Virtuálne LAN, Trunky (dot1q), Virtual trunk protocol (VTP)

CCNA Exploration Semester 3 - Kapitoly 3, 4

Ciele modulov

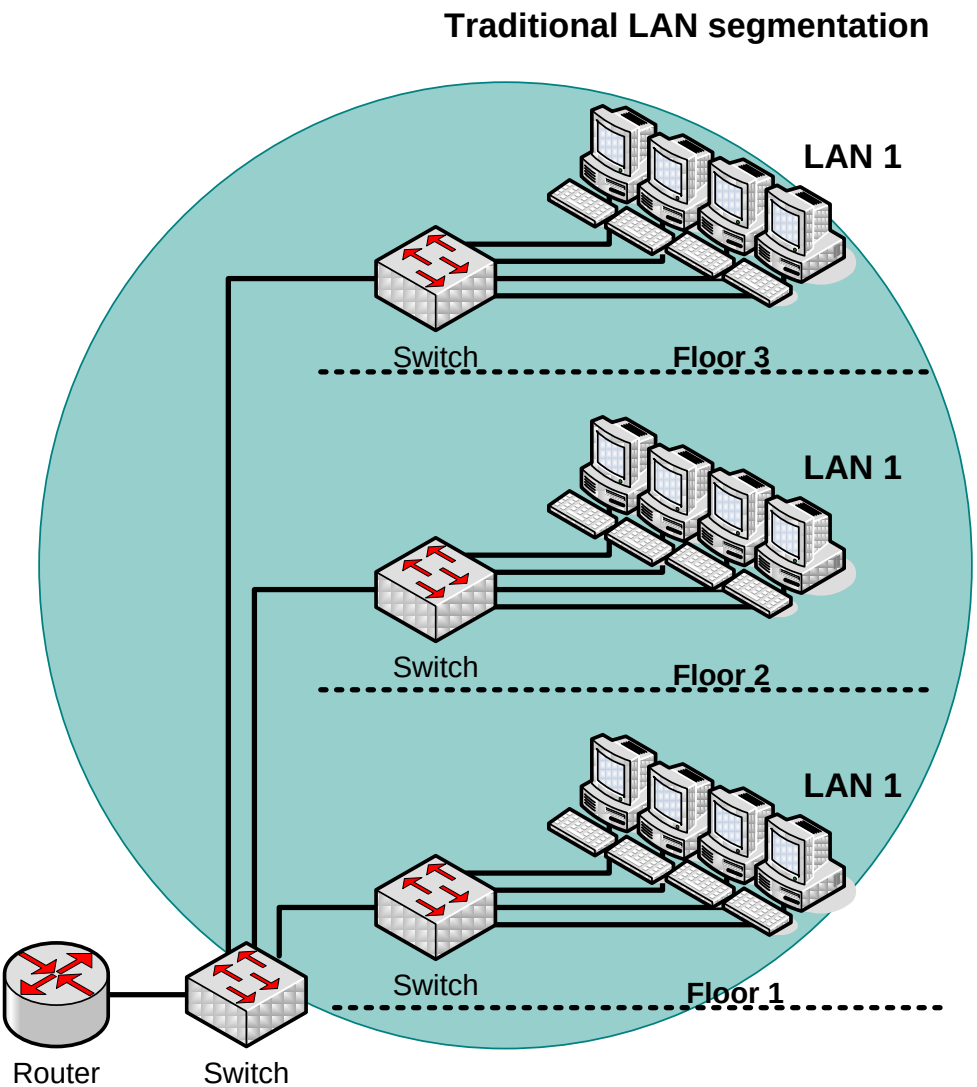
- Virtuálne LAN
- Trunk a trunkové mechanizmy 802.1q
- Virtual Trunking Protocol (VTP)
  - A jeho konfigurácia
- Dynamický trunk protokol (DTP)
- Chyby vo VLAN konfigurácii

VLANs

Virtuálne LAN (VLAN) - popis

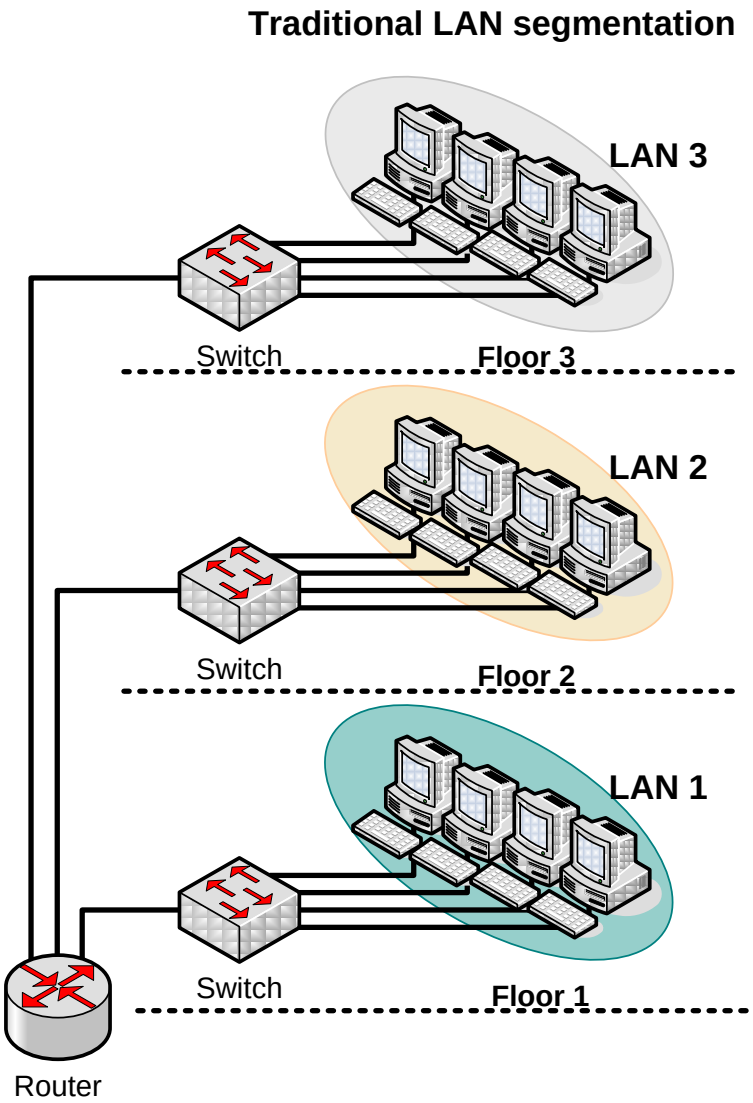
- Dôležitá vlastnosť Ethernet LAN prepínačov
- Virtual LAN (VLAN):
  - VLAN sú samostatné, **nezávislé** logické LAN siete, **definujúce broadcast doménu**, virtualizované v OS prepínača
  - VLAN umožňujú logicky segmentovať fyzické, prepínané LAN siete
    - Doteraz logické delenie záviselo od fyzickej dostupnosti portov prepínanej LAN siete
- Získame
  - Možnosti riadenia toku
  - Oddelenie fyzickej (geografickej) topológie od logickej
  - Môžeme vytvárať LAN siete napr.
    - Podľa funkcií v organizácií, projektových tímov, aplikácií a pod.

Tradičné LAN



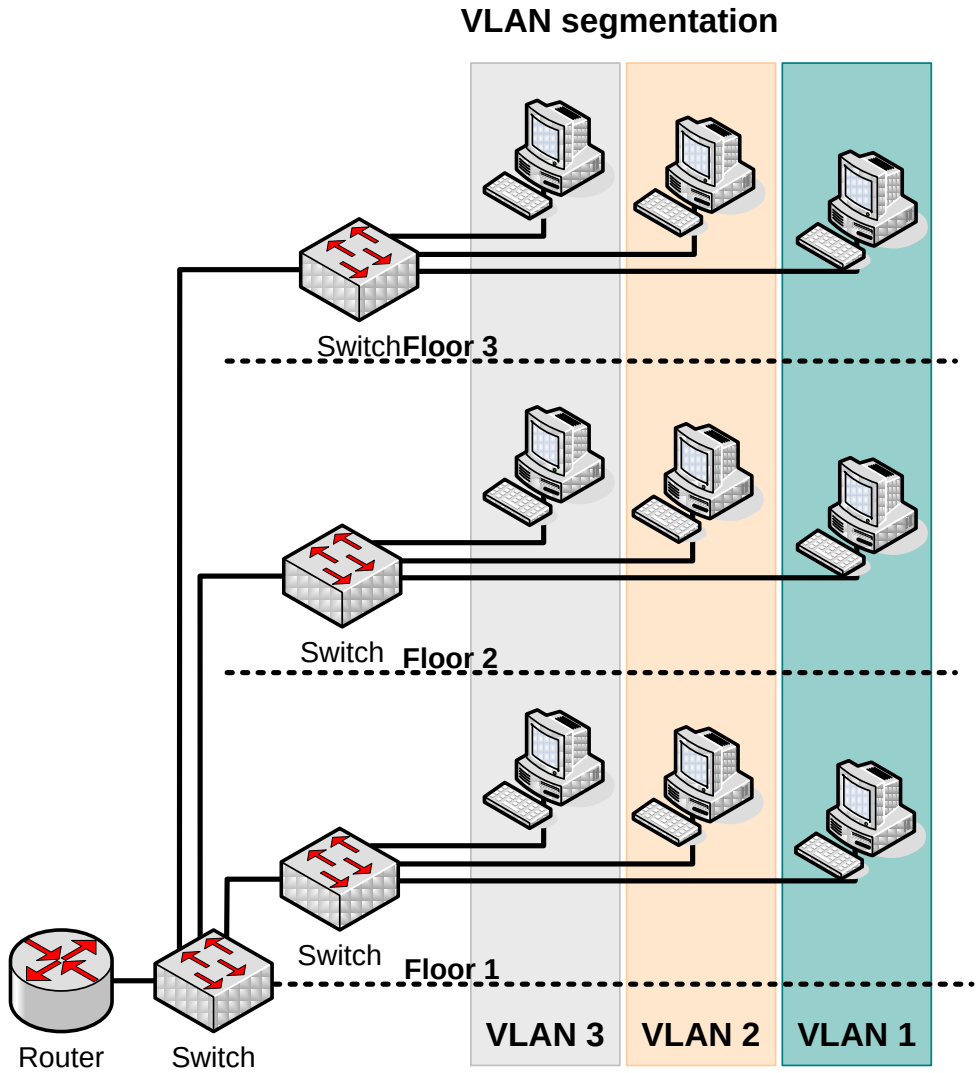
- **Tradičné LAN**
  - Nie je možné uskutočniť delenie koncových staníc podľa iných funkcií ako dostupnosť portov LAN sietí
  - Zariadenia je možné umiestniť len na daný fyzický segment
- Výhody
  - Jednoduchá počiatočná inštalácia a konfigurácia
- Problémy:
  - Veľké broadcast domény
  - Nedefinované hranice kam sa šíria neznáme a mcast rámce
  - Veľké oneskorenie
  - Zhoršená diagnostika
  - Bezpečnostné problémy
  - Pri raste siete náchylné na topo L2 slučky
    - Je potrebné STP

Tradičné LAN – segmentácia cez L3



- Riešenie broadcastu, riadenie toku, organizačné delenia a pod.
  - **Segmentácia siete** => použitím L3 zariadenia (smerovač)
  - **Alebo Virtual LAN**

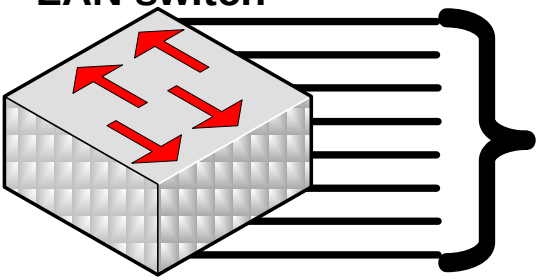
Virtuálna LAN



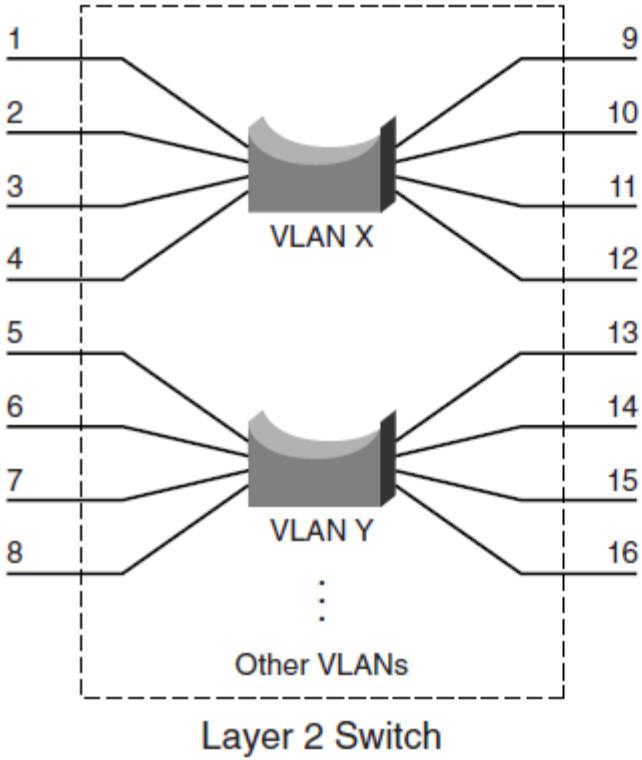
- **Virtuálna LAN**
  - Daná VLAN má všetky vlastnosti ako tradičná LAN
  - + logické členenie staníc podľa rôznych funkcií, kritérií
  - + nie je obmedzenie pri členení len na fyzický LAN segment, dostupnosť portov

Princíp VLAN

VLAN supported LAN switch



All ports the same LAN (functionality as traditional LAN switch)

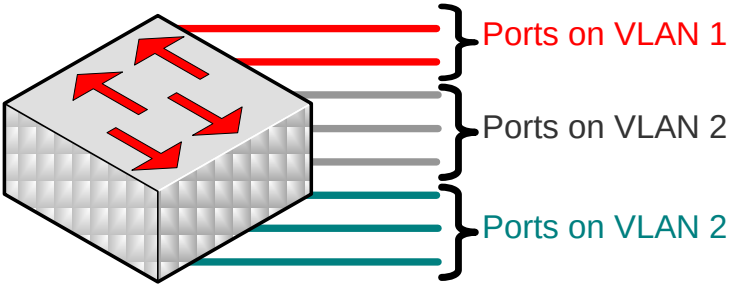


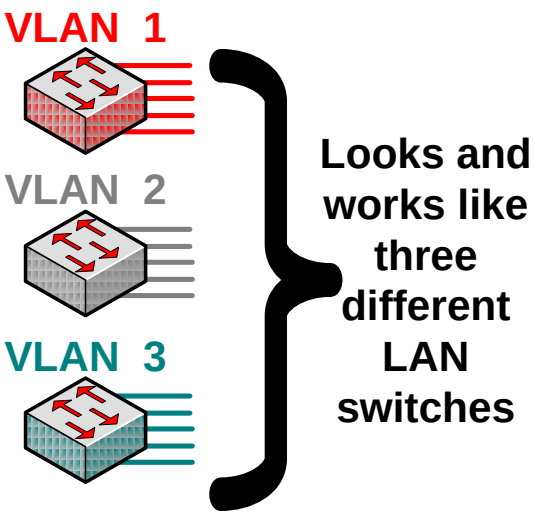
Forwarding Table

0000.1111.1111: port 11, vlan X
0000.2222.2222: port 6, vlan Y
0000.3333.3333: port 1, vlan X
0000.4444.4444: port 9, vlan X
0000.5555.5555: port 8, vlan Y
0000.6666.6666: port 14, vlan Y
0000.7777.7777: port 3, vlan X
0000.8888.8888: port 16, vlan Y

Broadcast: VLAN X: all VLAN X ports
Broadcast: VLAN Y: all VLAN Y ports

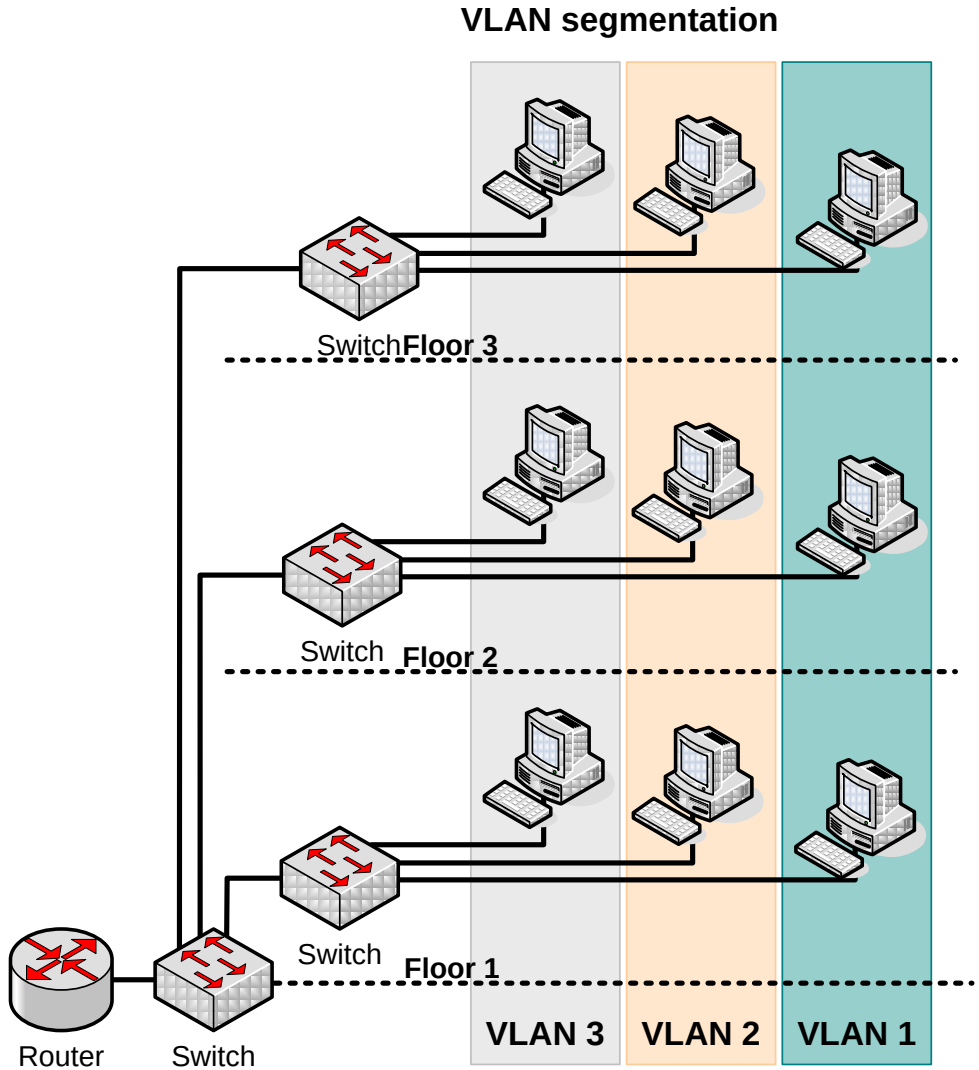
VLAN supported LAN switch





Looks and works like three different LAN switches

Broadcast domény a VLAN



- VLAN
  - Jeden prepínač viac VLAN
  - Jedna VLAN nad viacerými prepínačmi
  - Jedná VLAN jedna broadcast doména
  - Jedna VLAN jedna IP subsieť
    - Všetky hosty spoločný IP prefix
  - Komunikácia medzi VLAN
    - Vyžaduje smerovač
- Každý prepínač
  - Oddelenú Bridging table per VLAN
  - STP proces per VLAN

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
- Zvýšená priepustnosť
  - Segmentácia siete
    - Menej staníc, ktoré sa delia o prenosovú kapacitu
  - Redukcia broadcastu v sieti
- Šetrenie finančných prostriedkov na infraštruktúru

Typy VLAN - terminológia

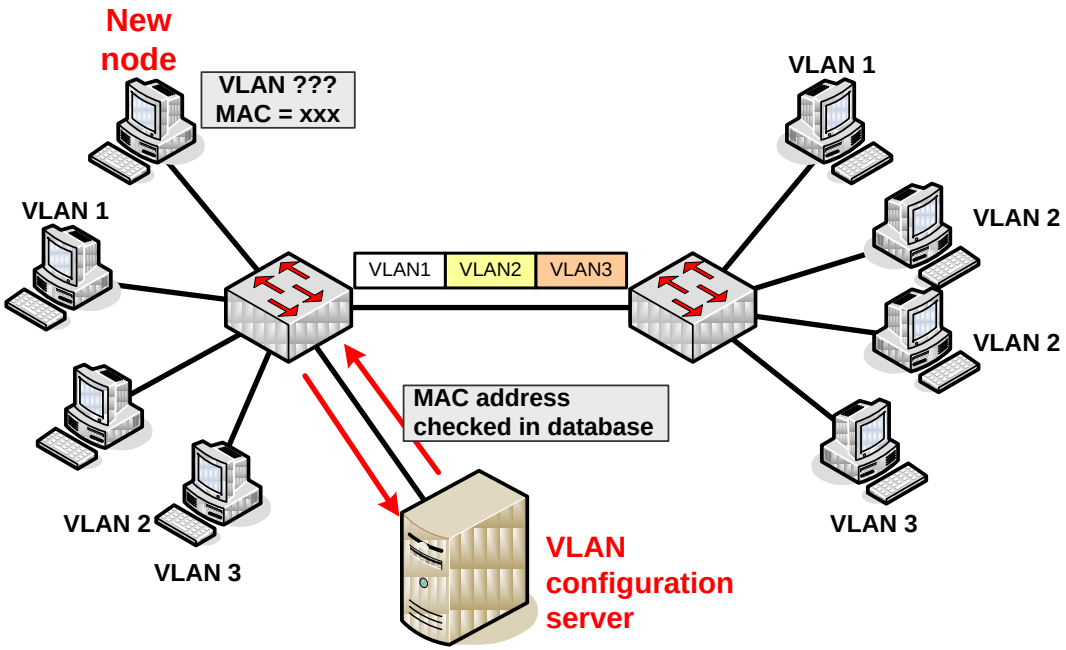
- **Default VLAN**
  - Na Cisco Catalyst **VLAN1**
    - Nie je možné zmazať, premenovať
  - Všetky porty sú default priradené do VLAN1
    - Aby PC mohli komunikovať aj bez do prepínača
  - CDP, STP komunikuje cez VLAN1 default
    - A user dáta ako každá bežná VLAN
- **Native VLAN**
  - Trunk je jej súčasťou
  - Dáta natívnej VLAN sú nesené neznačkované
- **Management VLAN**
  - Má priradenú **IP adresu**
    - Použitá za účelom manaž. prístupu na prepínač
  - Nemala by obsahovať user porty
- **Data VLAN**
  - Nesie používateľské dáta
- **Voice VLAN**
  - Oddelená pre VoIP

Typy VLAN (spôsoby vytvárania) - Statické

- **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**
  - Výhody
    - Bezpečnosť, jednoduchá konfigurácia a monitorovanie pohybu staníc v sieti

Typy VLAN (spôsoby vytvárania) - dynamické

- **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).



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**
  - identifikované VLAN ID 1006 – 4094
  - Určené pre providerov na rozšírenie služieb
  - Majú menej možností nastavenia ako Normálne VLAN
  - Sú uložené v running-config
  - Konfigurovateľné len ak je switch
    - **vtp mode transparent** pri VTPv1 a v2
    - VTPv3 podporuje v ľubovoľnom móde
- Cisco Cat2960 podporuje do 255 normálnych a rozšírených VLAN

VLAN ranges

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

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 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

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)

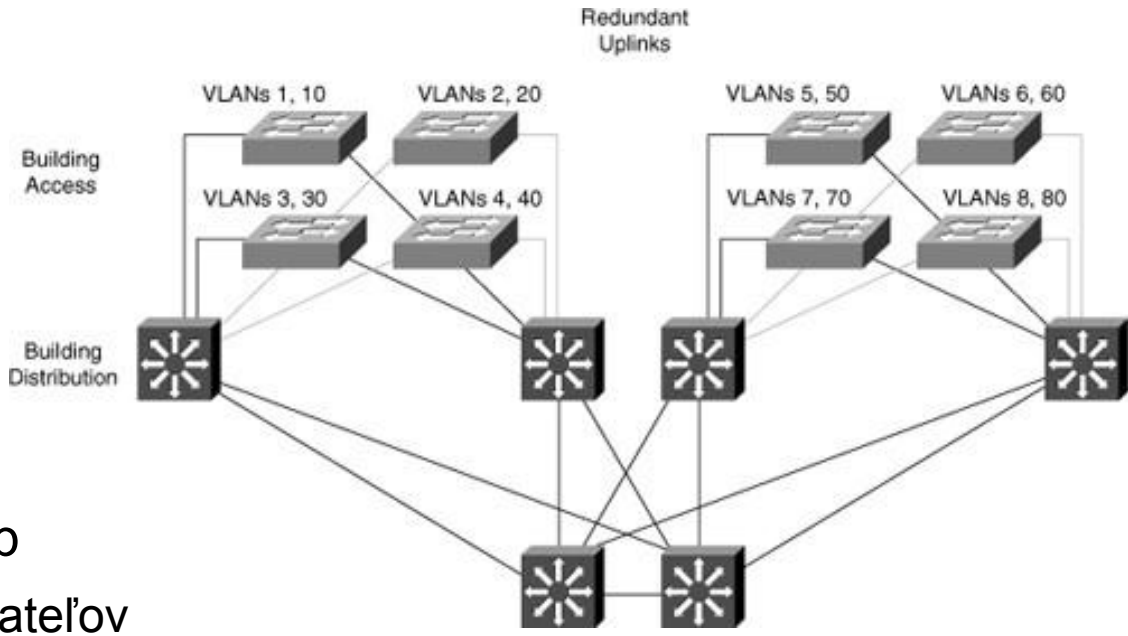
- Pôvodný koncept, ktorý odrážal pravidlo 80/20
  - Ktoré už dnes kvôli centralizácií serverov a Internetu neplatí
- VLAN sa rozprestierajú po celej sietí naprieč Access, Distro a Core vrstvou
  - Užívateľ v ľubovoľnej časti siete je stále v tej istej VLAN
- Užívatelia zgrupovaný skôr funkcionálne než 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

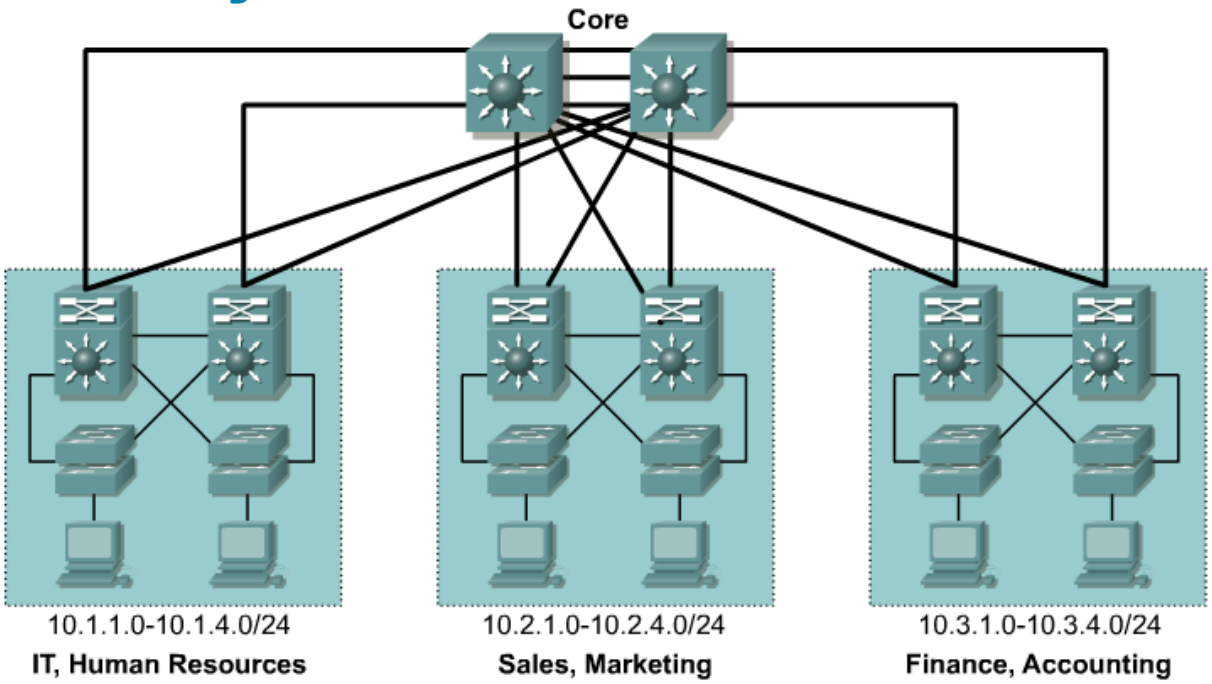


VLAN – **Odporúčania pri návrhu VLAN**

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

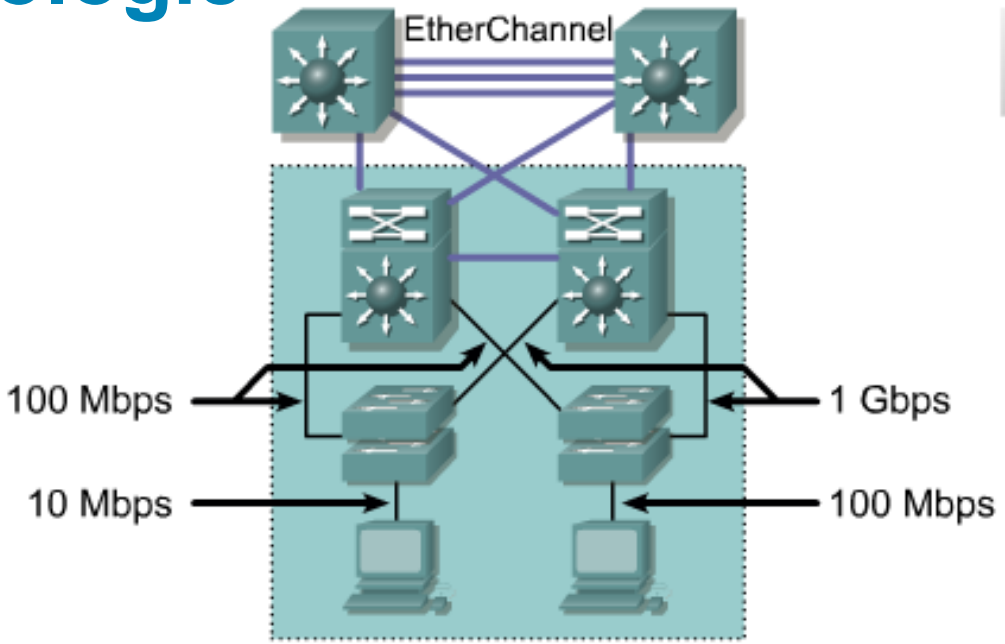
VLAN dizajn – adresovanie



- 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)

```
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:
  1. Vytvorenie VLAN
  2. Overenie VLAN konfigurácie
  3. Priradenie portu/portov prepínača do VLAN
  4. Overenie konfigurácie portov prepínača
  5. Overenie funkčnosti VLAN
     - Overenie adresy KZ
     - ping
  6. Implementácia zabezpečenia VLAN a prepínača
     - Napr. nová manažment VLAN
     - Parkovacia VLAN (inactive)
       - Kde priradím všetky nepoužité porty

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

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

- 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 database
    - Inač port neforwarduje data (je neaktívny) NIE JE PRAVDA!!!!
  - KS zdieľa IP adresu (prefix) s inými KS v danej VLAN.
- **Asociovanie**
  - Statické asociovanie
    - Konfiguráciou
  - Dynamické asociovanie
    - Na základe MAC adresy KS pripojeného 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
```

Vytvorenie access portu a asociovanie portu s VLAN

```
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
```

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
...
```

Preradenie portu prepínača do inej 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)#no switchport access vlan 2
Switch(config-if)#switchport access vlan 3


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
3 Marketing                            active Fa0/1
```

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
```

Overenie VLAN konfigurácie a priradenia portov

```
Switch#sh int INT SPEC switchport

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 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: On
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

! 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

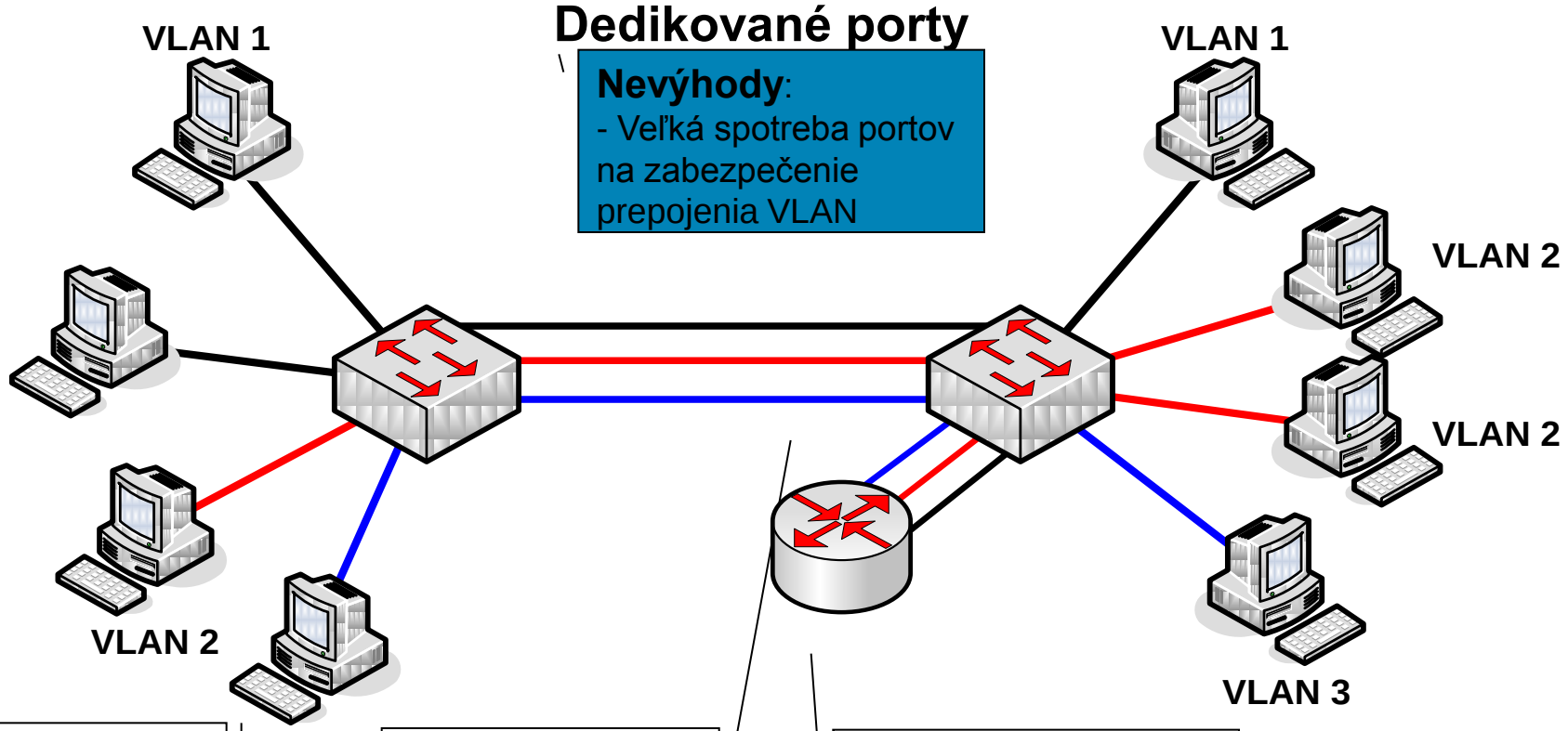
```
Switch(config)#default interface interface-id

Napr.

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

- Vrátenie default nastavenia na viac rozhraniach naraz

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

Prepájanie VLAN - Trunking mechanizmy a protokoly

Intra VLAN komunikácia - Dedikované porty

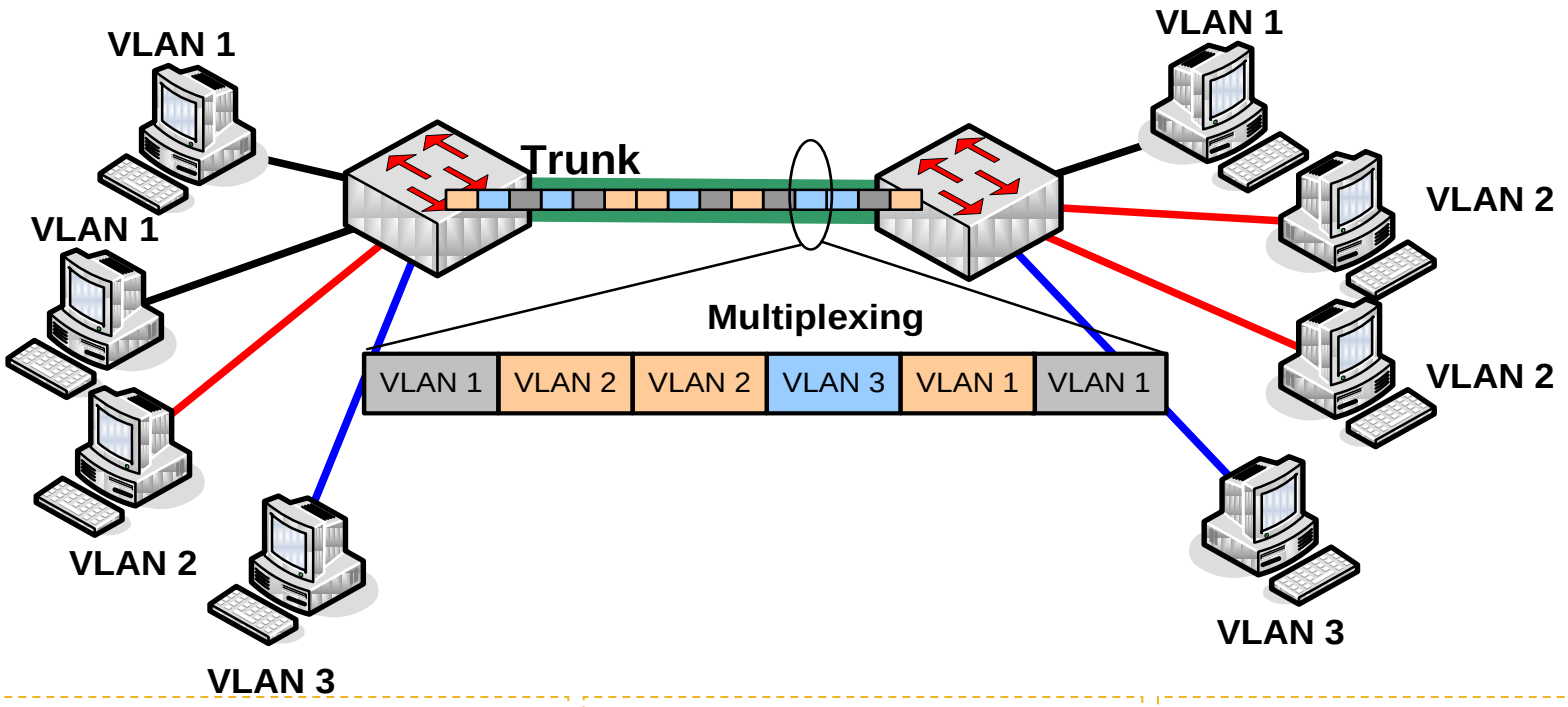


Predpokladajme dva prepínače s nakonfigurovanými 3 VLAN-ami. Ako zabezpečiť ich prepojenie?

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
  - Býva súčasťou tzv. **Native VLAN**
    - Rámce native VLAN prechádzajú trunk-om neznačkované
    - Oba konce trunk-u **musia byť** v tej istej Native VLAN

Trunk protokoly

- Trunk protokoly
  - Vyvinuté ako efektívne prostriedky prenosu rámcov rôznych VLAN cez fyzickú linku
  - Určujú akým spôsobom budú rámce multiplexované
- Dve značkovacie schémy (tagging schemes)
  - **ISL (Inter-Switch Link Protocol)**:
    - Proprietárny CISCO protokol
    - Optimalizovaný pre Cisco zariadenia
      - Problémy s kompatibilitou
    - Definuje enkapsuláciu rámcov cez trunk
      - K rámcu je pridaná nová hlavička s VLAN ID informáciou
  - **IEEE 802.1q**:
    - Značkovací VLAN štandard
    - Veľmi dobrá kompatibilita zariadení rôznych výrobcov
    - Preferované použitie
    - Nazývaný aj **dot1.q**

IEEE802.1q

Virtual Bridged Local Area Networks

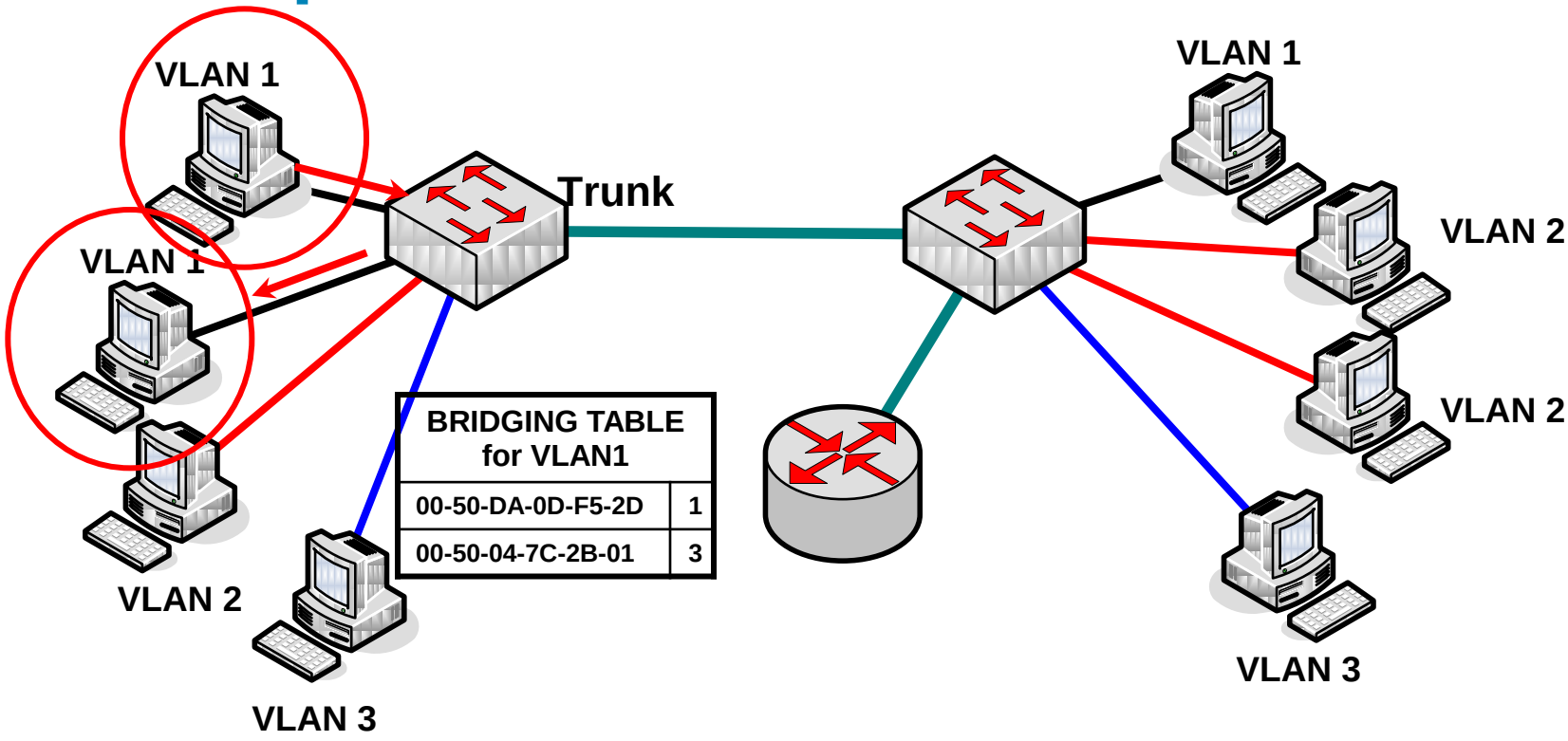
IEEE 802.1Q

- 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

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

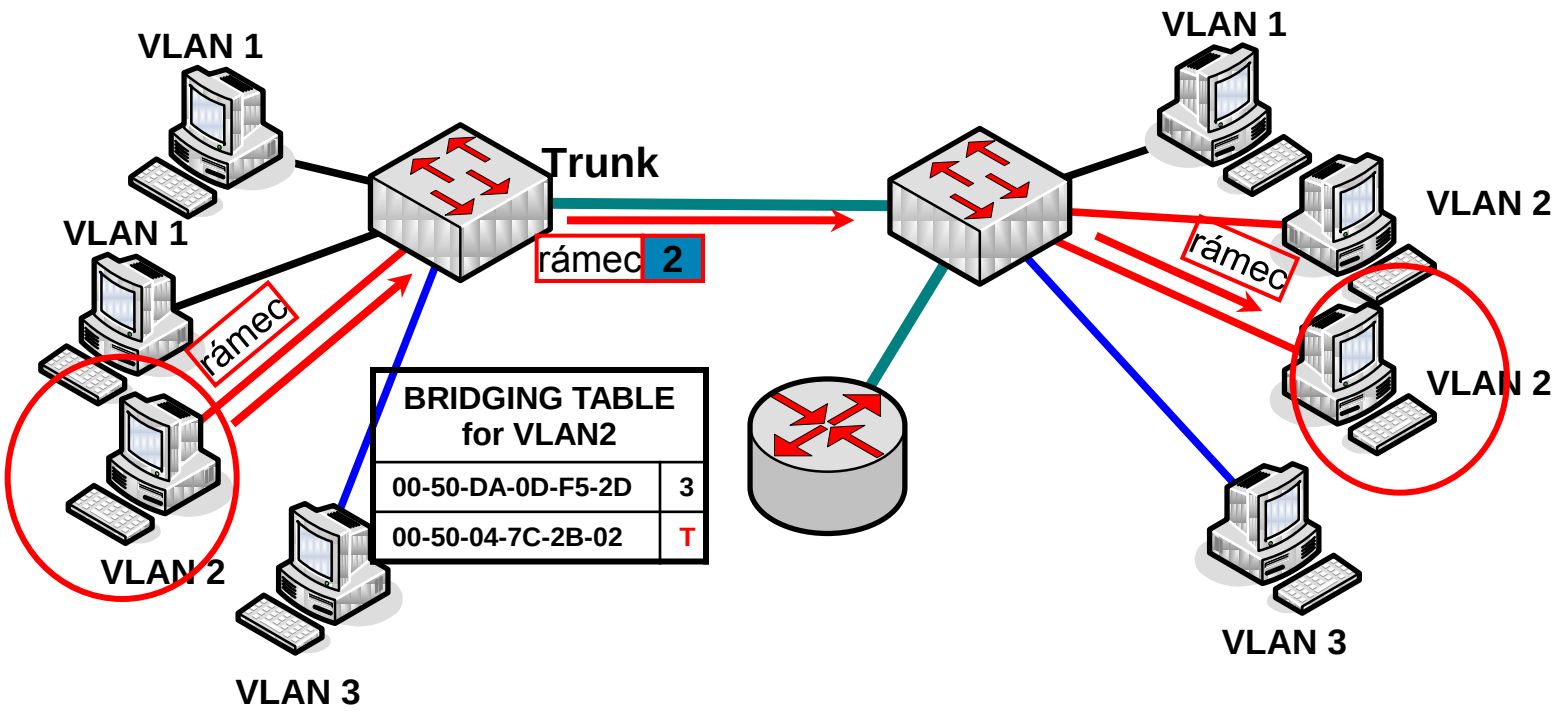


Príklad:
Komunikácia medzi stanicami vo vnútri VLAN (Intra VLAN) na to istom prepínači

-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



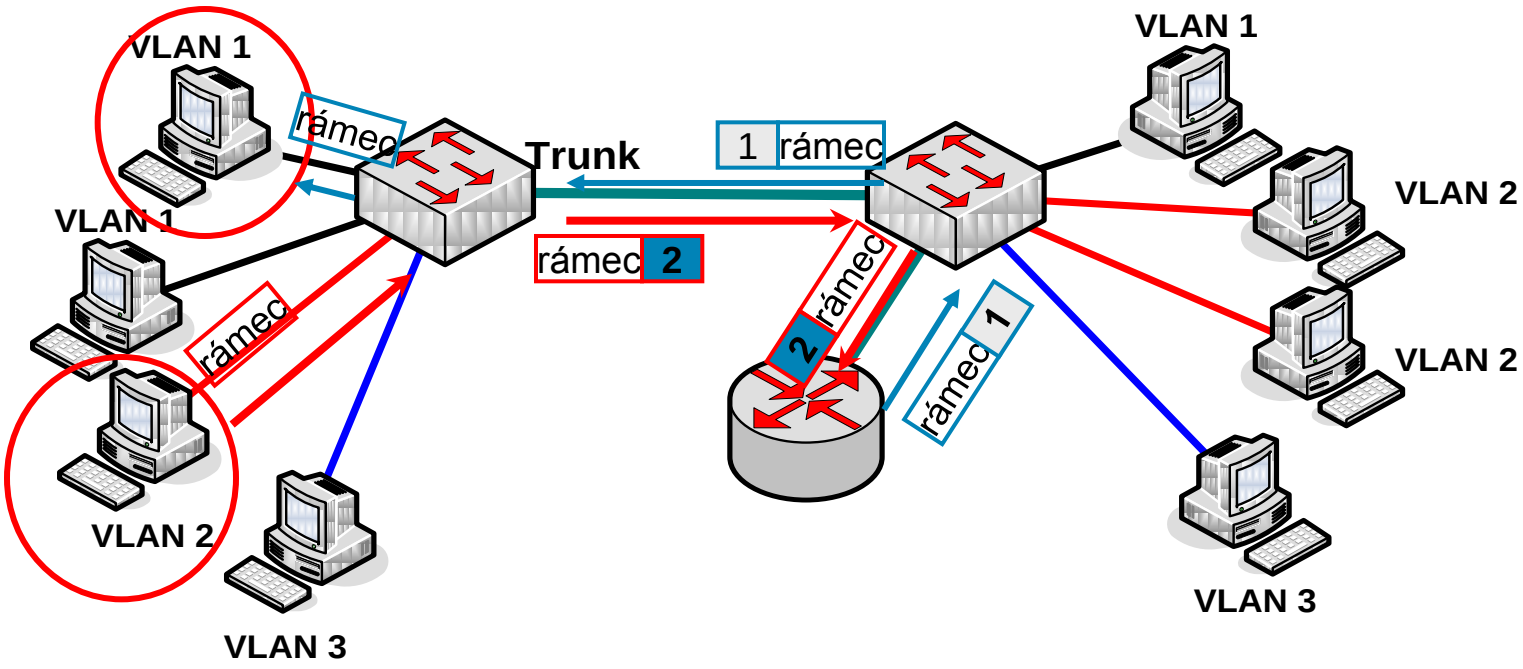
Príklad:
Komunikácia medzi stanicami vo vnútri VLAN (Intra VLAN) na **rôznych** prepínačoch.

-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

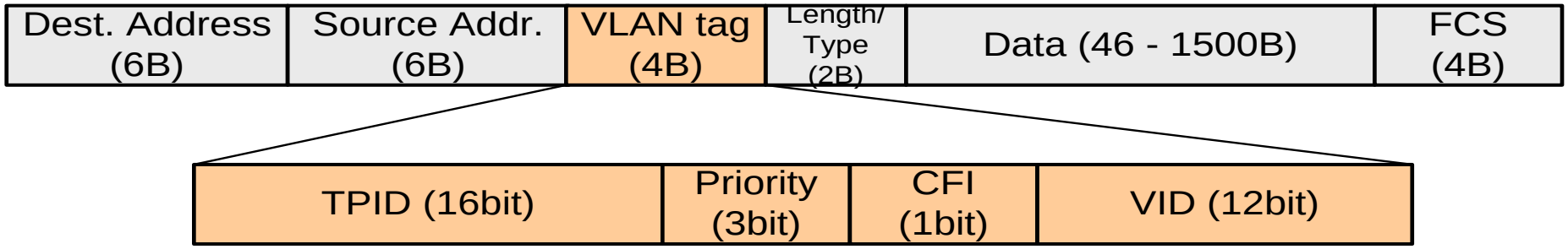
Rámec je **pozmenený (značkovaný) nakoľko vstupuje** na trunk port**!**

802.1q – Inter VLAN komunikácia



Príklad:
Komunikácia medzi stanicami **v rôznych** VLAN (Inter VLAN)

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
  - Použité v FDDI
  - CFI=0: MAC adresa je v kanonickom formáte
  - CFI=1: MAC adresa nie je v kanonickom formáte
- **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

Konfigurácia trunkov

Konfigurácia Trunk-u

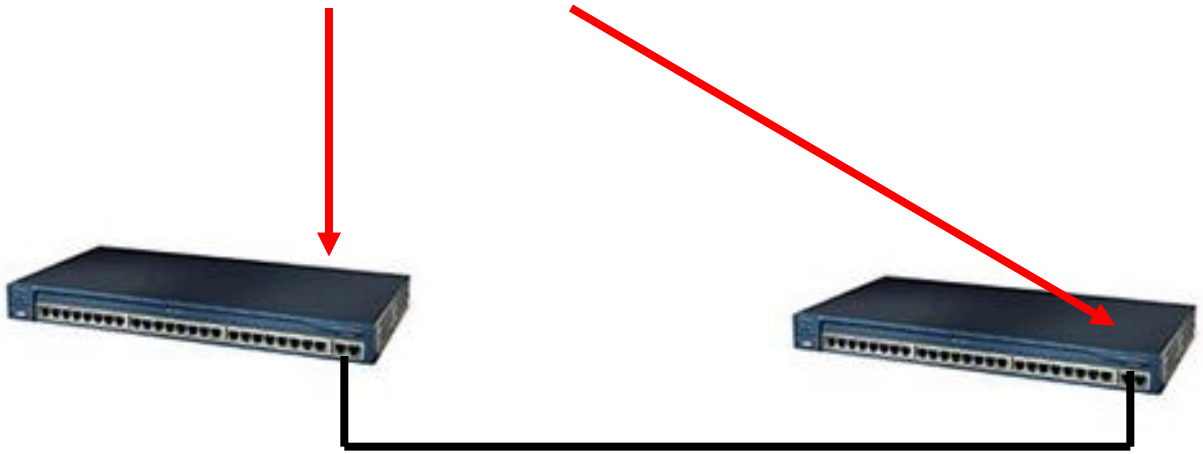
- Trunk môžeme konfigurovať
  - Manuálne (Staticky)
  - Dynamicky
    - Dynamic Trunking Protocol (DTP)
      - Allows dynamically negotiate trunk creation

Statická konfigurácia trunk portu Cat2950

cisco - HyperTerminal

File Edit View Call Transfer Help

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int gi 1/1
Switch(config-if)#switchport mode trunk
```



Connected 0:01:39 | Auto detect | TCP/IP | SCROLL | CAPS | NUM | Capture | Print echo

Doplnkové konfigurácie portu

```
! Zadefinovanie novej NATIVE VLAN
Switch(config-if)#switchport trunk native vlan 99

! Povolenie traverzovat trunk len urcitym VLAN
Switch(config-if)#switchport trunk allowed vlan ?
  WORD    VLAN IDs of the 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#
```

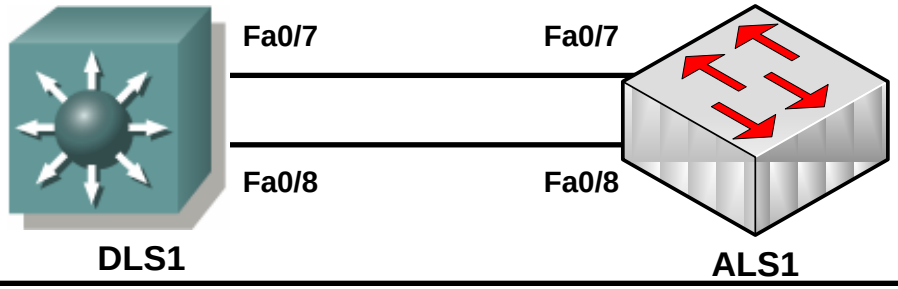
Overenie konfigurácie trunku

```
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

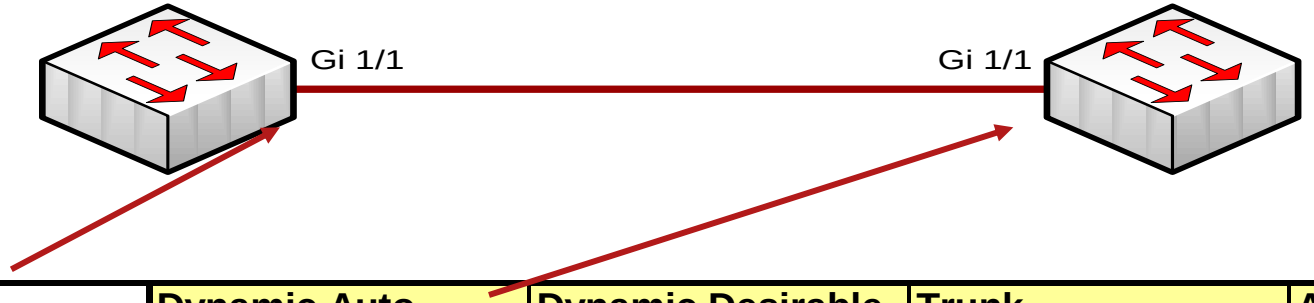
DTP - Dynamic Trunking Protocol

- Cisco proprietárny protokol
- Umožňuje automatické dohodovanie vytvárania trunkov zasielaním DTP rámcov medzi prepínačmi
- Defaultne je spúšťaný na Cisco zariadeniach
  - Ktoré ho podporujú
    - Nie všetky Cisco zariadenia podporujú DTP
  - Nijako neovplyvňuje možnosť statického zostavenia trunku či činnosť trunku

Operačné módy DTP

- **Dynamic Auto**
  - Default mód na Cat2960
  - Lokálny port prepínača 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
  - Lokálny port prepínača 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
  - Žiadne DTP rámce nebudú posielané
  - `Switch(config-if)#switchport nonegotiate`
- **Trunk („On“)**
  - Vytvorí trunk bez ohľadu na DTP žiadosti suseda alebo stav portu suseda
- **Access („Off“)**
  - Trunk nie je povolený na tomto porte

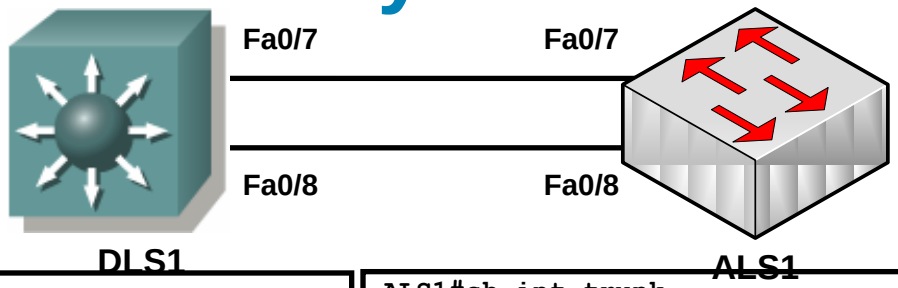
Operačné módy DTP – činnosť



	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 – statik trunk vs dynamic auto

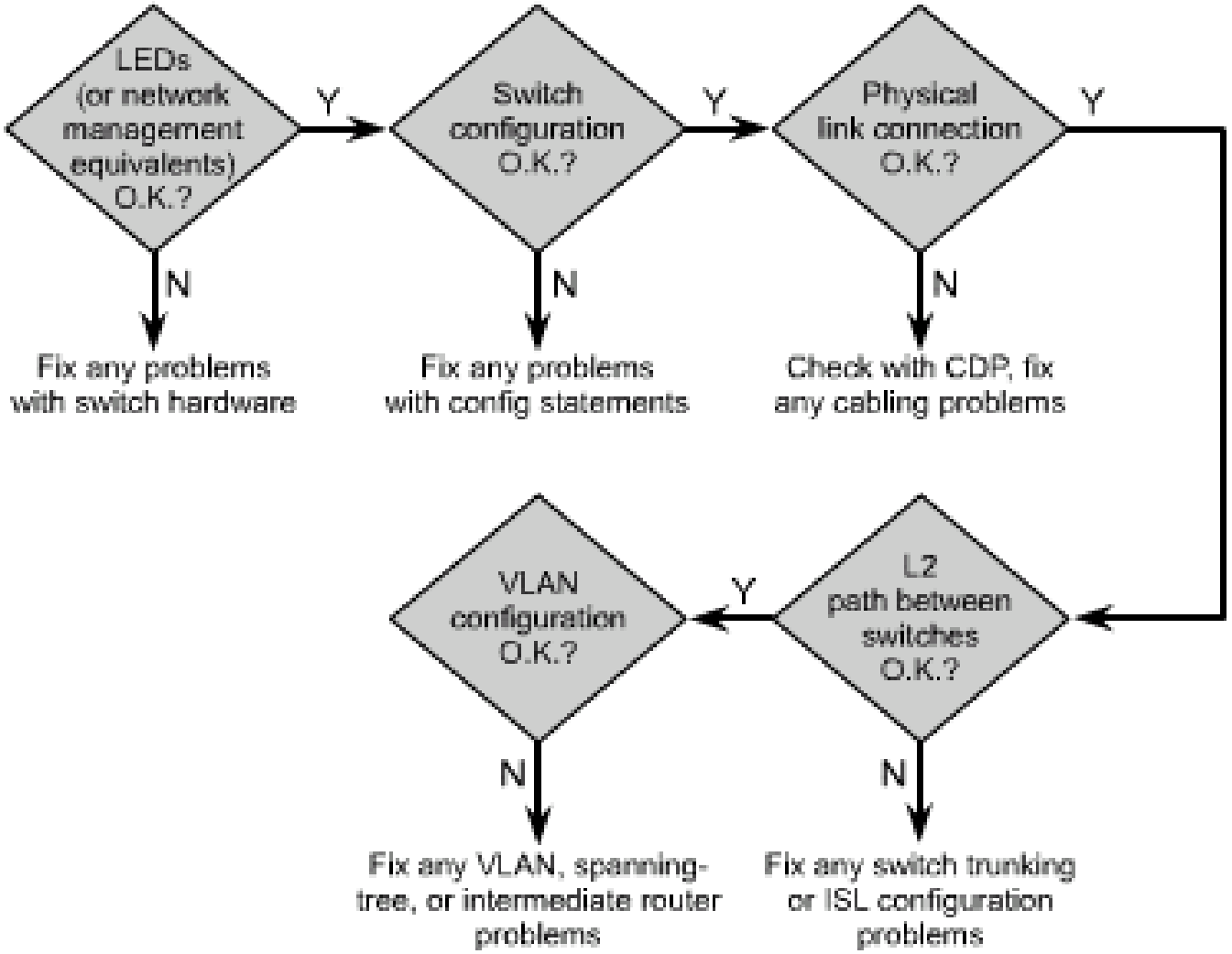



```
DLS1(config)#int ran fa 0/7 - 8
DLS1(config-if-range)#switchport trunk encapsulation
    dot1q
DLS1(config-if-range)#switchport mode trunk
DLS1#sh int trunk

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
```

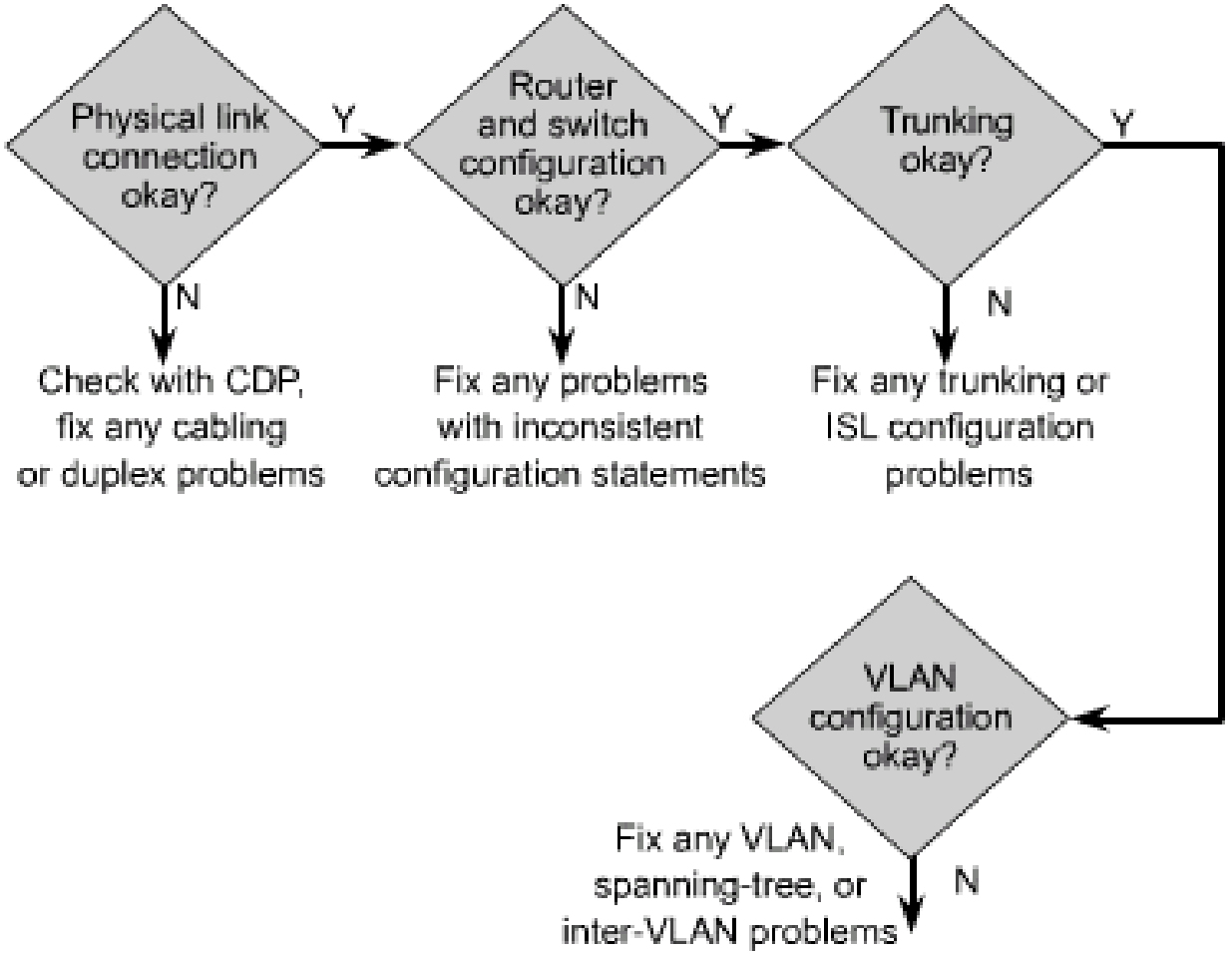
```
ALS1#sh int trunk

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
```

Diagnostika problémov

Hľadanie problému na L2 sieťach



Hľadanie problému vo 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 learrning guide]

Virtual Trunking Protocol (VTP)

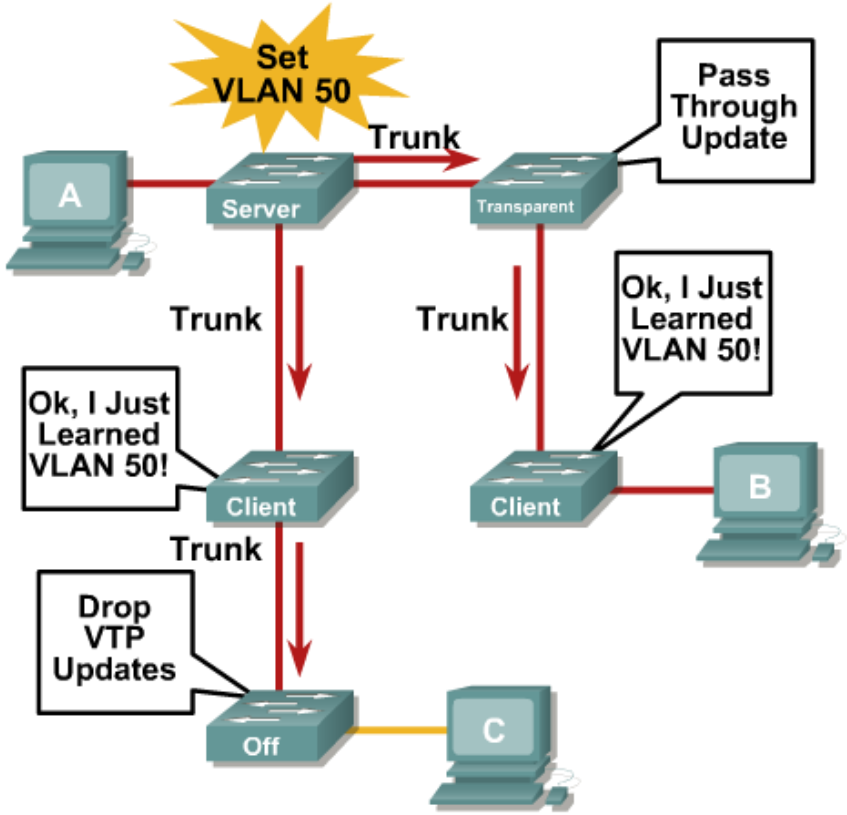
Virtual Trunking Protocol (VTP)

- 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 synchronizácia MSTP konfigurácie

Výhody použitia VTP

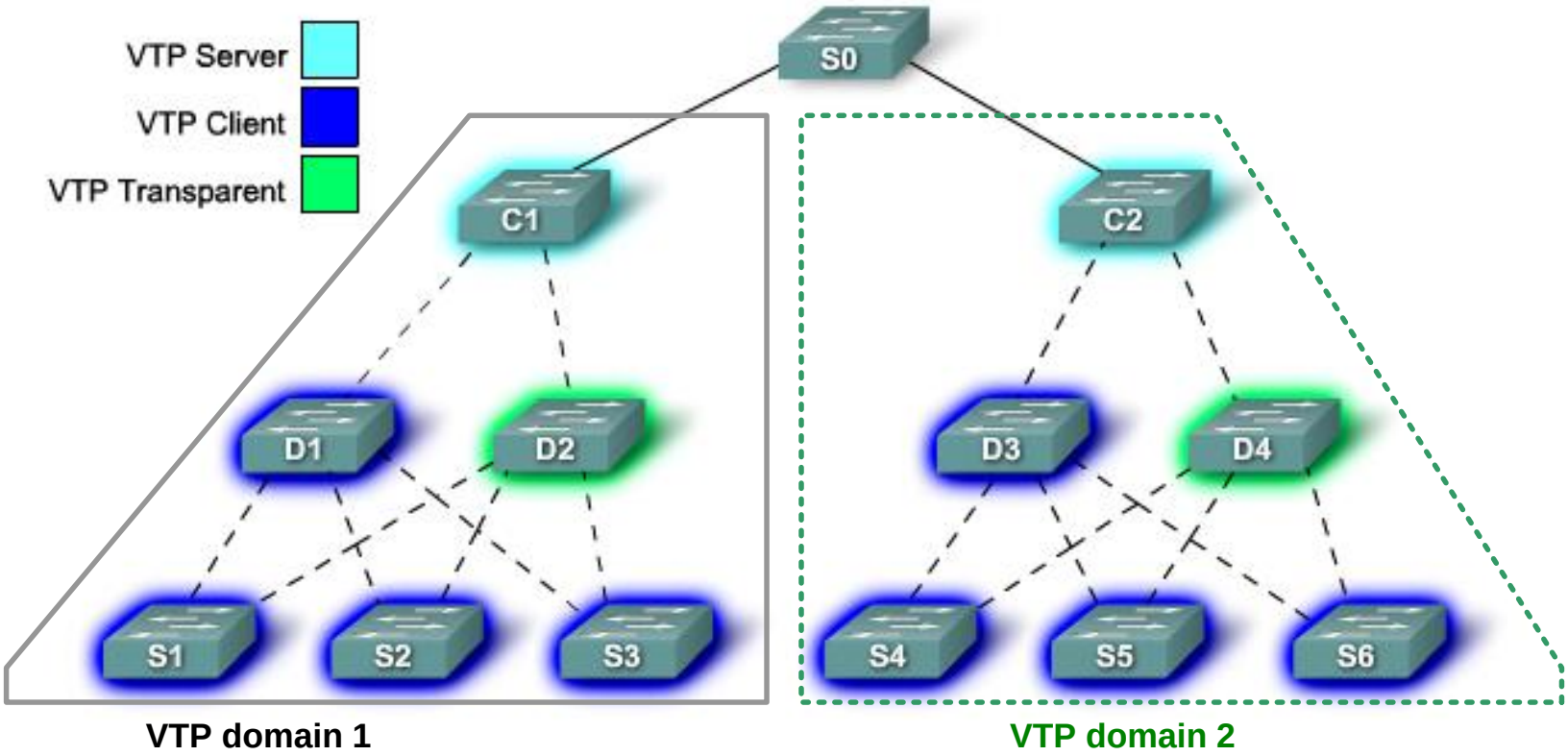


- Zjednodušený a konzistentný manažment VLAN naprieč prepínanou sieťou
- Uľahčené monitorovanie stavu VLAN
- Dynamické reportovanie aktuálnych zmien v konfigurácií VLAN sietí

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
  - Má vlastnú nezávislú VLAN databázu
  - Má vždy VTP číslo revízie 0
- Off
  - Ignoruje a nepreposiela VTP správy (len VTPv3 alebo CatOS)

VTP doména



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

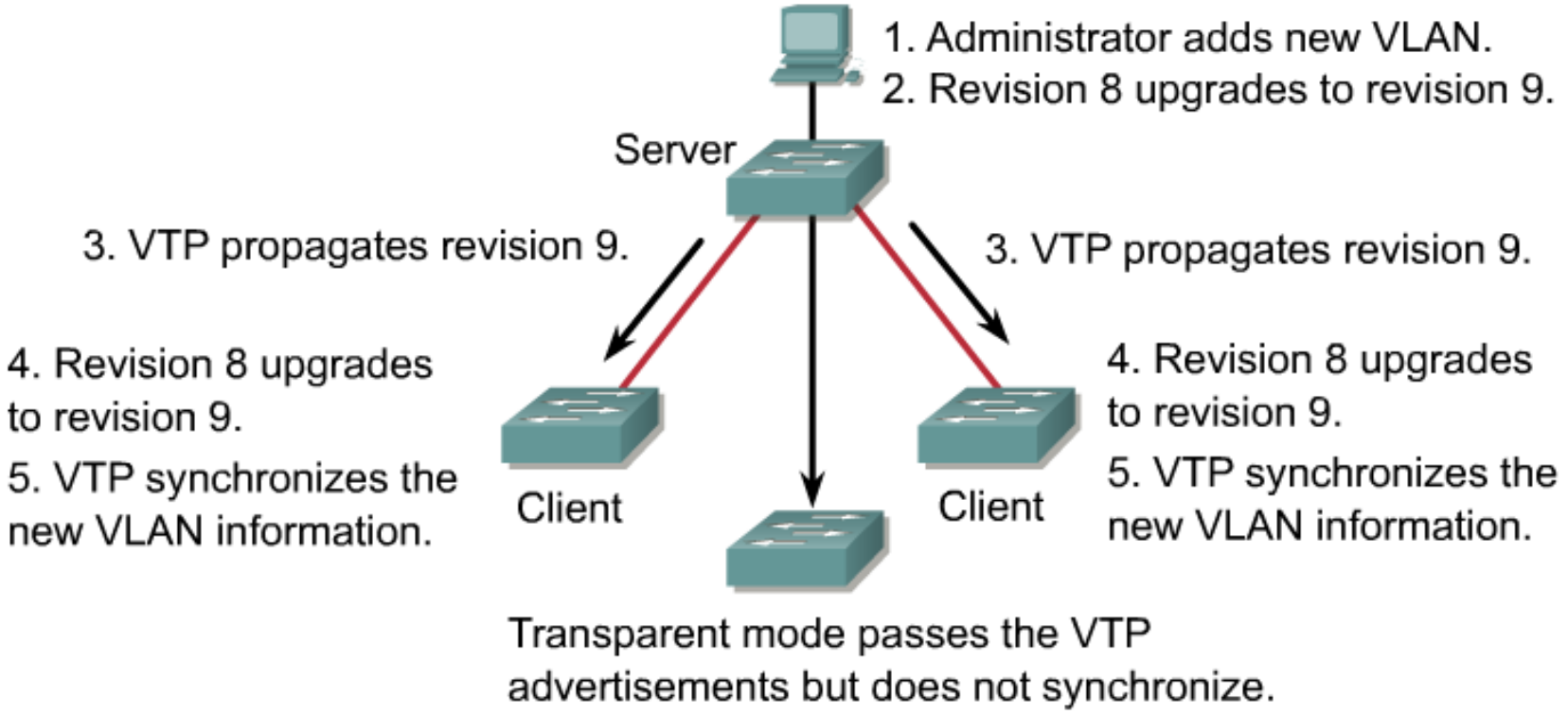
Propagovanie VTP informácií

- VTP používa dva druhy VTP správ (advertisements):
  - **Požiadavky** od VTP klientov, ktorí chcú info pri bootovaní
  - **Odpovede** (inzercia) od VTP serverov
- VTP používa tri typy VTP správ:
  - **Summary advertisements**
    - VTP *server* posiela sumárne VLAN info každých päť minút
      - Alebo keď bola zmena do VLAN databázy
    - *aj klient* zašle po zapnutí
      - Ako info čomu switch verí ohľadne VLAN
    - Obsahuje zoznam manažment domén, VTP verzií, doménové meno, konfiguračné revízne číslo, časovú značku,
      - Za ním nasledujú subset advertisements ak došlo k zmene vo VLAN DB
  - **Subset advertisements**
    - Následuje za Summary advertisements pri zmenách vo VLAN
    - Obsahuje detailné info o VLAN-ach, ktorým sa zmenil nejaký parameter
    - Jeden **Subset advertisements** per VLAN ID
  - **Advertisement requests**
    - Používa klient na vyžiadanie VLAN info ak je prijaté update s vyšším VTP číslom ako zapamätané alebo switch bol resetnutý, alebo zmenená doména
    - VTP server odpovedá so susbet advertisements

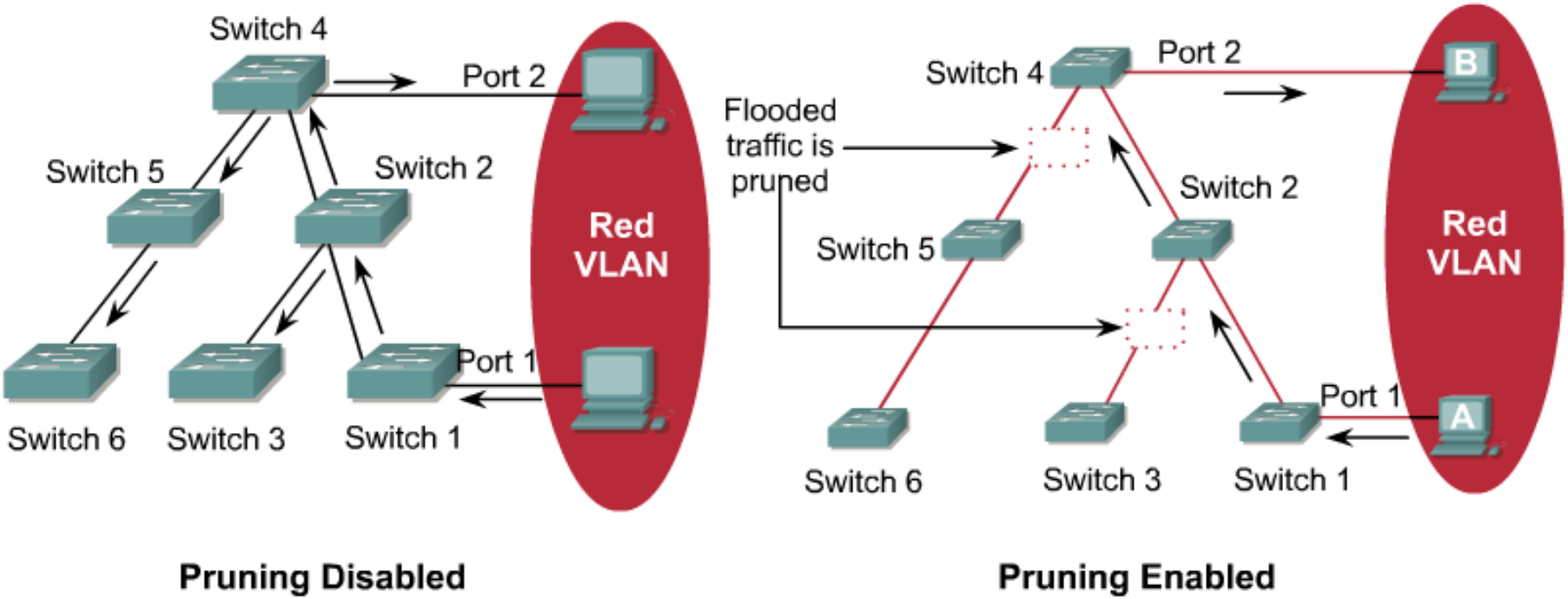
VTP správa

- VTP správa je:
  - Posielaná na Mcast adresu 01-00-0C-CC-CC-CC (All-VTP)
  - Enkapsulovaná do 802.1q formátu Ethernet LLC/SNAP rámca
- **Hlavička**
  - **Domain name –** Identifikuje VTP doménu prepínača.
  - **Domain name length** – Dĺžka doménového mena.
  - **Version** – Verzia VTP, buď VTP 1, VTP 2 or VTP 3. Cat2960 podporuje VTP 1 a VTP 2. 1 a 2 sú navzájom nekompatibilné.
  - **Configuration revision number** – Aktuálne číslo revízie updatu.
- **Telo**
  - Obsahuje fixné info:
    - VTP domain name
    - Identita prepínača posielajúceho správu, a časovú značku
    - MD5 otlačok konfiguračných parametrov VLAN
    - Formát rámca: ISL or 802.1Q
  - Info pre každú konfigurovanú VLAN:
    - VLAN IDs (IEEE 802.1Q)
    - VLAN name
    - VLAN type
    - VLAN state
    - Doplnkové informácie špecifické pre danú VLAN-u

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



- 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

Konfigurácia VTP

Základná konfigurácia VTP

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
```

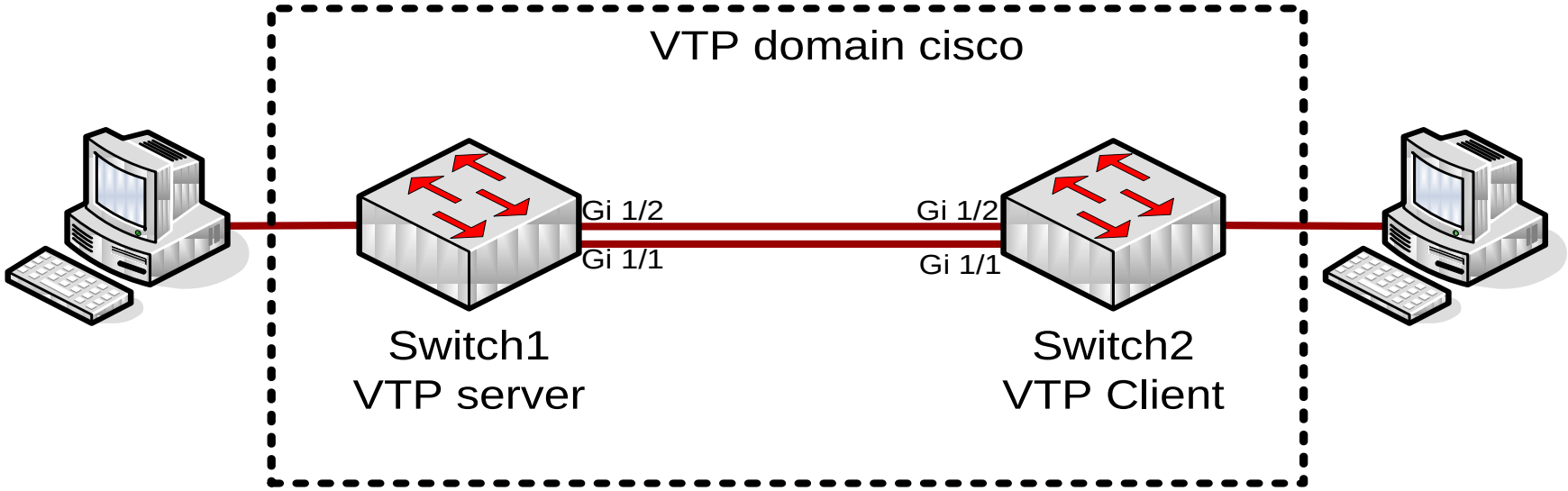
Overenie činnosti VTP

```
Switch#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                 : 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)
```

Overenie činnosti VTP

```
Switch#sh vtp counters
VTP statistics:
Summary advertisements received    : 1
Subset advertisements received     : 1
Request advertisements received    : 2
Summary advertisements transmitted : 5
Subset advertisements transmitted  : 5
Request advertisements transmitted : 0
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
---------------- ---------------- ---------------- ---------------------------
```

Príklad 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
...
```

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 aspoň jeden server?
- **Upozornenie**
  - **Vždy keď pridávaš nový prepínač do VTP domény, ubezpeč 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

Pár tipov

- VTP revízne číslo je uložené vo flash (vlan.dat)
  - Reštart 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
…
```

- 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
```