1#
```

- State suspend je propagovaný cez VTP a platí v celej VTP doméne
- VLAN môže byť lokálne deaktivovaná príkazom shutdown

Prepájanie VLAN - Trunking mechanizmy a protokoly

Intra VLAN komunikácia - Dedikované porty

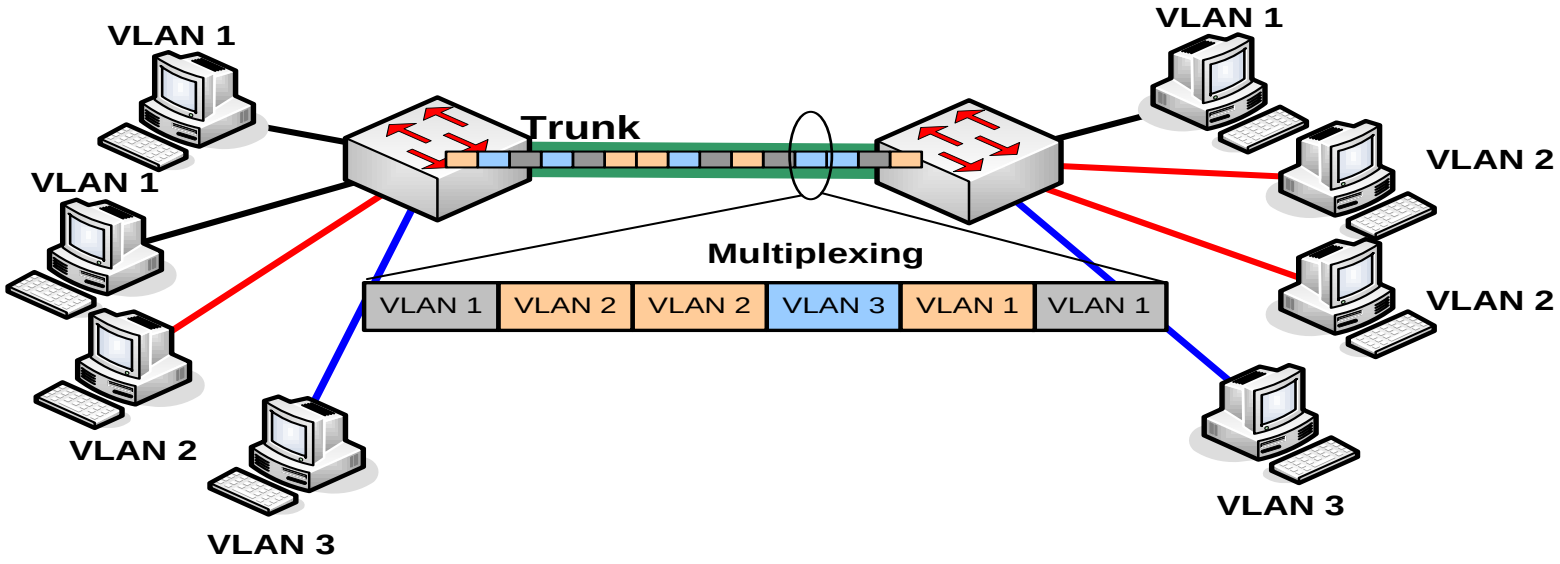


Predpokladajme dva prepínače s nakonfigurovanými 3 VLAN-ami. Ako zabezpečiť ich prepojenie?

Na komunikáciu medzi prepínačmi a VLAN určíme separátne fyzické porty pre každú VLAN.

Na inter VLAN komunikáciu potrebujeme smerovač. Na smerovači pre každú VLAN vyhradené rozhranie (port).

Intra VLAN komunikácia - Trunking



Trunk

- Fyzická alebo logická linka medzi prepínačmi
- Rámce sa **multiplexujú** cez Trunk

- **Ako rozlíšiť v multiplexovanom toku do ktorej VLAN patria ktoré rámce?**

- Rozlíšenie značkovaním rámcov podľa VLAN
- **Tzv. TAGGING**

Trunking

- **Trunking**
  - Poskytuje efektívnu cestu pre komunikáciu medzi prepínačmi
  - Spôsob ako poskytovať cestu dátam viacerých VLAN cez „internetwork“
  - **VLAN Backbone**
- **Trunk**
  - Fyzická alebo logická (etherchannel) linka
    - „Prenosový kanál medzi dvoma bodmi“
  - Tvorí „backbone“ pre rôzne Virtuálne LAN (VLAN) v prepínanej LAN sieti
  - Prepája prepínače navzájom
    - Pre potreby **Intra VLAN** komunikácie
  - Prepája prepínač (-e) so smerovačom (-čmi)
    - Pre **Inter VLAN** komunikácie
  - Rámce rôznych VLAN sú na trunk-u multiplexované

Trunk protokoly ISL a 802.1Q

- Trunk protokoly
  - Určujú akým spôsobom budú rámce (de)multiplexované cez spoločný prepoj medzi switchmi
- Trunk port
  - Patrí do viacerých VLAN, preto potrebuje rámce označovať kvôli identifikácii, do ktorej VLAN patria
- Cisco zariadenia obvykle podporujú dva trunk protokoly
  - ISL (Inter-Switch Link Protocol)
    - Proprietárny Cisco protokol, problémy s kompatibilitou
    - Jedná sa o enkapsulujúci protokol – celý pôvodný rámec vrátane pôvodnej FCS sa vloží do tela ISL rámca
    - K rámcu je pridaná nová hlavička s VLAN ID informáciou (26B dlhá + 4B CRC)
    - Cisco Document ID: 17056, „Inter-Switch Link and IEEE 802.1Q Frame Format“ – veľmi odporúčané čítanie
  - IEEE 802.1Q

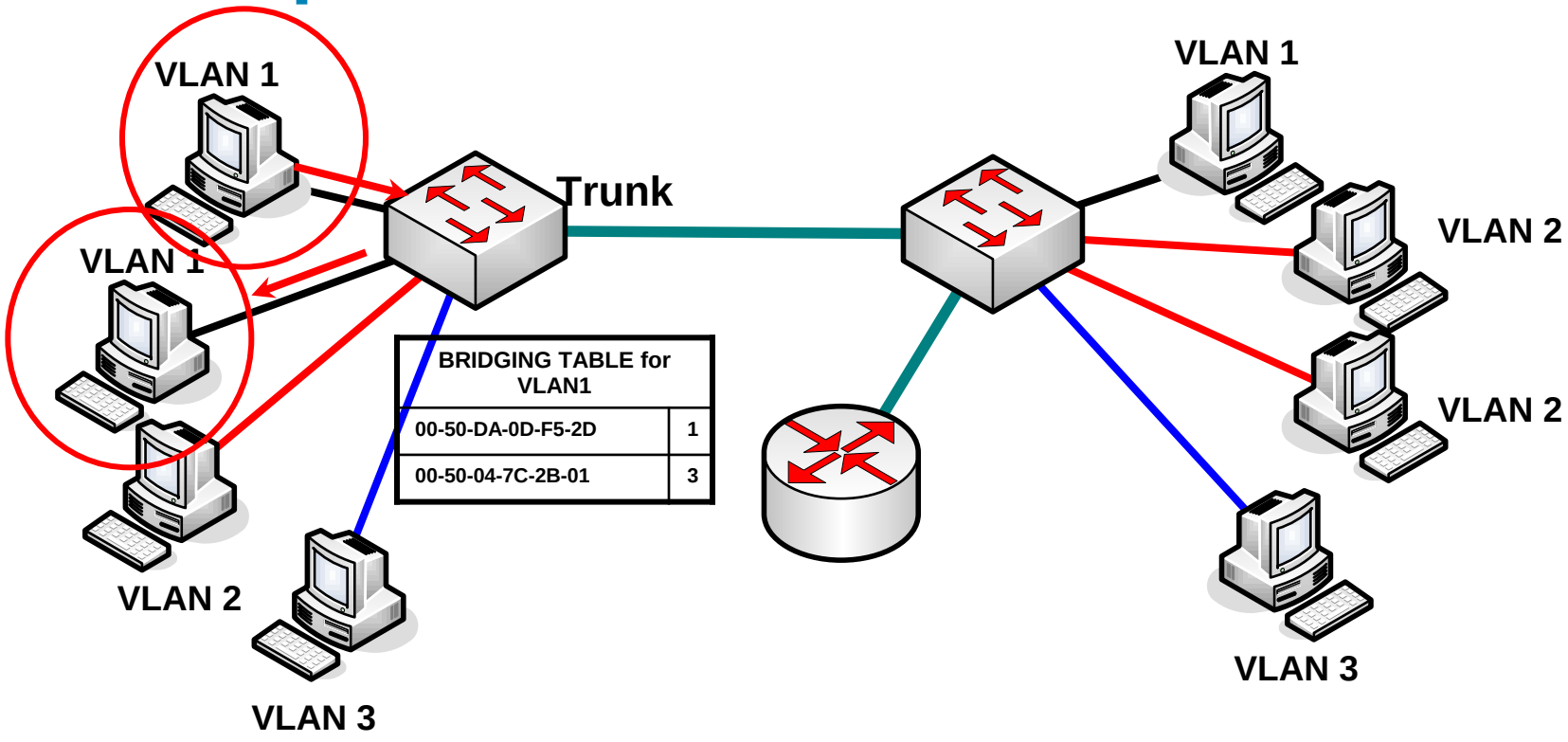
IEEE 802.1Q

- 802.1Q je otvorený IEEE štandard pre trunk prepoje
  - Zabezpečená interoperabilita zariadení rôznych výrobcov
  - Poskytuje menší overhead ako ISL
  - Podporuje QoS cez 802.1p
- Podstatou štandardu je pridanie novej 4B značky (tagu) do rámca prenášaného na trunku
    - Značka identifikuje VLAN, do ktorej rámec patrí
    - Značka je vložená do vnútra rámca, nejde o enkapsuláciu
- Značka sa pridáva
  - Medzi pole Source MAC a pole Type/Length
  - Do (skoro) všetkých rámcov na trunku
  - Pridanie značky znamená zmenu obsahu rámca, čo znamená prepočítanie FCS

Prenos rámcov pri IEEE 802.1Q

- Odosielajúci prepínač
  - Vloží 4B tag do rámca
  - Prepočíta FCS
  - Pošle rámec cez trunk
- Prijímajúci trunk prepínač (druhá strana)
  - Skontroluje FCS
  - Analyzuje hodnotu tagu a odstráni ho z rámca
  - Prenáša rámec vo VLAN danej hodnotou tagu
- Koncové stanice o tomto značkovaní nevedia
  - Na prístupové (access) porty sa rámec dostane v pôvodnom tvare bez značiek, pre stanice je celý proces transparentný

802.1q – Intra VLAN komunikácia

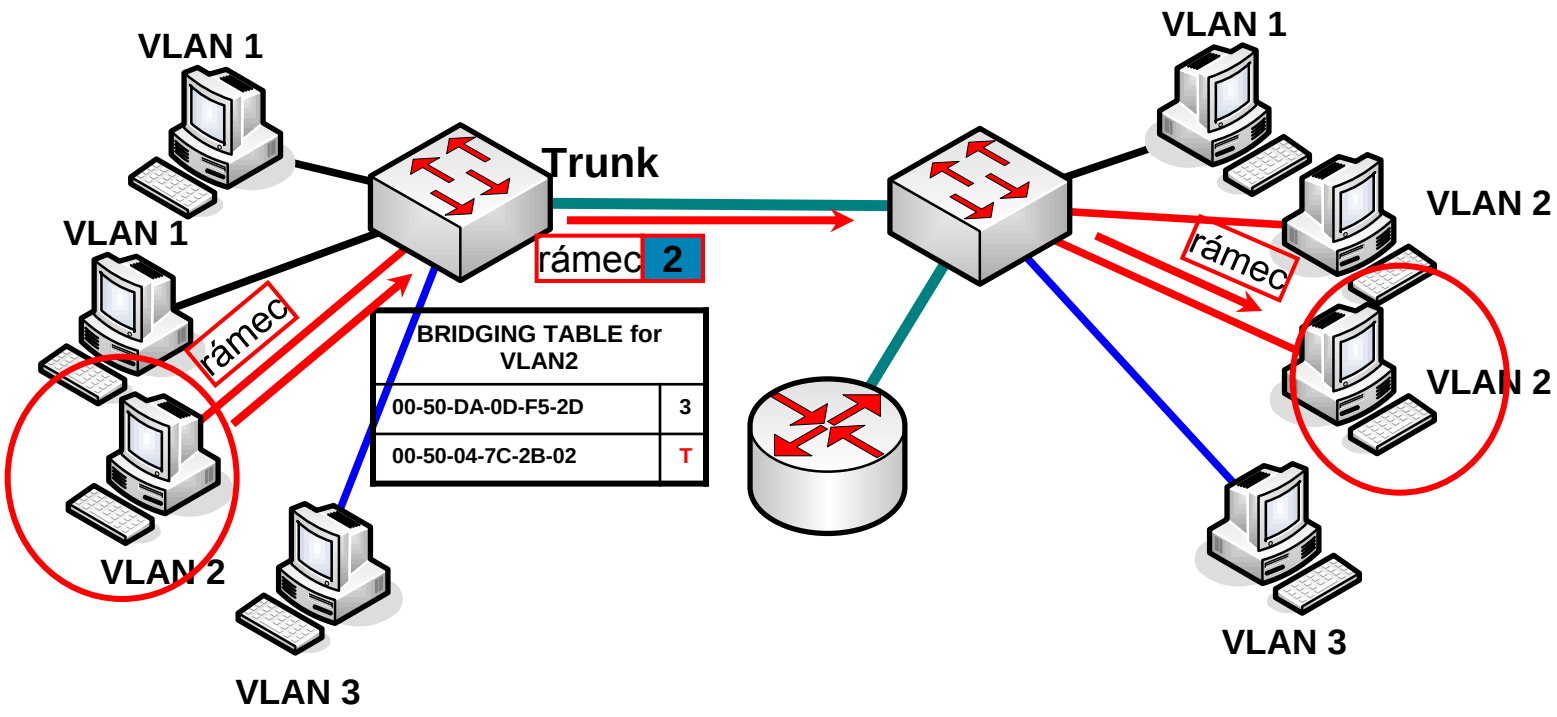


Príklad:
Komunikácia medzi stanicami vo vnútri VLAN (Intra VLAN) na to istom prepínači

-Prepínač príjme rámec na vstupnom porte (**VLAN Access port**).
-prezrie Bridging table for VLAN 1
-prepne rámec na výstupný port

Rámec nie je pozmenený (značkovaný) nakoľko nevstupuje na trunk port!
- Rámec je prepnutý ako na bežnom prepínači.

802.1q – Intra VLAN komunikácia



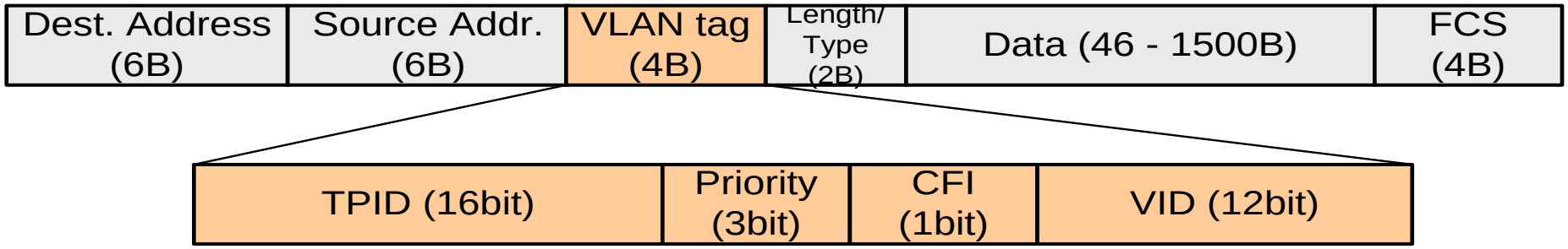
Príklad:
Komunikácia medzi stanicami vo vnútri VLAN (Intra VLAN) na **rôznych** prepínačoch.

-Prepínač príjme rámec na vstupnom porte (**VLAN Access port**).
-prezrie Bridging table for VLAN 2
-rámec musí byť prepnutý cez trunk
-vloží Tag, identifikujúci, že rámec je pre VLAN 2 (2)
- Prepne rámec na trunk port

-Prijímajúci prepínač príjme rámec
-prezrie Bridging table
-ak cieľová stanica je na jeho porte
-odstráni Tag
-prepne rámec

Rámec je **pozmenený (značkovaný) nakoľko vstupuje** na trunk port**!**

802.1q formát rámca



- **TPID (Tag Protocol Identifier)**: 16 bitov
  - Identifikuje rámec ako IEEE802.1q rámec
  - Nastavená hodnota 0x8100 pre tagovaný ethernet
- **Priority:** 3bity
  - Indikuje prioritu rámca podľa prioritizačnej schémy 802.1p
    - Použité na prioritizáciu rámcov
- **CFI (Canonical Format Indicator):** 1bit
  - CFI=0: MAC adresa je v kanonickom formáte (ethernet)
  - CFI=1: MAC adresa nie je v kanonickom formáte (FDDI)
- **VID (VLAN Identifier):** 12 bit
  - Jednoznačne a jedinečne identifikuje VLAN do ktorej patrí rámec
  - 4096 VLAN možných (0-4095)

Natívna VLAN

- Pri 802.1Q je Ciscom definovaná tzv. natívna VLAN
  - Táto VLAN nepoužíva na trunku značky (ako jediná)
  - Každý trunk port má svoju vlastnú natívnu VLAN (t.j. dva rôzne trunk porty môžu byť v rôznych natívnych VLAN)
  - Ak rámec patrí do natívnej VLAN, potom pri odoslaní trunk portom značku nedostane
  - Ak rámec prijatý na trunku nemá značku, switch ho zaradí do natívnej VLAN
- Pri 802.1Q musia byť oba konce trunku v tej istej natívnej VLAN
  - Štandardne je to VLAN 1
  - Evidentne, ak budú konce trunku patriť do rôznych natívnych VLAN, potom sa tieto VLAN „zlejú“ do jednej

Natívna VLAN (2)

- Koncept natívnej VLAN komplikuje život
  - Odporúča sa vytvoriť samostatnú a úplne nepoužívanú VLAN, ktorá bude použitá ako natívna VLAN na všetkých trunkoch
  - Ruky preč od VLAN1 a od natívnej VLAN
- Určite sa treba vyhnúť
  - Použitiu VLAN, ktorá je na nejakom trunku natívna, ako bežnej VLAN pre koncové stanice
  - Použitiu management VLAN ako natívnej VLAN (CCNA3 to mylne odporúča!)
- Na vyšších switchoch (3560 a vyššie) je možné používanie natívnej VLAN deaktivovať príkazom globálneho konfiguračného režimu

```
vlan dot1q tag native
```

Konfigurácia trunkov

Trunk konfigurácia

- Manuálne (Staticky)

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

- Dynamicky
  - Dynamic Trunking Protocol (DTP)
    - Dynamicky dohodnuté vytvorenie trunku
    - Podpora ISL aj dot1q

```
Switch(config-if)#switchport mode {dynamic {desirable | auto}}
```

Statická konfigurácia trunk portu

```
! Nastavenie enkapsulácie na 3550, 3560 (nie na 2950, 2960)
Switch(config-if)# switchport trunk encap { isl | dot1q }

! Konfigurácia trunku
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan VLAN_ID
Switch(config-if)# switchport trunk allowed vlan ?
  WORD    VLAN IDs of allowed VLANs when this port is in trunking mode
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  none    no VLANs
  remove  remove VLANs from the current list
```

Overenie konfigurácie trunku

```
Switch#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig1/1      on           802.1q         trunking      99
Gig1/2      auto         802.1q         trunking      99


Port        Vlans allowed on trunk
Gig1/1      1-1005
Gig1/2      1-1005

Port        Vlans allowed and active in management domain
Gig1/1      1,99,1002,1003,1004,1005
Gig1/2      1,99,1002,1003,1004,1005

Port        Vlans in spanning tree forwarding state and not pruned
Gig1/1      1,99,1002,1003,1004,1005
Gig1/2      1,99,1002,1003,1004,1005

Switch#
```

Overenie konfigurácie trunku

```
Switch#sh int gi 1/1 trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig1/1      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Gig1/1      1-1005

Port        Vlans allowed and active in management domain
Gig1/1      1,99,1002,1003,1004,1005

Port        Vlans in spanning tree forwarding state and not pruned
Gig1/1      1,99,1002,1003,1004,1005

Switch#
```

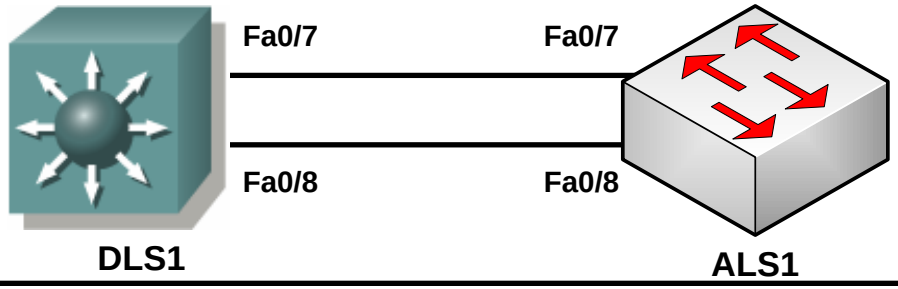
Overenie konfigurácie trunku

```
Switch#sh int gi 1/1 switchport
Name: Gig1/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Manazment_siete)
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
Appliance trust: none
```

Príkaz *switchport mode trunk* umiestni port do trvalého trunking módu

DTP je stále spustené, ak druhá strana je konfigurovaná ako trunk, dynamic desirable, or dynamic auto **TRUNK sa vytvorí**

Jedna strana static trunk a druhá static access




```
DLS1(config)#int ran fa 0/7 - 8
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
DLS1#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/7       on               802.1q         trunking      1
Fa0/8       on               802.1q         trunking      1
```

```
ALS1#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/7       on               802.1q         trunking      1
Fa0/8       on               802.1q         trunking      1

ALS1(config)#int fa 0/8
ALS1(config-if)#switchport mode access
ALS1(config-if)#^Z
ALS1#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/7       auto             802.1q         trunking      1
```

```
DLS1#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/7       on               802.1q         trunking      1
Fa0/8       on               802.1q         trunking      1
```

Dynamic Trunking Protocol (DTP)

Automatické dohodovanie vytvorenia trunku

DTP - Dynamic Trunking Protocol

- Cisco proprietárny protokol
- Umožňuje automatické dohodovanie vytvárania trunkov zasielaním DTP rámcov medzi prepínačmi
- Nie všetky Cisco zariadenia podporujú DTP
  - Obvykle je podporovaný iba na prepínačoch
  - Smerovače nerozumejú DTP a negenerujú jeho správy
  - DTP nijako neovplyvňuje možnosť statického zostavenia trunku či jeho činnosť (nemá nič spoločné s tým, ako sa prenášané rámce značkujú alebo enkapsulujú)

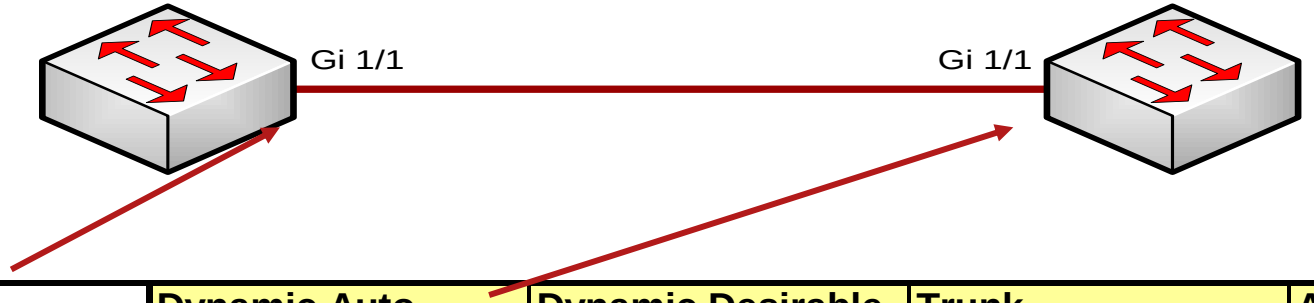
Operačné módy DTP

- **Dynamic Auto**
  - Default mód na Cat2960, 3560
  - Port oznamuje druhej strane, že je schopný byť trunkom, ale nevyžaduje prechod do trunk módu
  - `Switch(config-if)#switchport mode dynamic auto`
- **Dynamic Desirable**
  - Default mód na Cat2950, 3550
  - Port oznamuje druhej strane, že je schopný byť trunkom, a vyžaduje od druhej strany aby sa stala trunkom

  `Switch(config-if)#switchport mode dynamic desirable`
- **Nonegotiate**
  - Vypnutie DTP na porte prepínača, nebudú posielané žiadne DTP rámce

  `Switch(config-if)#switchport nonegotiate`
- **Statický trunk („On“)**
  - Vytvorí trunk bez ohľadu na DTP žiadosti suseda alebo stav portu suseda
- **Statický access („Off“)**
  - Trunk nie je povolený na tomto porte

Operačné módy DTP – činnosť



	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access

- DTP má slúžiť na úvodný rozbeh siete, po ustálení sa odporúča:
  - Porty staticky nastaviť ako trunk/access
  - DTP deaktivovať pomocou switchport nonegotiate
    - Zapnutá dynamická negociácia trunku na portoch, kde nemá byť môže viesť k útokom na sieť.

DTP konfigurácia

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet 5/8
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode dynamic desirable | auto
Switch(config-if)# no shutdown
Switch(config-if)# end
```

Overenie činnosti DTP

```
Switch#sh int gi 1/1 switchport
Name: Gig1/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
...
```

Lokálna strana je dynamic auto

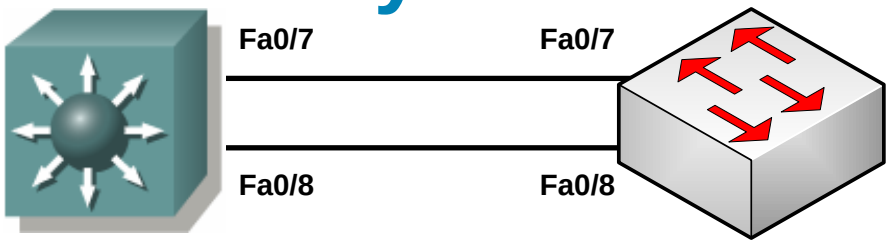
Druhá strana je dynamic desirable alebo trunk

```
Switch#sh dtp
Global DTP information
    Sending DTP Hello packets every 30 seconds
    Dynamic Trunk timeout is 300 seconds
    6 interfaces using DTP
```

Informácie o DTP na porte

```
DLS1#sh dtp interface fa 0/7
DTP information for FastEthernet0/7:
  TOS/TAS/TNS:                              TRUNK/ON/TRUNK
  TOT/TAT/TNT:                              802.1Q/802.1Q/802.1Q
  Neighbor address 1:                       001B53A1A487
  Neighbor address 2:                       000000000000
  Hello timer expiration (sec/state):       20/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
  ----------
  524 packets received (524 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
  839 packets output (839 good)
       524 native, 315 software encap isl, 0 isl hardware native
  0 output errors
  0 trunk timeouts
  1 link ups, last link up on Mon Mar 01 1993, 00:06:49
  0 link downs
```

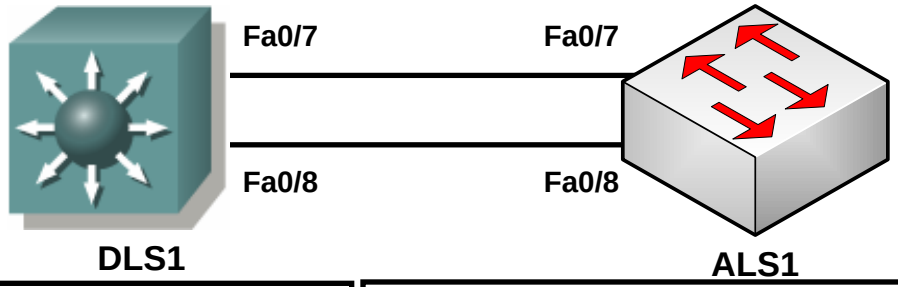
DTP – static trunk vs dynamic auto




```
DLS1(config)#int ran fa 0/7 - 8
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
DLS1#sh int trunk

Port        Mode             Encapsulation  Status
Fa0/7       on               802.1q         trunking      1
Fa0/8       on               802.1q         trunking      1

DLS1#sh int fa 0/7 switchport
Name: Fa0/7
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
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 Native VLAN tagging:
     enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

```
ALS1#sh int trunk

Port        Mode             Encapsulation  Status        Native
Fa0/7       auto             802.1q         trunking      1
Fa0/8       auto             802.1q         trunking      1


ALS1#sh int fa 0/7 switchport
Name: Fa0/7
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
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 Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

DTP – dynamic desirable vs access




```
DLS1(config)#int fa 0/7
DLS1(config-if-range)#switchport mode dynamic desirable
DLS1#sh int fa 0/7 trunk

Port        Mode             Encapsulation  Status
     Native vlan
Fa0/7       desirable        802.1q         not-trunking  1


DLS1#sh int fa 0/7 switchport
Name: Fa0/7
Switchport: Enabled
Administrative Mode: dynamic desirable
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)
Administrative Native VLAN tagging: enabled
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 Native VLAN tagging:
     enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

```
ALS1(config)#int fa 0/7
ALS1(config-if-range)#switchport mode access

ALS1#sh int fa 0/7 trunk

Port        Mode             Encapsulation  Status        Native
     vlan
Fa0/7       off              802.1q         not-trunking  1

ALS1#sh int fa 0/7 switchport
Name: Fa0/7
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
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 Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

Debug dtp

```
dls2#debug dtp ?
  aggregation  Show DTP debug user message aggregation
  all          All DTP debugging messages
  decision     Show DTP debug decision table
  events       DTP events
  oserrs       DTP OS errors
  packets      DTP packet processing
  queue        Show DTP debug packet queueing
  states       DTP state transitions
  timers       DTP timer events
```

```
*Mar  1 01:21:41.505: DTP-event:Fa0/11:Received packet event
../dyntrk/dyntrk_process.c:2200
*Mar  1 01:21:41.513: DTP-event:Fa0/12:Received packet event
../dyntrk/dyntrk_process.c:2200
*Mar  1 01:21:41.539: DTP-event:Fa0/7:Received packet event
../dyntrk/dyntrk_process.c:2200
*Mar  1 01:21:41.555: DTP-event:Fa0/8:Received packet event
../dyntrk/dyntrk_process.c:2200
*Mar  1 01:21:41.622: DTP-event:Fa0/10:Received packet event
../dyntrk/dyntrk_process.c:2200
*Mar  1 01:21:41.715: DTP-event:Fa0/9:Received packet event
../dyntrk/dyntrk_process.c:2200
```

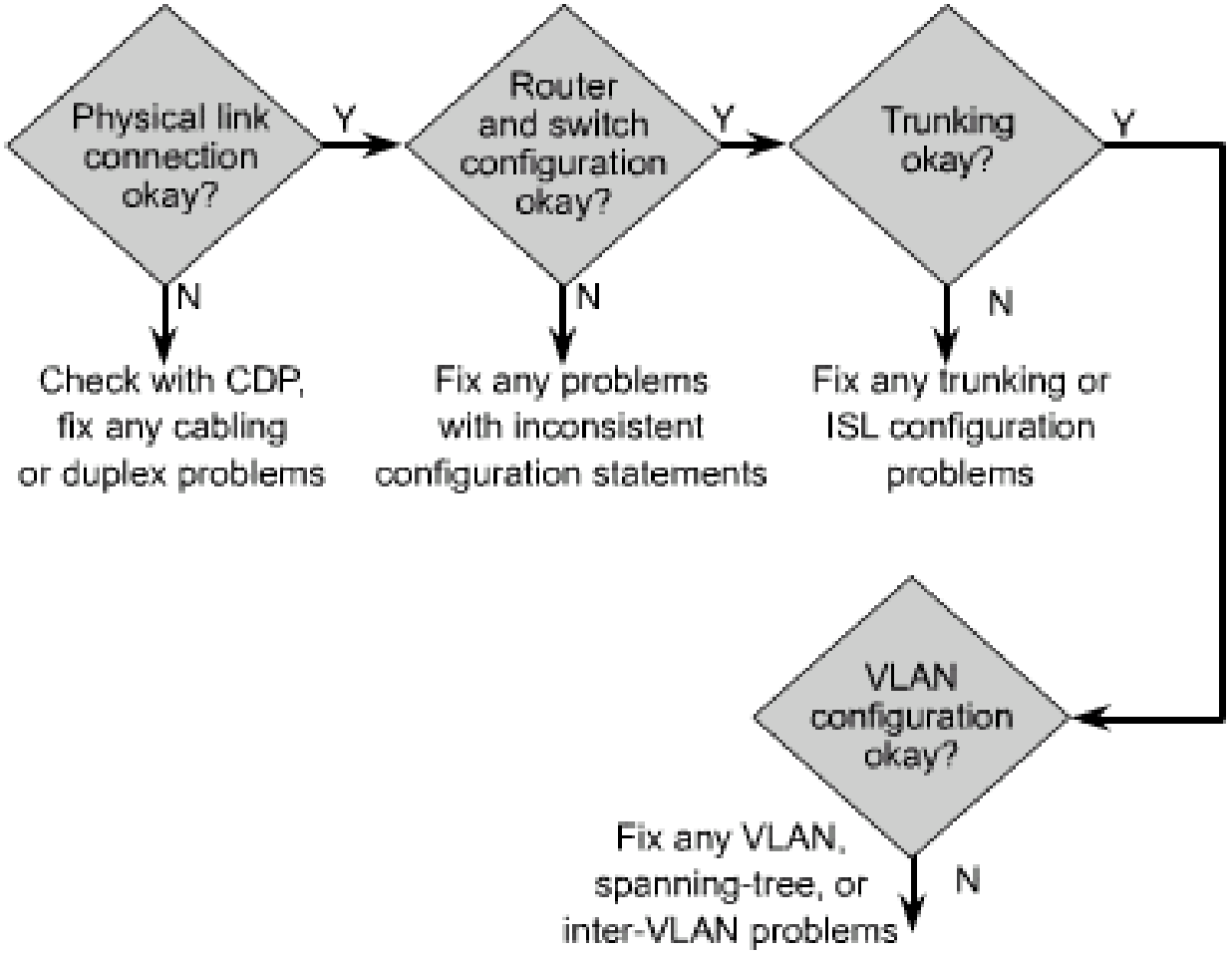
DTP – záverečné poznámky

- DTP má slúžiť na úvodný rozbeh siete a zabránenie problémom s neplatnou konfiguráciou dvojíc portov
  - Po úspešnom rozbehu siete je vhodné DTP deaktivovať
- DTP si vo svojich správach posiela meno VTP domény
  - Pre úspešné dojednanie trunku je potrebné, aby VTP doména na oboch switchoch bola identická
  - Ak sa názov VTP domény nezhoduje, DTP nebude schopné správne dojednať režim činnosti prepoja

Diagnostika problémov

Hľadanie problému vo VLAN

- Fyzické zapojenie
- Over a koriguj konfiguráciu prepínača
- Over konfiguráciu a stav trunk prepojov
- Over konfiguráciu VLAN



Chyby vyplývajúce zo zle konfigurovanej natívnej VLAN

- Native VLAN
  - Native VLAN musí byť zhodná na oboch koncoch trunku
  - Štandardne je VLAN1 použitá ako native VLAN.
  - Z hľadiska bezpečnosti je vhodné vybrať za native VLAN samostatnú úplne nepoužívanú VLAN
- Možné problémy pri nezhode natívnych VLAN:
  - Môže dôjsť k vytváraniu Layer 2 slučiek
  - Dôjde k pretekaniu dát z jednej VLAN do druhej
- Cisco switche pomocou CDP a STP detegujú nezhodu native VLAN a port dočasne zablokujú, pokým problém nebude odstránený

Typické chyby pri VLAN a trunkoch

- Nesedia natívne VLAN na oboch koncoch trunku

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
   GigabitEthernet1/1 (99), with Switch GigabitEthernet1/1 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
   GigabitEthernet1/1 (99), with Switch GigabitEthernet1/1 (1).
```

- Zlyhanie vytvorenia trunku
  - Nesedia automat. trunk módy alebo statické trunk resp. access nastavenia na rôznych koncoch trunku
    - Na jednej strane switchport access a na druhej switchport trunk
    - Na jednej strane switchport access na druhej DTP auto or desirable
  - Prepínače nie sú v tej istej VTP doméne
  - Rozdielna enkapsulácia na koncoch trunku
- Nesprávne nastavenie L3 adresácie nad VLAN
  - Strata IP konektivity or neštandardné správanie
- Nesprávne nastavený zoznam povolených VLAN nad trunkom
  - Chýba povolenie VLAN, ktorá si to vyžaduje
  - Strata konektivity or neštandardné správanie

“Best practises” pre VLAN dizajn

- Použi Local VLAN model
  - Per Access switch block použi max od 1 do 3 VLAN
  - VLAN definuj len na skupine access prepínačov a distro prepínačov
- Nepriraďuj nepoužité porty do VLAN 1 (použi „blackhole“ VLAN)
  - „blackhole“ VLAN nemá routing položku, je izolovaná
    - Používaná ako „penalty“ box
- Ak sa dá separuj Voice, data, multicast, manažment, native, default a blackhole VLAN
- Pri local VLAN sa vyhni používaniu VTP
- Pre trunk porty vypni DTP, a použi dot1.q, nie ISL
- Manuálne konfiguruj Access porty
- Zabráň prevádzke z VLAN 1 okrem manažmentu
  - CDP, DTP, VTP, STP, SSH, PaGP, LACP, apod.
- Nepoužívaj Telnet

[cisco foundation lerarning guide]

Virtual Trunking Protocol (VTP)

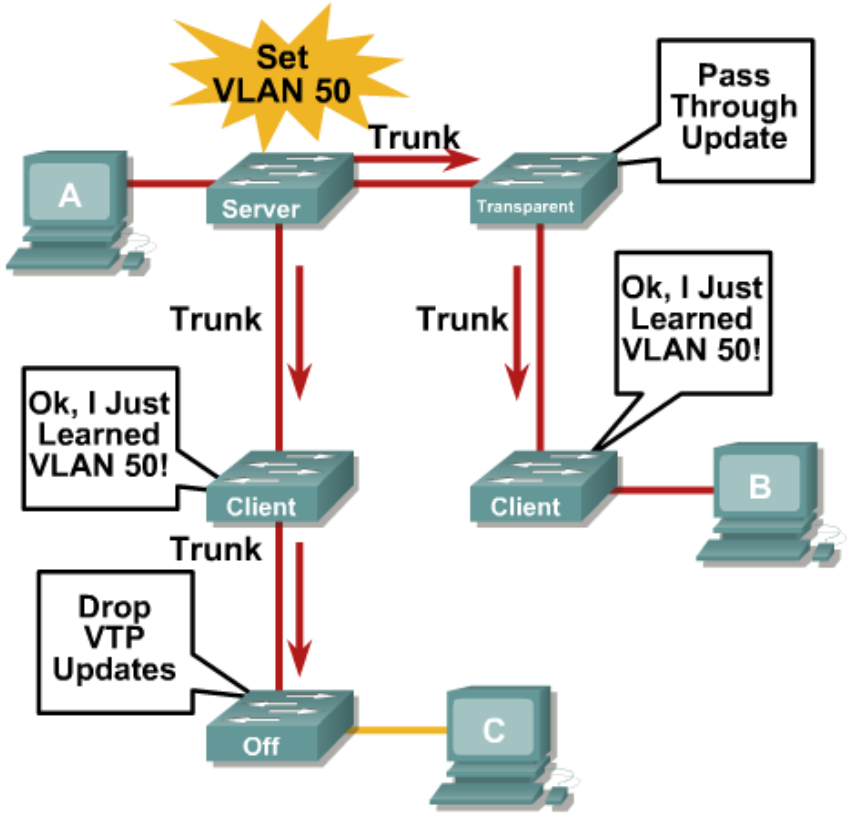
Virtual Trunking Protocol (VTP)

- Je Cisco proprietárny protokol
  - Vyvinutý za účelom distribúcie a synchronizácie VLAN databáz cez sieť
  - Minimalizuje konfiguračné chyby alebo inkonzistenciu v definícii VLAN
    - typy VLAN, duplicita mien
- VTP správy sa prenášajú výlučne cez trunk porty
  - Používa dot1q or ISL rámce
  - Prenášané cez manažment VLAN (def. VLAN 1)
- Tri verzie
  - VTPv1 a VTPv2 boli donedávna dominantné
  - VTPv3 bolo pôvodne podporované len na high-end switchoch, od verzie IOSu 12.2(52)SE je k dispozícii na všetkých Catalyst switchoch
  - VTPv1 a VTPv2 prenášajú iba info o VLAN 1-1005
  - VTPv3 prenášajú info o všetkých VLAN
- Catalyst podporuje verzie VTP 1, 2, 3
  - V2 je najbežnejšia, ale default je v režime v1
    - Navzájom nekompatibilné

Rozdiely medzi VTP verziami

- VTPv2 pridáva oproti VTPv1 tieto funkcie:
  - Podpora pre Token Ring VLANs
  - Podpora neznámych TLV vo VTP správach (VTPv2 tieto TLV uloží a prepošle, aj keď im nerozumie; VTPv1 ich zahodí)
  - VTPv2 Transparent switch preposiela VTP správy bez kontroly názvu domény alebo verzie (1 alebo 2)
  - Kontrola konzistencie VLAN databázy sa realizuje iba pri konfiguračnom zásahu, nerobí sa pri prijatí VTP správ
- VTPv3 pridáva oproti VTPv2 tieto funkcie:
  - Podpora extended-range VLANs (1025-4094), Private VLANs
  - Zlepšená autentifikácia
  - Ochrana proti neželanému prepísaniu domény
    - Akceptujú sa správy len od primárneho servera s vyšším rev. #
    - Backup server zálohuje active server, nemôže však nič meniť
  - Možnosť deaktivovať VTP na vybranom porte
  - VTPv3 je zovšeobecnený protokol na distribúciu obsahu ľubovoľnej databázy
    - Ako jedna z aplikácií je okrem VLAN synchronizácia MSTP konfigurácie

Výhody použitia VTP

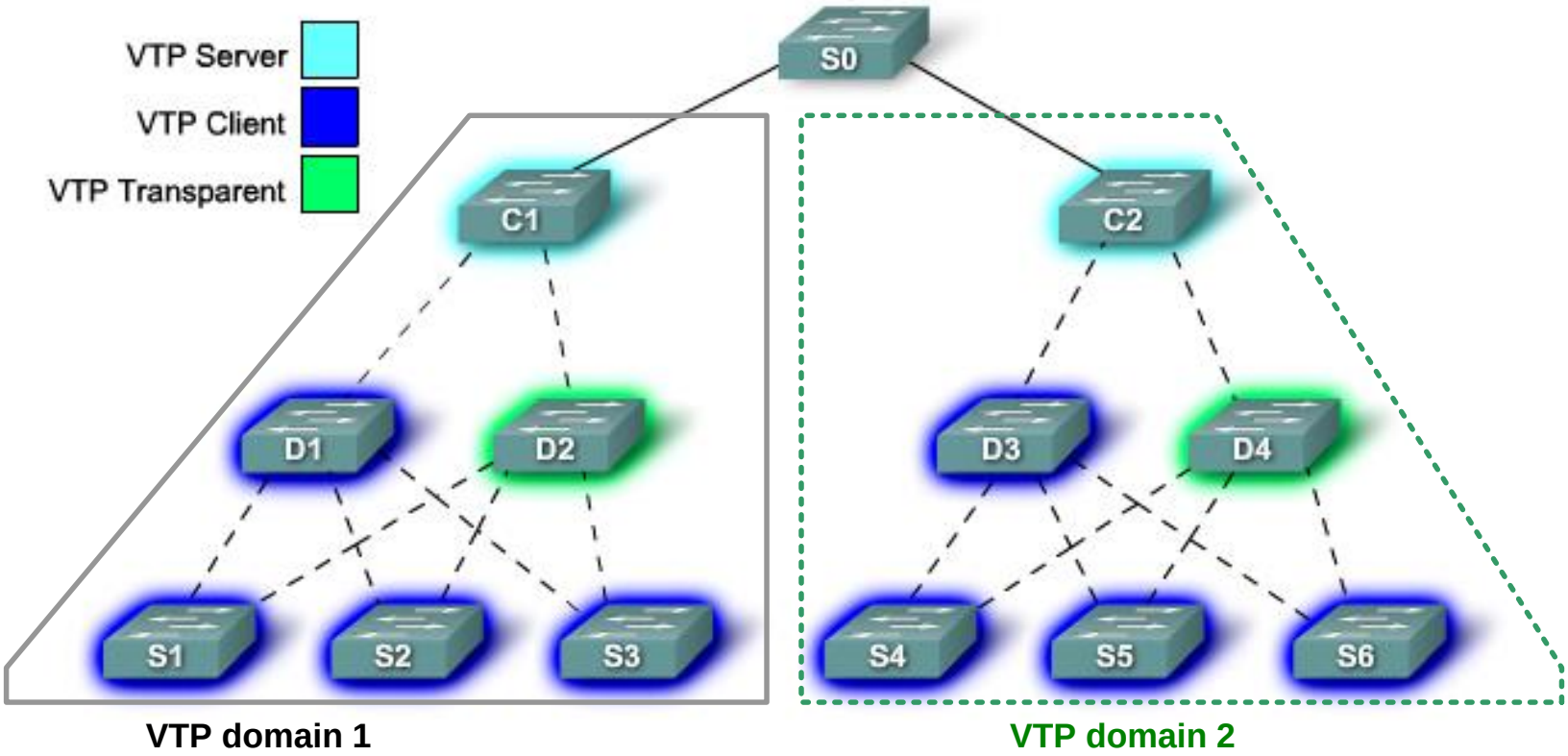


- Zjednodušený a konzistentný manažment VLAN naprieč prepínanou sieťou
- Uľahčené monitorovanie stavu VLAN
- Dynamické reportovanie aktuálnych zmien v konfigurácií VLAN sietí

VTP módy

- Server
  - Môže modifikovať VLAN databázu s platnosťou pre celú VTP doménu
  - Spracováva a preposiela prijaté VTP správy pre danú doménu
  - Informácia o VLAN sa ukladá iba do súboru vlan.dat
- Client
  - Adaptuje sa na zmeny VLAN databázy, no sám nemá právo nič modifikovať
  - Spracováva a preposiela prijaté VTP správy pre danú doménu
  - Informácia o VLAN sa ukladá iba do súboru vlan.dat
- Transparent
  - Nie je skutočným členom domény
  - Preposiela VTP správy, ale ignoruje ich obsah (len verzie2 a 3)
  - Má vlastnú nezávislú VLAN databázu
  - Má vždy VTP číslo revízie 0
- Off
  - Ignoruje a nepreposiela VTP správy (len VTPv3 alebo CatOS)

VTP doména



- Združenie jedného a viac prepínačov, ktoré budú zdieľať VLAN info a budú spolu komunikovať
- Identifikovaná spoločným menom
- Prepínač môže byť len v jednej doméne

Propagovanie VTP informácií

- VTP používa štyri typy VTP správ
- ***Summary advertisement***
  - Súhrnné informácie o VLAN databáze generované každých 5 minút alebo hneď po modifikácii VLAN databázy
    - Posiela server *aj klient* (zašle po zapnutí a nabootovaní)
      - Ako info čomu switch verí ohľadne VLAN
      - Môže spôsobiť prepísanie existujúcich dát
  - Prepínač pri jej prijatí kontroluje doménové meno, a rev. Číslo
    - ak nesedí meno or nižšie rev. číslo, správa sa ignoruje
- ***Subset advertisement***
  - Nasleduje za Summary advertisements pri zmenách vo VLAN
  - Obsahuje detailné info o VLAN, ktorým sa zmenil nejaký parameter
- ***Advertisement requests***
  - Vyžiadanie VLAN databázy, ak je prijatý Summary Adv. s vyšším číslom revízie, po reštarte prepínača alebo zmene jeho VTP domény
  - Odpoveďou je summary a jeho subset advertisement
- ***VTP Join správy***
  - Využívané pri VTP Pruningu

VTP summary advertisment

Version (1 byte)	Type (Summary Adv) (1 byte)	Number of subset advertisements to follow (1 byte)	Domain name length (1 byte)
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision Number (4 bytes)			
Updater Identity (orginating IP address: 4 bytes)			
Update Time Stamp (12 bytes)			
MD5 Digest hash code (16 bytes)			

- VTP správa je:
  - Posielaná na Mcast adresu 01-00-0C-CC-CC-CC (All-VTP)
- **Správa obsahuje**
  - **Version** – Verzia VTP, buď VTP 1, VTP 2 or VTP 3. Cat2960 podporuje VTP 1 a VTP 2. 1 a 2 sú navzájom nekompatibilné.
  - **Typ správy (summar. adv.)**
  - **Počet nasledujúcich subset advert. správ**
  - **Domain name length** – Dĺžka doménového mena.
  - **Domain name –** Identifikuje VTP doménu prepínača.
  - **Configuration revision number** – Aktuálne číslo revízie updatu.
  - **Identita updatera**
  - **Časová značka**
  - **MD5 hash**

VTP subset advertisment správa

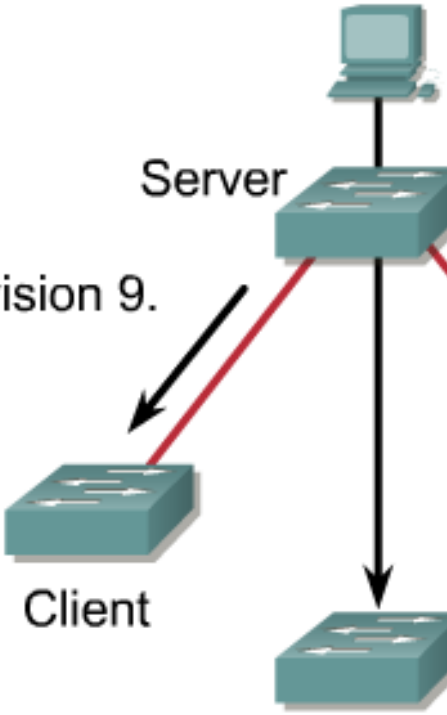
- Obsahuje Info o patričných zmenách vo vlan

0	1	2	3
Version (1 byte)	Type (Subset Adv) (1 byte)	Subset sequence number (1 byte)	Domain name length (1 byte)
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision Number (4 bytes)			
VLAN Info Field 1 (see below)			
VLAN Info Field ...			
VLAN Info Field N			

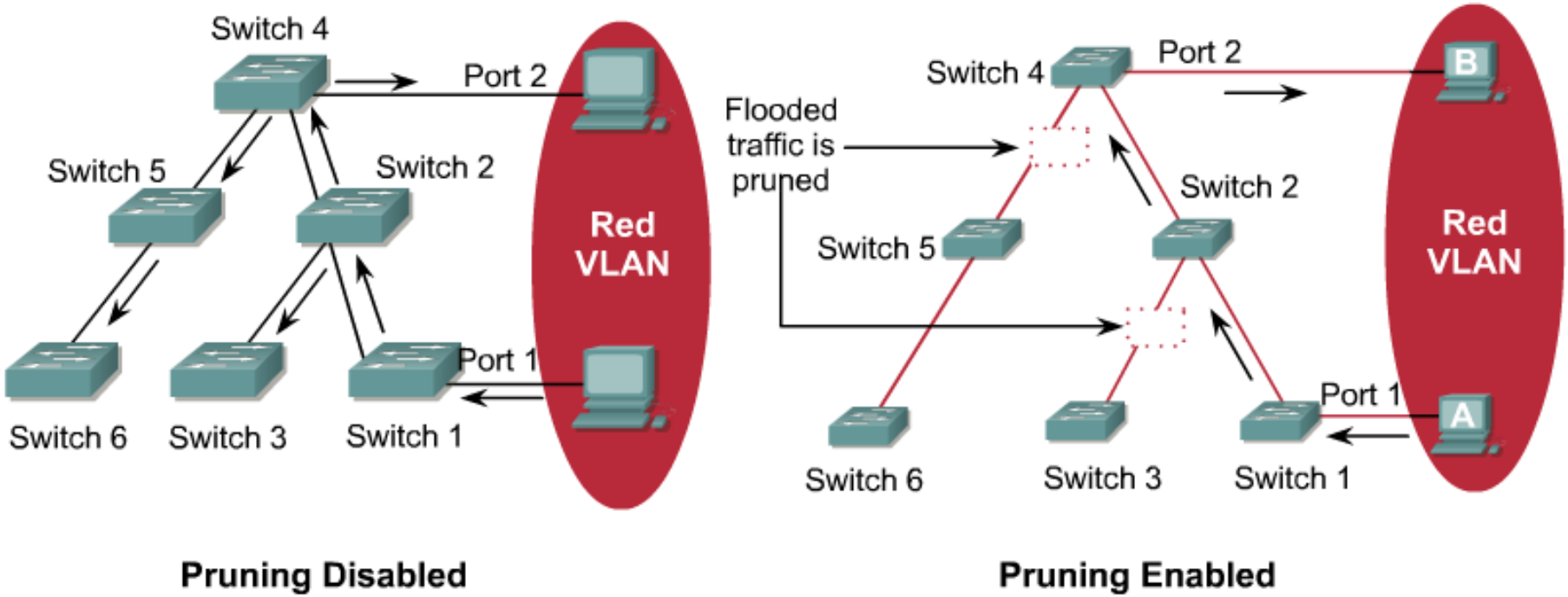
- VLAN info field

0	1	2	3
Info Length	VLAN Status	VLAN Type	VLAN Name Length
VLAN ID		MTU Size	
802.10 SAID **(Security Association Identifier)**			
VLAN Name (padded with zeros to multiple of 4 bytes)			

Činnosť VTP


1. Administrator adds new VLAN.
2. Revision 8 upgrades to revision 9.
Server
3. VTP propagates revision 9.
3. VTP propagates revision 9.
4. Revision 8 upgrades to revision 9.
5. VTP synchronizes the new VLAN information.
Client
Client
4. Revision 8 upgrades to revision 9.
5. VTP synchronizes the new VLAN information.
Transparent mode passes the VTP advertisements but does not synchronize.

VTP pruning



Pruning Disabled **Pruning Enabled**

- Zabraňuje šíreniu broadcastu do smerov, kde nie je potrebný (nie je port v danej VLAN)
  - Trunk nesie všetku prevádzku všetkých VLAN
  - Redukuje prevádzku Bcastu na sieti
  - Konfiguruje sa len na VTP serveroch
  - Ak máme transparent sw. odporúča sa vypnúť

Konfigurácia VTP

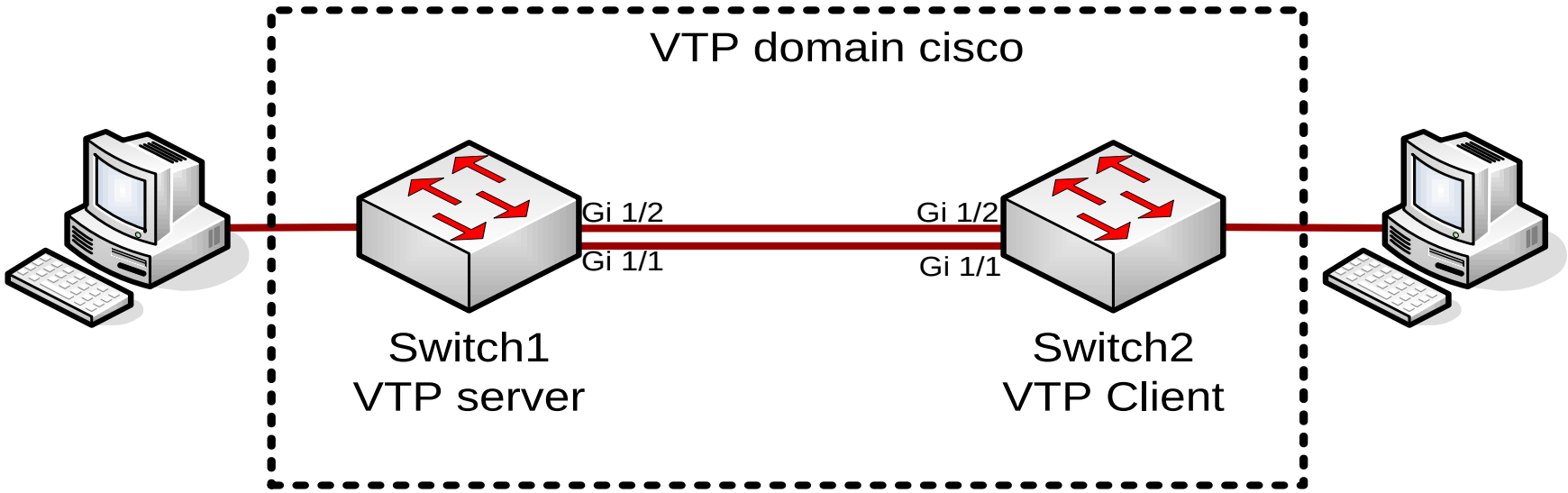
Základná konfigurácia VTP (v1 a v2)

1. Zisti/urči verziu VTP, ktorá sa bude používať/používa
2. Urči doménu
   - Hranice
   - Meno: Znakovo citilivé
3. Urči v akom móde budú tie ktoré prepínače pracovať
   - Odporúča sa jeden, max dva VTP servery pre doménu, ostatní sú klienti
4. Urči heslo, ktorým bude daná doména zabezpečená
   - Heslo je MD5 šifrované
5. Ak je potrebné zapni **pruning**

VTP konfiguračné príkazy

```
Switch(config)#vtp domain MENO_DOMENY
Switch(config)#vtp mode {client | server | transparent}
Switch(config)#vtp password TVOJE_HESLO

! Default je vtp v2 capable ale v móde vtp v1
! Kvôli kompatibilite
Switch(config)#vtp version {1 | 2}

!Len na VTP serveroch
Switch(config)#vtp pruning
```

Príklad VTP konfigurácie



Príklad konfigurácie

```
Switch1(config)#vtp mode server
Device mode already VTP SERVER.
Switch1(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
Switch1(config)#vtp password cisco
Setting device VLAN database password to cisco
Switch1(config)#^Z
%SYS-5-CONFIG_I: Configured from console by
    console
Switch1#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x00 0xCE 0xAD
    0x12 0xF0 0x96 0x31 0xF0
Configuration last modified by 0.0.0.0 at 3-1-93
    00:02:37
Local updater ID is 0.0.0.0 (no valid interface
    found)
```

```
Switch2(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch2(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
Switch2(config)#vtp pass cisco
Setting device VLAN database password to cisco
Switch2(config)#^Z
%SYS-5-CONFIG_I: Configured from console by
    console
Switch2#sh vtp sta
Switch2#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x00 0xCE
    0xAD 0x12 0xF0 0x96 0x31 0xF0
Configuration last modified by 0.0.0.0 at 3-1-
    93 00:02:37
Switch2#
```

Príklad konfigurácie

```
Switch1(config)#vlan 10
Switch1(config-vlan)#name Testovacia
Switch1(config-vlan)#^Z
%SYS-5-CONFIG_I: Configured from console by
    console
Switch1#sh vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 64
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x02 0xE1 0x6C
    0xC2 0x0D 0xEE 0x8C 0x4F
Configuration last modified by 0.0.0.0 at 3-1-93
    00:07:17
Local updater ID is 0.0.0.0 (no valid interface
    found)
Switch1#sh vlan

VLAN Name                               Status
    Ports
---- -------------------------------- ---------
    -------------------------------
...
10 Testovacia                           active
...
```

```
Switch2#sh vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 64
Number of existing VLANs        : 6
VTP Operating Mode              : Client
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x02 0xE1
    0x6C 0xC2 0x0D 0xEE 0x8C 0x4F
Configuration last modified by 0.0.0.0 at 3-1-
    93 00:07:17
Switch#sh vlan

VLAN Name                               Status
    Ports
---- -------------------------------- --------
    - -------------------------------
...
10 Testovacia                           active
...
```

Overenie činnosti VTP

```
Switch#sh vtp status
VTP Version                     : 1
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : Null
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A
   0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

Ak sa objaví iný VTP server s doménou, prázdny sa k nej pripojí.

Overenie činnosti VTP

```
Switch#sh vtp counters
VTP statistics:
Summary advertisements received    : 7
Subset advertisements received     : 5
Request advertisements received    : 2
Summary advertisements transmitted : 8
Subset advertisements transmitted  : 13
Request advertisements transmitted : 3
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0


VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Fa 0/8           43071            42766             5
```

Používanie VTPv3

- VTPv3 musí byť aktivovaná na prepínačoch manuálne
- Prepínač môže byť server/klient/transparent pre jednotlivé druhy databáz nezávisle
  - VLAN, MST, Unknown (placeholder pre budúce druhy databáz)
- Vo VTPv3 doméne sú dva druhy serverov
  - *Primárny server*: má právo modifikovať databázu
  - *Sekundárny server:* zálohuje dáta posielané prim. serverom.
  - Primárny server môže byť iba jeden v doméne
  - Primárny server sa nekonfiguruje, ale jeho funkciu si administrátor vyžiada z privilegovaného príkazového riadku
  - Prechod do roly primárneho servera môže byť chránený heslom, pričom toto heslo môže byť znečitateľnené
- VTPv3 switch môže byť v tej istej doméne ako VTPv2 sw.
  - Vie poslať VTPv2 správy
  - Ale neakceptuje správy od v1 a v2 zariadení

Konfigurácia VTPv3

```
Switch(config)# vtp version 3
Switch(config)# vtp domain MENO_DOMENY
Switch(config)# vtp mode { client | server | transparent | off}
                         [ vlan | mst | unknown  ]
Switch(config)# vtp password HESLO hidden
```

```
Switch(config)# vtp version 3
Switch(config)# vtp domain MENO_DOMENY
Switch(config)# vtp mode server vlan
Switch(config)# vtp mode client mst
Switch(config)# vtp password HESLO hidden
Switch(config)# end
Switch# vtp primary mst
System can become primary server for Mst feature only when configured
as a server

Switch# vtp primary vlan
This system is becoming primary server for feature vlan
Enter VTP Password:
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
Switch#
```

Časté chyby pri konfigurácii VTP

- Chyby:
  - Musí byť aktívny trunk
  - Nekompatibilné verzie VTP
  - Nesedí VTP meno domény
  - Nesedí VTP heslo pre doménu
  - Všetky prepínače sú VTP client
- Skontroluj:
  - či je OK domain name
  - či je OK domain password
  - skontroluj VTP version
  - skontroluj trunk links
  - skontroluj VTP modes
  - je tam server?
- **Upozornenie**
  - **Vždy keď pridávaš nový prepínač do VTP domény, uisti sa, že jeho revízne číslo je nižšie ako aktuálne používané !! !! !!**
    - Ináč hrozí riziko prepísania a straty aktuálne platných VLAN dát (aj pri VTP klient)
      - Platí najvyššie revízne číslo
  - Default VTP nastavenie prepínača je domain **Null, revision num. =0, mód server**
    - Ak príjme update zo servera v danej doméne, prípojí sa k danej doméne, zmení rev. Number

- Viac: Troubleshooting VLAN Trunk Protocol (VTP), DocID 98155

Pár tipov

- VTP revízne číslo je uložené vo flash (vlan.dat)
  - Reštart prepínača ho nepomôže resetnúť
- Zmena revízneho čísla VTP
  - Zmenou domény na inú a späť

```
Switch(config)#vtp domain Ina_domena
Switch(config)#vtp domain Povodna_domena
Switch(config)#^Z
Switch2#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 6
…
```

- Zmenou módu na transparent a späť na server
- Zakázanie VTP na prepínači

```
Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)#^Z
```

Vymazanie prepínača pripojeného do väčšej živej siete s VTP

- Môže nastať situácia kedy zmazané VLAN (vlan.dat) sa nám neustále nanovo objavujú na prepínači (znovu naučením cez VTP)

```
Switch#conf t
Switch(config)#
Switch(config)#interface range FastEthernet 0/1 -24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range GigabitEthernet
0/1 -2
Switch(config-if-range)#shutdown
15:45:59: %LINK-5-CHANGED: Interface GigabitEthernet0/2,
changed state to administratively down
Switch(config-if-range)#exit
Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)#no vlan ID_VLANY
```

Debug vtp

```
DLS1#debug sw-vlan vtp ?
  events       vtp events
  packets      vtp packets
  pruning      vtp pruning events
  redundancy   vtp redundancy
  xmit         vtp packets transmitted
```

```
DLS1(config)#debug sw-vlan vtp events
DLS1(config)#vlan 10
DLS1(config-vlan)#exit
DLS1#
*Mar  1 05:30:08.908: VTP LOG RUNTIME: Transmit vtp summary, domain netlab,
   rev 6, followers 1, tlv blk size 5 (inc #tlv field),
   MD5 digest calculated = 99 45 75 AA D3 0B 5A C4 9F 25 E1 FE BC 4E 39 59

*Mar  1 05:30:08.925: VTP LOG RUNTIME: Summary packet received, domain =
   netlab, rev = 6, followers = 1, length 77, trunk Fa0/7

*Mar  1 05:30:08.925: VTP LOG RUNTIME: Summary packet rev 6 equal to domain
   netlab rev 6

*Mar  1 05:30:08.925: VTP LOG RUNTIME: Subset packet received, domain =
   netlab, rev = 6, seq = 1, length = 224
```

Debug sw-vlan vtp events – VTP domain mismatch

```
*Mar  1 00:36:39.828: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed
to swlab.

*Mar  1 00:36:40.960: %DTP-5-DOMAINMISMATCH: Unable to perform trunk
negotiation on port Fa0/11 because of VTP domain mismatch.

*Mar  1 00:36:40.969: %DTP-5-DOMAINMISMATCH: Unable to perform trunk
negotiation on port Fa0/12 because of VTP domain mismatch.
```

Debug sw-vlan vtp events - VTP password mismatch

```
*Mar  1 00:51:04.912: VTP LOG RUNTIME: Summary packet received, domain = swlab, rev = 2,
followers = 1, length 77, trunk Fa0/9

*Mar  1 00:51:04.912: VTP LOG RUNTIME: Summary packet rev 2 greater than domain swlab rev 1

*Mar  1 00:51:04.912: VTP LOG RUNTIME: Domain swlab currently not in updating state

*Mar  1 00:51:04.912: VTP LOG RUNTIME: pdu len 77, #tlvs 1

*Mar  1 00:51:04.912: VTP LOG RUNTIME: Subset packet received, domain = swlab, rev = 2, seq
= 1, length = 280

*Mar  1 00:51:04.912: VTP LOG RUNTIME: MD5 digest failing
calculated = 16 98 BB 99 5F 15 60 04 11 73 1D B3 17 A3 8D 8B
transmitted = 37 76 F2 00 3B 16 04 91 5C 1A F0 ED 79 90 7C DD
```

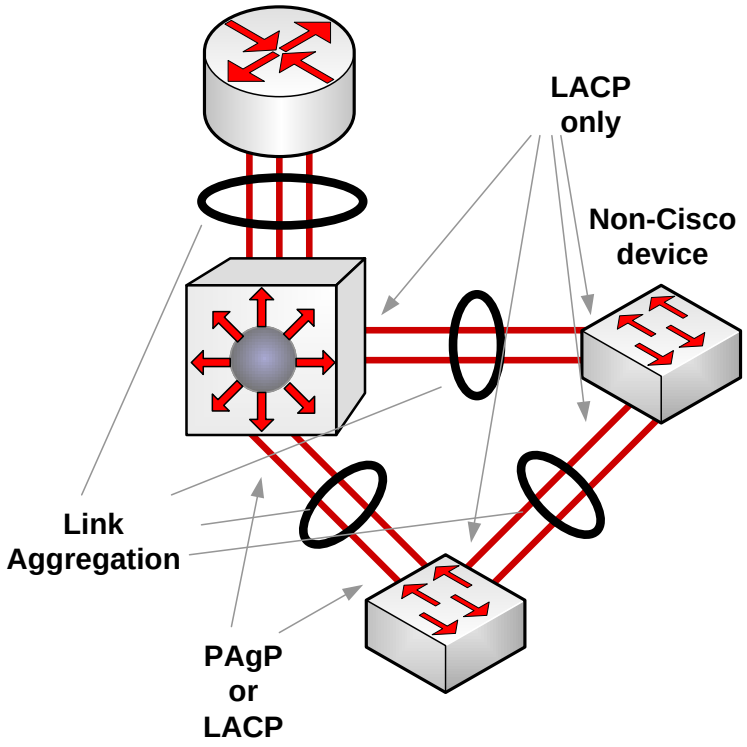
Link Aggregation cez EtherChannel, PAgP, LACP

Link Aggregation cez EtherChannel

- Technológia umožňujúca logicky zgrupovať fyzické prepínané porty do niekoľkonásobne výkonnejšieho prenosového kanála
- Poskytuje väčšiu priepustnosť
  - Vytvára logické porty vysokých rýchlostí
  - Switch-switch, switch-router, switch-server
  - Môžem združovať od 2 do 8 fyzických portov do jedného logického
  - Všetky fyzické rozhrania musia mať rovnakú rýchlosť, duplex a VLAN info
- Znižuje oneskorenie, zahltenie
- Poskytuje load-balance cez fyzické linky EtherChannelu
  - MAC, IP, IP+TCP/UDP
- Zjednodušuje konfiguráciu
  - Konfigurujem logický port a nie jednotlivé fyzické
- Zvyšuje redundanciu
  - Ak zlyhá jedna fyzická linka, stále môžem používať zvyšujúce
- Zjednodušuje činnosť niektorých protokolov
  - Napr. STP vidí celý EtherChannel ako jediný port

Implementácie agregácie linky

- EtherChannel využíva podporný signalizačný protokol na zostavenie združených kanálov
  - Overenie, či všetky linky idú k tomu istému zariadeniu
  - Overenie, či na susednom zariadení sú porty združené
  - Overenie, či schopnosti a vlastnosti portov dovoľujú z nich vytvoriť spoločný kanál
- PAgP (Port Aggregation Protocol):
  - Cisco proprietárny
- LACP (Link Aggregation Protocol):
  - IEEE štandard 802.3ad
- Oba protokoly sú rovnocenné
  - avšak nie kompatibilné



EtherChannel PAgP a LACP módy

PAgP	LACP
Auto: Pasívny stav, linka odpovedá na výzvy o vytvorenie EtherChannelu, ale neinicializuje jeho vytvorenie sama. Default mód.	**Passive:** To isté čo PAgP auto. Default mód.
Desirable: Mód, kedy linka je v aktívnom stave, aktívne žiada o zostavenie kanála posielaním PAgP paketov na druhú stranu.	**Active:** V tomto móde je linka v aktívnom dohadovacom stave, port iniciuje založenie (auto negotiation) kanálu posielaním LACP správ.
On: Tento mód vynúti prechod portu do EtherChannel kanála bez PAgP alebo LACP.	**On:** To isté čo „**On**“ pri PAgP.

Nastavenia režimov

Mód	Auto	Desirable	On	Off
Auto	No channel	Channel	No channel*	No channel
Desirable	Channel	Channel	No channel	No channel
On	No channel*	No channel	Channel	No channel
Off**	No channel	No channel	No channel	No channel

- Režim „ON“ nerobí PAGP negociáciu
- ** vypnutý režim cez slovíčko **NO** (channel je off mode)

Podmienky na vytvorenie EtherChannel

- Vytvorenie EtherChannel má nasledujúce obmedzenia pre porty, ktoré ho budú tvoriť:
  - Všetky porty rovnakú rýchlosť
  - Všetky porty rovnaký duplex
  - EtherChannel sa nevytvorí ak jeden z portov je SPAN (switched port analyzer)
  - Všetky porty priradené do rovnakých VLAN or musia byť trunk
  - Ak sú trunk, musia mať rovnaký rozsah povolených VLAN
  - Pri L3 EtherChannel sa priraďuje IP adresa logickému portu a nie fyzickým
  - Všetky zmeny aplikované na portchannel interface ovplyvnia ehterchannel,
    - všetky zmeny aplikované na fyzický port ovplyvnia len fyzický port

Distribúcia prevádzky nad Etherchannel – Load Balance

- EtherChannel nedistribuje rámce na princípe round-robin obsluhy
  - Riziko doručenia rámcov v nepôvodnom poradí
- Používa niektorú distribučnú politiku (závislú od platformy a používateľa)
- Load balancing môže byť založené na nasledujúcich kritériách:
  - **src-mac**: Source MAC address
  - **dst-mac**: Destination MAC address
  - **src-dst-mac**: Source and destination MAC addresses
  - **src-ip:** Source IP address
  - **dst-ip:** Destination IP address
  - **src-dst-ip:** Source and destination IP addresses (*default*)
  - **src-port:** Source TCP/User Datagram Protocol (UDP) port
  - **dst-port:** Destination TCP/UDP port
  - **src-dst-port:** Source and destination TCP/UDP ports

Konfigurácia EtherChannel

Konfigurácia EtherChannel

- Konfigurácia PAgP
  - Priradenie fyzických portov do kanála s daným číslom a v danom móde

```
channel-group GROUP_NUMBER mode {MODE}
```

    - Nie viac ako šesť kanálov
  - Nastavenie protokolu (ak treba)

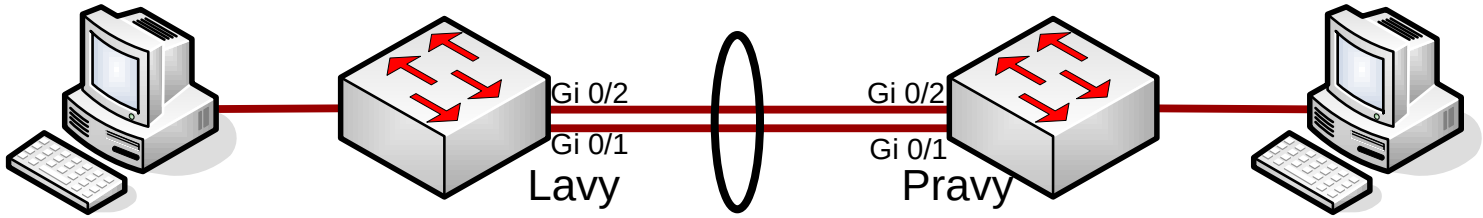
```
channel-protocol {pagp | lacp}
```

  - Konfigurácia logického EtherChannelu

```
interface port-channel
CHANN_GROUP_NUMBER
```

Vytvorí logický interface, ktorý sa ďalej konfiguruje

Príklad konfigurácie – PAgP L2 etherchannel



- Vytvorenie etherchannelu a následne trunku

```
Pravy(config)#int range gi 0/1 -2
Pravy(config-if-range)#channel-group 1 mode
   desirable
Creating a port-channel interface Port-channel 1
Pravy(config-if-range)#exit
Pravy(config)#int port-channel 1
Pravy(config-if)#switchport mode trunk
Pravy(config-if)#end
```

```
Lavy(config)#int ra gi 0/1 -2
Lavy(config-if-range)#channel-group 1 mode
   desirable
Lavy(config-if-range)#end
```

Čísla majú len lokálny význam, nemusia byť zhodné

Overenie konfigurácie – sh int trunk

```
Lavy#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         auto         802.1q         trunking      1

Port        Vlans allowed on trunk
Po1         1-4094

Port        Vlans allowed and active in management domain
Po1         1

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1
Lavy#
```

```
Pravy#sh int trunk

Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      1

Port        Vlans allowed on trunk
Po1         1-4094

Port        Vlans allowed and active in management domain
Po1         1

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1
Pravy#
```

Overenie konfigurácie etherchannel

```
Switch# show etherchannel
```

```
Switch# show etherchannel summary
```

```
Switch# sh etherchannel port-channel
```

```
Switch# sh etherchannel CHANN_GROUP port-channel
```

```
Switch# sh etherchannel detail
```

```
Switch# sh interface etherchannel
```

```
Switch# sh interface TYPE SPEC etherchannel
```

Overenie konfigurácie
sh etherchannel

```
Pravy#sh etherchannel
 Channel-group listing:
                 ----------------------

Group: 1
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   PAGP

Group: 2
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
```

Overenie konfigurácie – sh etherchannel summary

```
Lavy#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate
    aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------
    -------------------------------
1    Po1(SU)         PAgP       Gi0/1(P)
    Gi0/2(P)
7    Po7(SU)         LACP       Gi0/3(P)
    Gi0/4(P)

Lavy#
```

```
Pravy#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate
    aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------
    -----------------------------------
1    Po1(SU)         PAgP       Gi0/1(I)
    Gi0/2(I)
7    Po7(SU)         LACP       Gi0/3(P)
    Gi0/4(P)

Pravy#
```

SU
S - Switched
U – Up – In use

SD
S - Switched
D - Down

Overenie konfigurácie – sh etherchannel 1 port-channel

```
Pravy#sh etherchannel 1 port-channel
                Port-channels in the group:
                ---------------------------

Port-channel: Po1
------------

Age of the Port-channel   = 00d:00h:13m:45s
Logical slot/port   = 2/1          Number of ports = 2
GC                  = 0x00010001       HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   PAgP

Ports in the Port-channel:

Index   Load   Port     EC state         No of bits
------+------+------+------------------+-----------
  0     00     Gi0/1    Desirable-Sl        0
  0     00     Gi0/2    Desirable-Sl        0

Time since last port bundled:    00d:00h:09m:19s    Gi0/1

Pravy#
```

Channel number

Two physical ports

Remote site is OK, with compatible configuration

PAGP protocol

Desirable mode

Overenie konfigurácie – sh etherchannel detail

```
Pravy# sh etherchannel detail
                Channel-group listing:
                ----------------------

Group: 1
----------
Group state = L2
Ports: 2   Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol:   PAgP
Minimum Links: 0
                Ports in the group:
                -------------------
Port: Gi0/1
------------

Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Desirable-Sl    Gcchange = 0
Port-channel  = Po1         GC   = 0x00010001      Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =   PAgP

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
        d - PAgP is down.
```

Overenie konfigurácie
sh interface etherchannel

```
Pravy#sh interface etherchannel
----
Giga 0/1:
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Desirable-Sl    Gcchange = 0
Port-channel  = Po1         GC   = 0x00010001      Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =   PAgP

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
        d - PAgP is down.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                                Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count    Priority   Method  Ifindex
Gi0/1     SC    U6/S7   H       30s      1         128        Any      5001

Partner's information:

          Partner               Partner          Partner          Partner Group
Port      Name                  Device ID        Port       Age   Flags   Cap.
Gi0/1     Lavy                  0017.9446.ad00   Gi0/1      26s   SC      10001

Age of the port in the current state: 0d:00h:06m:33s
...
...
...
```

Overenie konfigurácie

```
Pravy#sh etherchannel ?
  <1-6>           Channel group number
  detail          Detail information
  load-balance    Load-balance/frame-distribution scheme
   among ports in
                  port-channel
  port            Port information
  port-channel    Port-channel information
  protocol        protocol enabled
  summary         One-line summary per channel-group
  |               Output modifiers
  <cr>
```

```
Pravy# sh run
```

```
Pravy# sh run interface port-channel NUMBEr
```

Zrušenie EtherChannelu

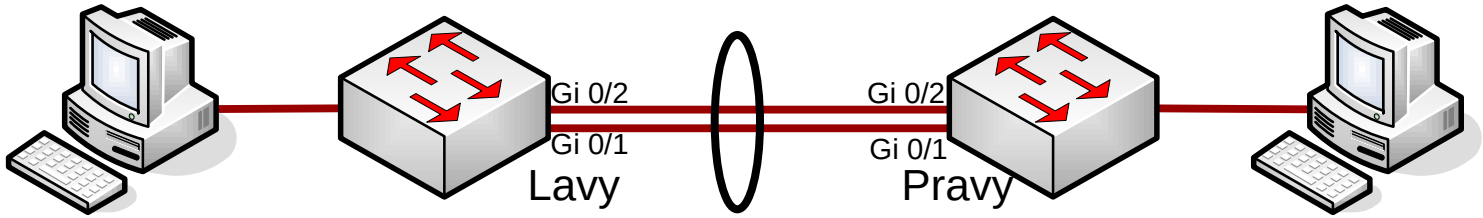
```
Pravy(config)#no int port-channel 1
Pravy(config)#int range gi 0/1-2
Pravy(config-if)# no channel-group 1 mode
Pravy(config-if)# no shut
```

```
Lavy(config)#no int port-channel 1
Lavy(config)#int range gi 0/1-2
Lavy(config-if)# no channel-group 1 mode
Lavy(config-if)# no shut
```

Konfigurácia Layer 3 EtherChannels

```
! Assign and Configure the Physical Interfaces
! =============================
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end


! Create and configure Port-Channel Logical Interfaces
! =============================
Switch# configure terminal
Switch(config)# interface port-channel 5
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.10.20.10 255.255.255.0
Switch(config-if)# end
```

Príklad konfigurácie – LACP L2 etherchannel




```
Pravy(config)#int ra gi 0/1-2
Pravy(config-if-range)#channel-protocol lacp
Pravy(config-if-range)#channel-group 1 mode active
```

```
Lavy(config)#int ra gi 0/1-2
Lavy(config-if-range)#channel-protocol lacp
Lavy(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

Lavy(config-if-range)#exit
Lavy(config)#int port-channel 1
Lavy(config-if)#switchport mode trunk
Lavy(config-if)#
```

Overenie konfigurácie LACP – sh etherchannel summary

```
Lavy#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate
    aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------
    ------------------------------
1      Po1(SU)          LACP      Gi0/1(P)
    Gi0/2(P)

Lavy#
```

```
Pravy#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate
    aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------
    ---------------------------------
1      Po1(SU)          LACP      Gi0/1(P)
    Gi0/2(P)

Pravy#
```

Overenie konfigurácie LACP

sh etherchannel protocol

```
Lavy#sh etherchannel protocol
                Channel-group listing:
                ----------------------

Group: 1
----------
Protocol:  LACP

Lavy#
```

sh ip int brief

```
Pravy#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  1.1.1.2         YES manual up                    up

… omitted …

GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  up                    up
Port-channel1          unassigned      YES unset  up                    up
```

Zrušenie LACP EtherChannelu

```
Pravy(config)#no int port-channel 1
Pravy(config)#int range gi 0/1-2
Pravy(config-if)# no shut
```

```
Lavy(config)#no int port-channel 1
Lavy(config)#int range gi 0/1-2
Lavy(config-if)# no shut
```

Configuring Etherchannel Load Balancing

- Load balancing can be based on the following variables:
  - **src-mac**: Source MAC address //*def. for 2960/3560*
  - **dst-mac**: Destination MAC address
  - **src-dst-mac**: Source and destination MAC addresses
  - **src-ip:** Source IP address
  - **dst-ip:** Destination IP address
  - **src-dst-ip:** Source and destination IP addresses (default)
  - **src-port:** Source TCP/User Datagram Protocol (UDP) port
  - **dst-port:** Destination TCP/UDP port
  - **src-dst-port:** Source and destination TCP/UDP ports

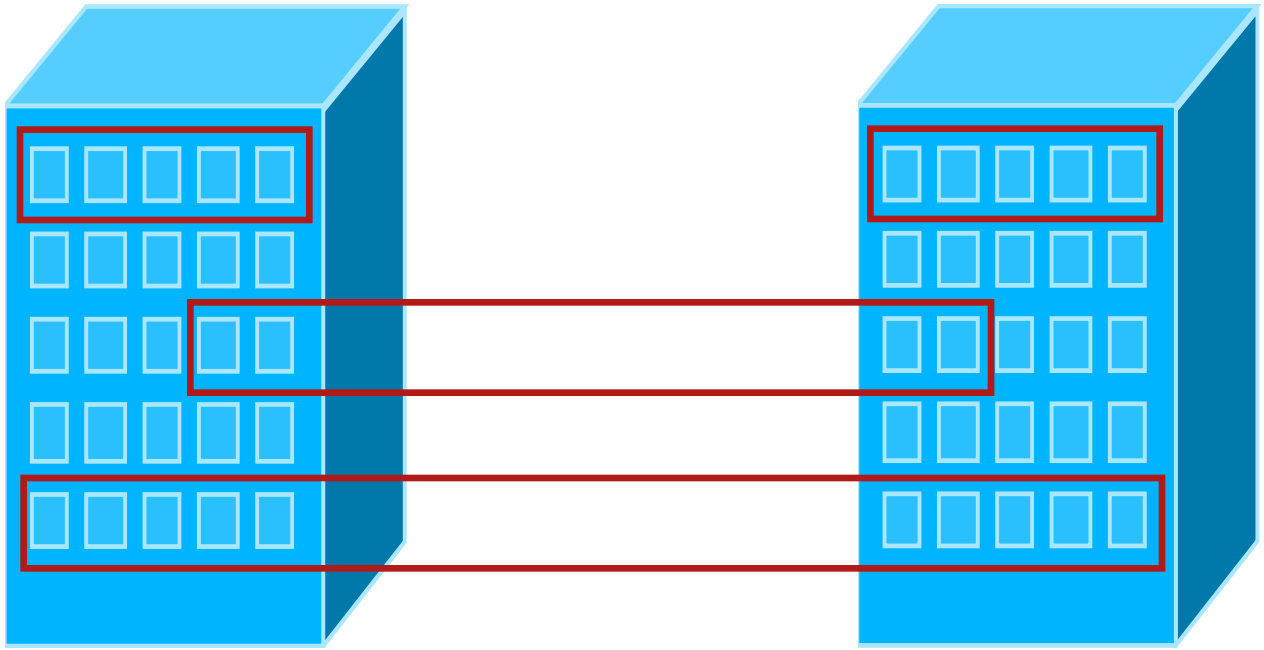
```
! Load Balance sa konfiguruje pre celý prepínač
Switch(config)# port-channel load-balance TYPE
Switch(config)# exit
….
Switch# show etherchannel load-balance
EtherChannel Load-Balancing Configuration: src-dst-ip
```

Privátne VLAN

Kópia aj v module 6 – Securing Campus LAN

Privátne VLAN

- Predstavte si, že máte dva bytové domy
- Všetky byty chcú mať konektivitu do internetu
- Jednotlivé byty chcú mať vzájomnú konektivitu takto:



- Nevyznačené byty nechcú mať vzájomnú konektivitu
- Ako by ste riešili túto sieť?

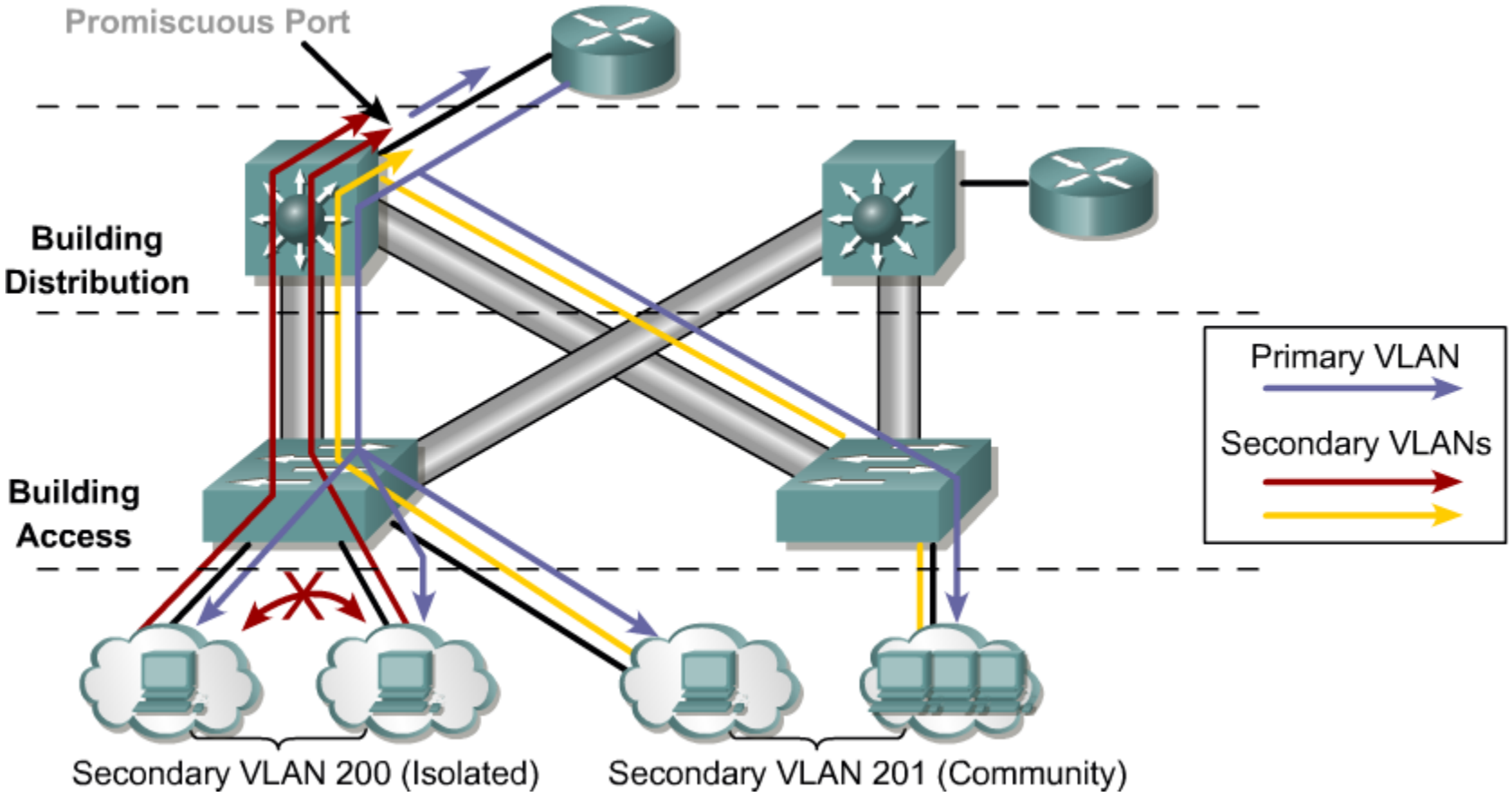
Privátne VLAN

- Privátne VLAN dokážu tento problem veľmi elegantne riešiť
- Podstatou privátnych VLAN je možnosť vnútorne rozdeliť jednu VLAN na niekoľko podskupín
  - Pôvodná VLAN sa volá primárna VLAN
  - Každá podskupina bude na prepínačoch reprezentovaná samostatnou VLAN – tzv. sekundárnou VLAN
  - Sekundárne VLAN môžu byť dvoch typov:
    - **Komunitné:** členské stanice komunitnej VLAN môžu navzájom komunikovať. Pod jednou primárnou VLAN môže byť ľubovoľný počet sekundárnych komunitných VLAN
    - **Izolované:** členské stanice izolovanej VLAN nemôžu navzájom komunikovať. Pod jednou primárnou VLAN môže byť najviac jedna sekundárna izolovaná VLAN
  - Zvonku toto členenie nevidno – navonok existuje iba jedna VLAN (primárna) a iba jedna IP sieť

Privátne VLAN

- Privátna VLAN je teda komplex niekoľkých komunitných a najviac jednej izolovanej sekundárnej VLAN, zastrešený jednou primárnou VLAN
- Tento komplex však musí mať nejaký vchod a východ
  - **Promiskuitný port**: port, ktorý môže komunikovať s ktorýmkoľvek iným portom v hociktorej komunitnej alebo izolovanej VLAN pod danou primárnou VLAN
- Pravidlá komunikácie v privátnej VLAN sú teda tieto:
  - Port v konkrétnej komunitnej VLAN môže komunikovať len s portmi v tej istej komunitnej VLAN, s trunkovými portmi a s promiskuitným portom
  - Port v konkrétnej izolovanej VLAN môže komunikovať len s trunkovými portmi a s promiskuitným portom

Privátne VLAN

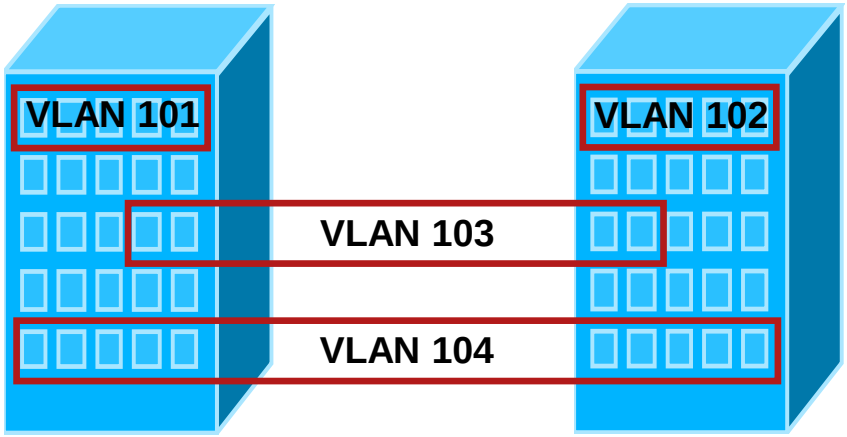


Privátne VLAN

- Ako sa robí značkovanie na trunkoch v prípade privátnych VLAN?
  - Ak rámec vošiel portom v komunitnej alebo izolovanej VLAN, na trunku dostane značku príslušnej sekundárnej VLAN
  - Ak rámec vošiel promiskuitným portom, na trunku dostane značku primárnej VLAN
- Pokiaľ je k externému routeru, ktorý je bránou pre túto privátnu VLAN, privedený celý trunk, vzniká problém
  - Ako routeru vysvetliť, že všetky sekundárne VLAN, ktoré na trunku vidí, sú v skutočnosti jediná primárna VLAN?
  - Riešenie: tzv. promiskuitné trunk porty pre privátne VLAN, ktoré automaticky zamenia značku sekundárnej VLAN za značku príslušnej primárnej VLAN, podporované na Cat4500 a 7600
  - Tohto obmedzenia sa netreba zbytočne obávať – obvykle bude smerovanie riešené pomocou SVI, alebo k externému routeru povedie promiskuitný port, ktorý nepoužíva značkovanie

Konfigurácia privátnych VLAN

```
vtp transparent
vlan 199
 private-vlan isolated

vlan 101-104
 private-vlan community

vlan 100
 private-vlan primary
 private-vlan association 101-104
 private-vlan association add 199
```




```
interface fa0/1 ! Komunitny port
 switchport mode private-vlan host
 switchport private-vlan
   host-association 100 101

interface fa0/2 ! Izolovany port
 switchport mode private-vlan host
 switchport private-vlan
   host-association 100 199

interface fa0/3 ! Promisc port
 switchport mode private-vlan prom
 switchport private-vlan
  mapping 100 101-104,199

interface Vlan100 ! Promisc SVI
 private-vlan mapping 101-104,199
```

Privátne VLAN – záverečné poznámky

- Privátne VLAN nie sú podporované s VTPv1 a VTPv2
  - VTPv3 podporuje privátne VLAN, ale je veľmi zriedkavé
- Privátne VLAN sú podporované len na multilayer prepínačoch Catalyst 3560 a vyššie
  - Na 2950/2960/3550 existujú iba tzv. chránené porty konfigurované príkazom `switchport protected`
  - Dva chránené porty na jednom prepínači navzájom nekomunikujú – chovajú sa ako členovia izolovanej VLAN
  - Táto izolácia sa však nedá zabezpečiť, ak sú chránené porty na dvoch rôznych prepínačoch
  - Chránené porty sa niekedy volajú Private VLAN Edge