Stretnutie 2: Virtuálne LAN

SWITCH Modul 2

Virtuálne LAN (VLAN)

- VLAN sú samostatné, nezávislé broadcastové domény vytvárané iba logikou prepínača
- VLAN umožňujú virtualizovať fyzické prepínané LAN
  - 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.

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“

Statické členstvo portu vo VLAN

- Port môže byť do VLAN priradený buď staticky, alebo sa jeho členstvo môže priebežne meniť
- Statické členstvo vo VLAN nastavuje administrátor na porte manuálne
  - Priraďuje fyzický port prepínača do VLAN port po porte
  - Port sám nie je schopný zmeniť svoje členstvo vo VLAN
  - Každý port je členom nejakej VLAN (port nemôže zostať „visieť vo vzduchu“)
  - Známe aj ako port-based, port-centric
- Výhodou je absolútna kontrola a deterministický dizajn, nevýhodou je vyššia administratívna náročnosť

Dynamické členstvo portu vo VLAN

- Pri dynamickom členstve switch v istom momente určí, do akej VLAN má pripojené zariadenie patriť
- Kritériá môžu byť formálne rôzne
  - MAC adresa pripojeného zariadenia
  - IP adresa
  - Typ protokolu
  - Meno a heslo prihláseného používateľa
- Dynamické členstvo si vyžaduje istý riadiaci mechanizmus
  - VLAN Membership Policy Server (VMPS) – Cisco proprietárne
  - RADIUS spojený s 802.1X – otvorené riešenie

Interná práca switcha s VLAN

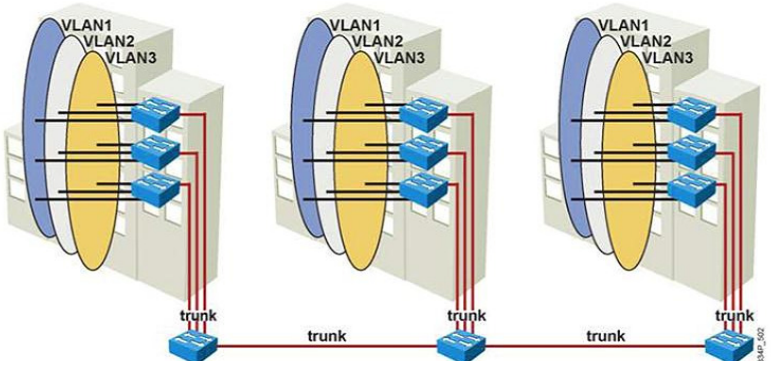
- Implementovanie podpory VLAN z pohľadu logiky switcha je relatívne jednoduché
  - MAC tabuľka sa rozšíri o stĺpec VLAN
  - Riadok MAC tabuľky bude teda obsahovať informácie v tvare <VLAN> | <MAC> | <Port>
- Rámec vchádzajúci portom bude spracovaný podľa tohto postupu:
  - Ak je jeho zdrojová MAC adresa 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

- Pôvodný koncept, ktorý odrážal pravidlo 80/20
  - 80% prevádzky zostáva vo VLAN, 20% odchádza do iných sietí
  - Tento koncept dnes už neplatí
- VLAN sa rozprestierajú po celej sieti naprieč Access, Distro a Core
- VLAN boli vytvárané pre isté pracovné skupiny (podľa funkcie)



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.

Rozdelenie rozsahov VLAN na Cisco prepínačoch

- **Normal Range VLANs**
  - VLAN ID je v rozsahu 1 – 1005
  - ID od 1002 do 1005 sú rezervované pre Token Ring a FDDI VLAN
  - VLAN ID 1 a 1002 – 1005 sú automaticky vytvorené a nemôžu byť zmazané
  - Konfigurácia VLAN je uložená v súbore vlan.dat vo Flash pamäti a môže byť aj súčasťou startup-config (a teda v „NVRAM“)
- **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

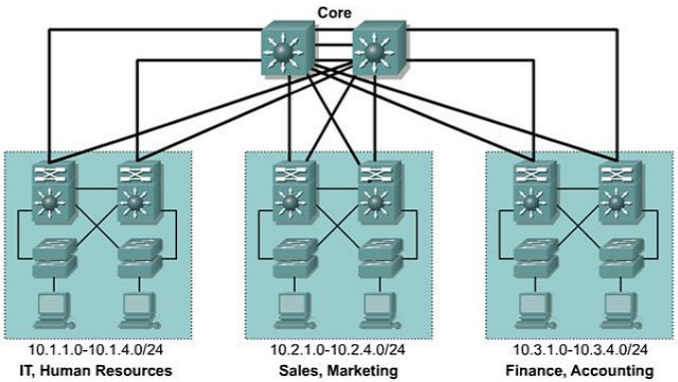
Podpora VLAN na prepínačoch Catalyst

Typ prepínača	Maximálny počet VLAN	Rozsah VLAN ID
2940	4	1 - 1005
2950/2955	250	1 - 4094
2960	255	1 - 4094
2970/3550/3560/3750	1055	1 - 4094
2848G/2980G/4000/4500	4094	1 - 4094
6500	4094	1 - 4094

Maximálny počet VLAN a rozsah ich ID môže závisieť od platformy aj od verzie IOSu

Odporúčania pri návrhu VLAN

VLAN dizajn – adresovanie



- IP adresový priestor alokovať v súvislých blokoch
- Jednej VLAN alokovať jednu IP sieť
- VLAN by nemala prekračovať distribučnú vrstvu

Ďalšie fakty na zváženie pri návrhu VLAN

- 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

Implementácia statických VLAN

Postup pri vytváraní VLAN

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

Vytvorenie VLAN – Globálny konfiguračný režim

```
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#
```

Preferovaný spôsob, možnosť vytvárať normal aj extended range VLAN

Vytvorenie VLAN – VLAN database režim

```
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 ...
```

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

- Prístupový port (access port)
  - Asociovaný len s jednou VLAN
  - Táto VLAN musí existovať vo VLAN databáze
  - Pripojené zariadenie je v spoločnej VLAN, a teda aj v spoločnej IP sieti, s ostatnými členmi tej istej VLAN
- Možnosti
  - Statické asociovanie konfiguračným príkazom
  - Dynamické asociovanie
    - Na základe MAC adresy alebo overenia pri prihlásení
    - Založené na VMPS alebo RADIUS + 802.1X protokoloch

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 portu prepínača do VLAN – makro „switchport host“

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# int fa 0/1
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
```

Vytvorenie access portu a asociovanie portu s VLAN

Priradenie rozsahu portov prepínača do VLAN a 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
...
```

Nepriame vytváranie 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
```

Zmazanie VLAN konfigurácie

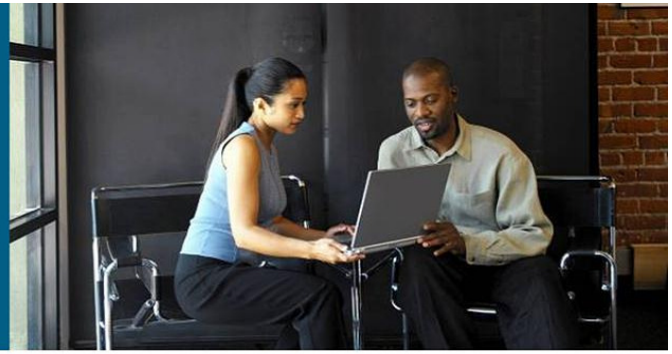
```
! Zmazanie vlan.dat (potrebný je reštart)
Switch# delete flash:vlan.dat

! Odstránenie VLAN 5
Switch(config)# no vlan 5

! VLAN database režim
Switch# vlan database
Switch(vlan)# no vlan 5
Switch(vlan)# exit

! Odstránenie portu z inej VLAN (port sa vráti do VLAN 1)
Switch(config)# interface fastethernet 0/5
Switch(config-if)# no switchport access vlan
```

Nepoužité porty do inactive VLAN

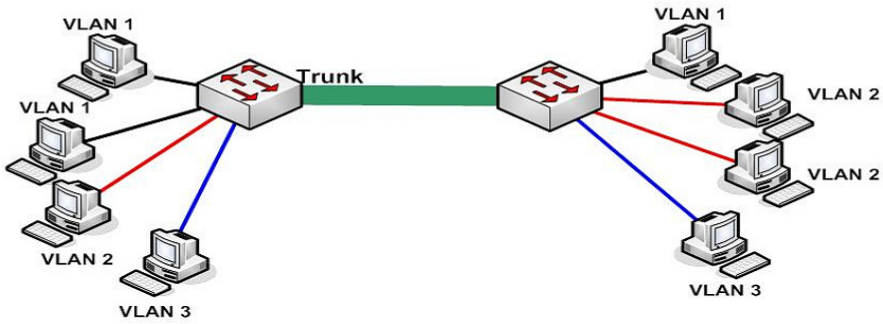
```
Switch(config)# vlan 99
Switch(config-vlan)# state suspend ! Globálne cez VTP
Switch(config-vlan)# shutdown ! Lokálne
```

- VLAN je možné administratívne deaktivovať
  - Deaktivovaná resp. pozastavená VLAN zostáva existovať, ale úplne sa pozastaví jej činnosť – prenos dát, STP, ...
  - Pozastaviť VLAN je možné lokálne alebo VTP-globálne
- Príkaz **`state suspend`** je propagovaný cez VTP, platí v celej VTP doméne a pozastaví VLAN globálne
- Príkaz **`shutdown`** pozastaví VLAN len na danom switchi
- Okrem zrejmých dôvodov, kedy je vhodné VLAN dočasne deaktivovať, je vhodné mať jednu deaktivovanú VLAN ako „parkovaciu“ VLAN pre nevyužité porty

VLAN Trunking



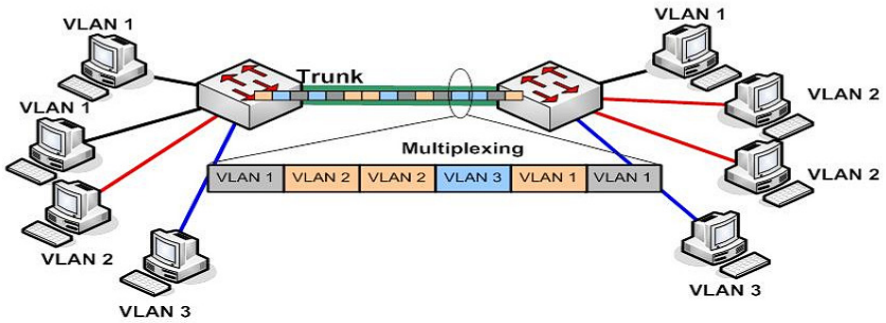
Intra VLAN komunikácia - Trunking



Trunk
Prepoj medzi prepínačmi, ktorý prenáša rámce mnohých VLAN

Rámce sa **multiplexujú** cez trunk

Intra VLAN komunikácia - Trunking



Trunk
Prepoj medzi prepínačmi, ktorý prenáša rámce mnohých VLAN

Rámce sa **multiplexujú** cez trunk

Ako rozlíšiť, do ktorej VLAN patria jednotlivé rámce?

Rozlíšenie značkovaním rámcov podľa VLAN

Tzv. TAGGING

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

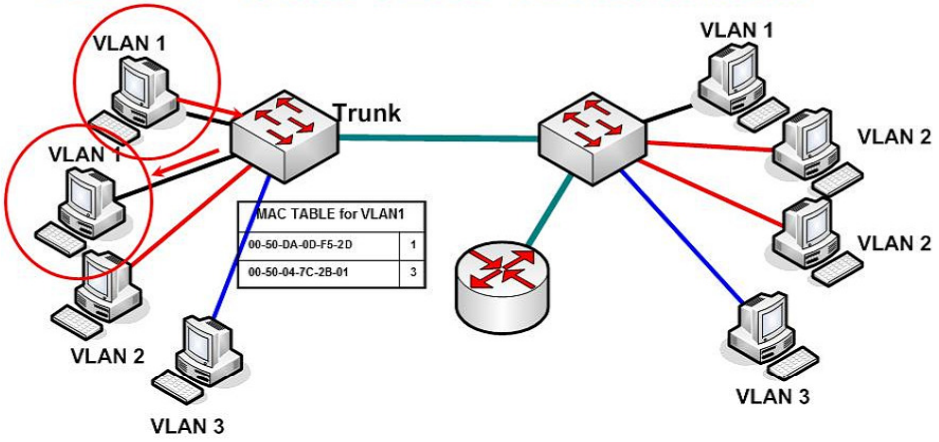
IEEE 802.1Q

- 802.1Q je otvorený IEEE štandard pre trunk prepoje
  - Zabezpečená interoperabilita zariadení rôznych výrobcov
- 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 tom istom prepínači	Prepínač príjme rámec na vstupnom porte (**Access port**) Prezrie MAC table pre VLAN 1 Prepne rámec na výstupný port	**Rámec nie je pozmenený (značkovaný), lebo nevstupuje na trunk port!** Rámec je prepnutý ako na bežnom prepínači

Natívna VLAN (1)

- 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

```
Switch(config)# vlan dot1q tag native
```

Konfigurácia trunkov

Konfigurácia trunk prepojov

- Manuálne (staticky)

```
Switch(config-if)# switchport trunk encapsulation { dot1q | isl }
Switch(config-if)# switchport mode trunk
```

- Dynamicky – cez Dynamic Trunking Protocol (DTP)
  - Dynamicky dohodnuté vytvorenie trunku
  - Podpora ISL aj 802.1Q

```
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 encapsulation { isl | dot1q }

! Konfigurácia trunku
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate ! Deaktivuje DTP - odporúča sa
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         n-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#
```

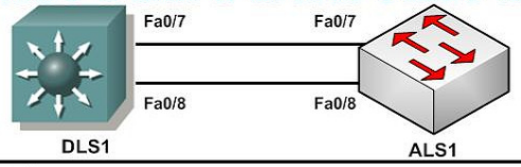
Overenie konfigurácie trunku

```
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 aj na statickom trunk porte, aby druhá strana vedela, že realizujeme trunking

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
```

Dynamic Trunking Protocol

DTP – Dynamic Trunking Protocol

- Cisco proprietárny protokol (U.S. Patent 6445715)
- Umožňuje automatické dohodnutie 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)

Režimy DTP

- Dynamic Auto
  - Predvolený na 2960, 3560
  - Port oznamuje druhej strane, že je schopný byť trunkom, ale nevyžaduje trunking

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

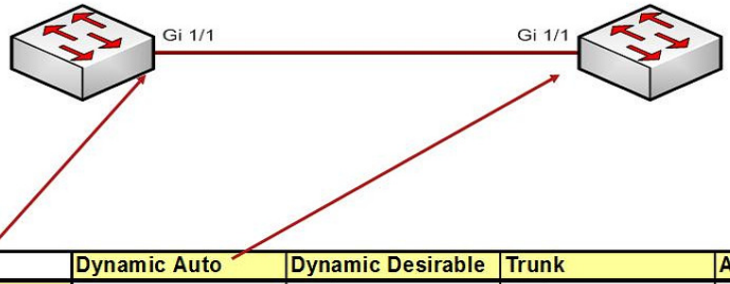
- Dynamic Desirable
  - Predvolený na 2950, 3550
  - Port oznamuje druhej strane, že je schopný byť trunkom a vyžaduje trunking

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

- 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
- Nonegotiate
  - Vypnutie DTP na porte prepínača
  - Žiadne DTP rámce nebudú posielané
  - Má zmysel iba pre porty v režime static trunk

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

Kombinácie DTP režimov



	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, ale rozhodne by nemalo zostať aktívne
  - Porty staticky nastaviť ako trunk/access
  - DTP deaktivovať pomocou **`switchport nonegotiate`**

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
```

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 dyn 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
```

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

Typické chyby pri VLAN a trunkoch

- Nesúhlasia 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
  - Na jednej strane `switchport access`, na druhej `switchport trunk`
  - Na jednej strane `switchport access`, na druhej DTP `auto` / `desirable`
  - Na jednej strane DTP režim, na druhej strane trunk a DTP deaktivované
  - Prepínače nie sú v tej istej VTP doméne
  - Rozdielna enkapsulácia na koncoch trunku
- Nesprávne nastavenie L3 adresovania nad VLAN
  - Strata IP konektivity alebo neštandardné správanie
- Nesprávne nastavený zoznam povolených VLAN nad trunkom
  - Chýba povolenie VLAN, ktorá si to vyžaduje
  - Strata konektivity a/alebo neštandardné správanie

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

VLAN Trunking Protocol

VLAN Trunking Protocol (VTP)

- Cisco proprietárny protokol pre uľahčenie práce s VLAN
  - Hromadná správa databázy VLAN sietí na všetkých switchoch
- VTP správy sa prenášajú výlučne cez trunk porty
- 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 prenáša info o všetkých VLAN
- Cisco Document ID: 10558, „Understanding VLAN Trunk Protocol (VTP)“
- Cisco dokument „VTP Version 3“

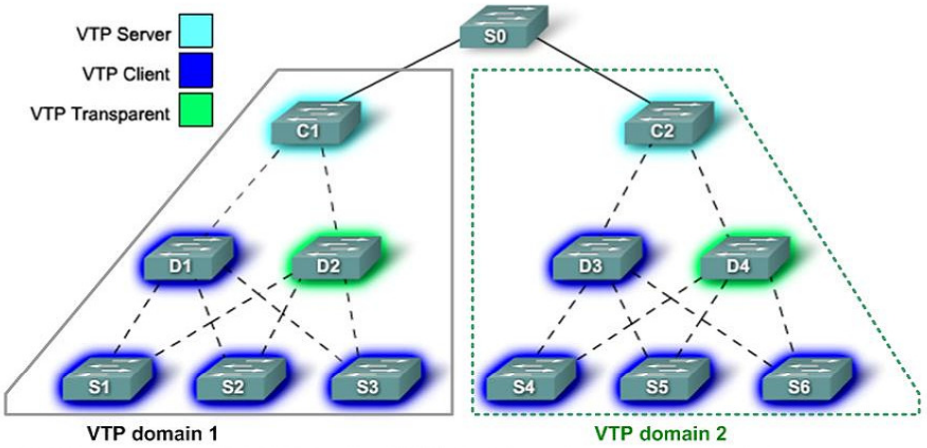
Rozdiely medzi VTP verziami

- 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, Private VLANs
  - Zlepšená autentifikácia
  - Ochrana proti neželanému prepísaniu domény (tzv. primárny server)
  - Možnosť deaktivovať VTP na vybranom porte
  - VTPv3 je zovšeobecnený protokol na distribúciu obsahu ľubovoľnej databázy. Ako jedna z aplikácií je synchronizácia MSTP konfigurácie

VTP režimy

- 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



- Zoskupenie prepínačov, ktoré budú zdieľať VLAN databázu
- Identifikovaná spoločným menom
- Prepínač môže byť len v jednej doméne

VTP správy

- VTP používa štyri typy VTP správ
- Summary advertisement
  - Súhrnné informácie o VLAN databáze generované každých 5 minút alebo hneď po modifikácii VLAN databázy
  - Obsahuje VTP verziu, doménové meno, číslo revízie, časovú značku, počet nasledujúcich subset advertisement správ
- Subset advertisement
  - Nasleduje za Summary advertisements pri zmenách vo VLAN
  - Prenášajú postupne obsah celej VLAN databázy
- Advertisement requests
  - Vyžiadanie VLAN databázy, ak je prijatý Summary Adv. s vyšším číslom revízie, po reštarte prepínača alebo zmene VTP domény
  - Odpoveďou je summary a subset advertisement
- VTP Join správy
  - Využívané pri VTP Pruningu

VTP konfiguračné príkazy

```
Switch(config)# vtp domain MENO_DOMENY
Switch(config)# vtp mode { client | server | transparent }
Switch(config)# vtp password HESLO [ hidden ] ! Hidden len v3

! Default je VTP v2 capable, ale v móde VTP v1
Switch(config)# vtp version { 1 | 2 | 3 }

! Stačí 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)
```

Ak sa objaví iný VTP server s doménou, čistý switch sa jej prispôsobí.

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
---------------- ---------------- ---------------- ---------------------------
```

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#
```

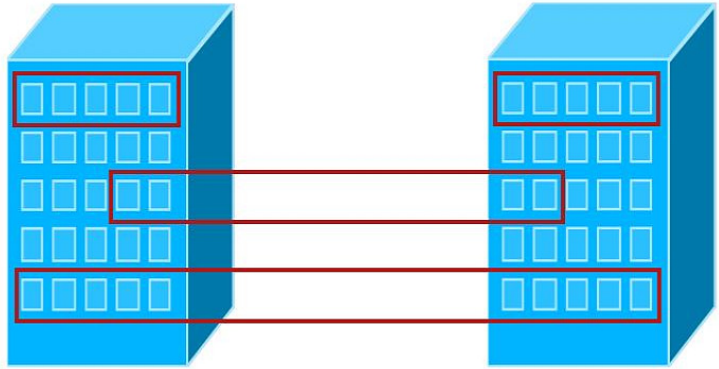
Časté chyby pri konfigurácii VTP

- Chyby:
  - Nefunkčné trunk prepoje
  - Nekompatibilné verzie VTP
  - Nesúhlasí VTP meno domény
  - Nesúhlasí VTP heslo domény
  - Chýba VTP server
- Skontrolovať:
  - VTP doménové meno
  - VTP doménové heslo
  - VTP verziu
  - Trunk prepoje
  - VTP režimy
  - Prítomnosť VTP servera
- Pred pridaním nového switcha do VTP domény sa VŽDY uistiť, že jeho revízne číslo je nižšie ako aktuálne používané
  - Inak tento switch prepíše VTP doménu vlastnou databázou
  - VTP revízne číslo sa nuluje pri zmene mena domény alebo pri prechode do transparentného režimu – využiť na vynulovanie
  - VTP revízne číslo sa nevynuluje obyčajným reštartom, lebo sa nachádza vo vlan.dat

Privátne VLAN

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 (RFC 5517) 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

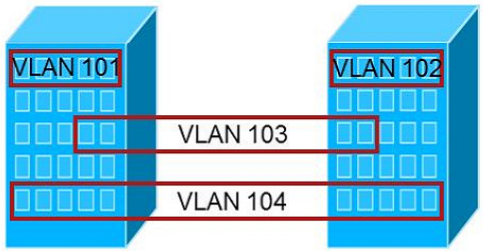
Privátne VLAN

- 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

Konfigurácia privátnych VLAN

```
vtp transparent ! Iba pri VTPv1/2
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
- 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 (vtedy môžu byť vhodné izolované PVLAN trunk porty na distribučných prepínačoch)
  - Chránené porty sa niekedy volajú Private VLAN Edge

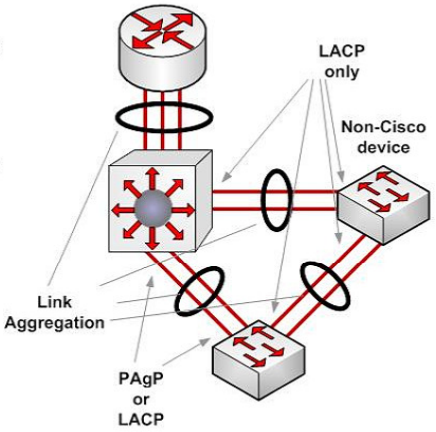
EtherChannel

Link Aggregation cez EtherChannel

- Technológia umožňujúca logicky združiť fyzické porty do niekoľkonásobne výkonnejšieho prenosového kanála
- Viaceré výhody
  - Poskytuje väčšiu priepustnosť
  - Znižuje pravdepodobnosť oneskorenia alebo zahltenia
  - Ponúka viaceré metódy pre rozkladanie záťaže
    - MAC, IP, IP+TCP/UDP
  - Zjednodušuje konfiguráciu
    - Konfiguruje sa len logický port, fyzické porty zdedia konfiguráciu
  - Prináša ďalšiu formu redundancie
    - Ak zlyhá jedna fyzická linka, EtherChannel stále pracuje
  - 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, U.S. Patent 6163543
- LACP (Link Aggregation Protocol):
  - IEEE štandard 802.3ad
- Oba protokoly sú rovnocenné



EtherChannel PAgP a LACP módy

PAgP	LACP
Auto: Pasívny stav, port odpovedá na výzvy o vytvorenie EtherChannel kanála, ale neinicializuje jeho vytvorenie sám.	**Passive:** To isté, čo PAgP Auto
Desirable: Aktívny stav, kedy port cielene žiada o zostavenie EtherChannel kanála.	**Active:** To isté, čo PAgP Desirable
On: Tento mód vynúti prechod portu do EtherChannel kanála bez PAgP alebo LACP.	**On:** To isté, čo PAgP On

Konfigurácia EtherChannel

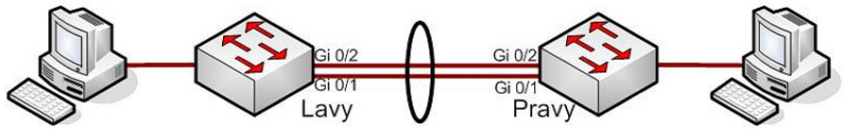
- Vytvorenie EtherChannel kanála
  - Nastavenie protokolu (iba kvôli blbuvzdornosti)

    `channel-protocol { pagp | lacp }`
  - Priradenie fyzických portov do kanála s daným číslom a v danom móde

    `channel-group GROUP_NUMBER mode { MODE }`
  - Konfigurácia logického EtherChannelu

    `interface port-channel GROUP_NUMBER`

Príklad konfigurácie – PAgP L2 etherchannel



- Vytvorenie PAgP EC a jeho konfigurácia ako trunk

```
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
```

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: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------
    -------------------------------
1      Po1(SU)         PAgP      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)         PAgP      Gi0/1(I)
    Gi0/2(I)

Pravy#
```

SU
S - Switched
U - Up

SD
S - Switched
D - Down

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#
```

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
```

Upozornenia ku konfigurácii EC

- Ak sa konfiguruje EC v režime **on**, je zásadne potrebné všetky združované porty na oboch switchoch **vypnúť** ešte pred ich zaradením do EC
  - Inak hrozí vznik prepínacích slučiek!!!
  - Z tohto istého dôvodu sa porty automaticky vypnú pri zrušení EC
  - Kedykoľvek je to možné, treba sa režimu **on** vyhnúť
- Pri zmene režimu existujúceho EC je vhodné nielen odstrániť príkazy **channel-group**, ale aj samotné rozhranie Port-channel
  - Odstránenie rozhrania Port-channel priamo zruší aj konfiguráciu z členských fyzických rozhraní
- Kvôli kompatibilite je vo všeobecnosti lepšie používať LACP namiesto PAgP
  - Výnimku tvorí tzv. Virtual Switching System (VSS)

Konfigurácia load-balancing mechanizmu pre EC

- Load-balancing môže vychádzať z týchto údajov:
  - **src-mac**: Zdrojová MAC
  - **dst-mac**: Cieľová MAC
  - **src-dst-mac**: Zdrojová XOR cieľová MAC
  - **src-ip:** Zdrojová IP
  - **dst-ip:** Cieľová IP
  - **src-dst-ip:** Zdrojová XOR cieľová IP
  - **src-port:** Zdrojový TCP/UDP port
  - **dst-port:** Cieľový TCP/UDP port
  - **src-dst-port:** Zdrojový XOR cieľový TCP/UDP port

```
! Load Balance sa konfiguruje pre celý prepínač
Switch(config)# port-channel load-balance TYPE
Switch(config)# exit
….
Switch# show etherchannel load-balance
```

Poznámky k load-balancingu na EC

- Rovnomerné rozdelenie prevádzky sa dá dosiahnuť, ak EC má 2, 4 alebo 8 portov
  - Iný počet portov vedie k nerovnomerným pomerom rozdelenia
  - Nie je však pravdou, že v EC môže byť iba 2, 4 alebo 8 portov (EC môže obsahovať ľubovoľný počet portov od 1 do 8)
- Document ID: 12023, „Understanding EtherChannel Load Balancing and Redundancy on Catalyst Switches“


CISCO