MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Opakovanie - switching

PS2 – prednáška 1

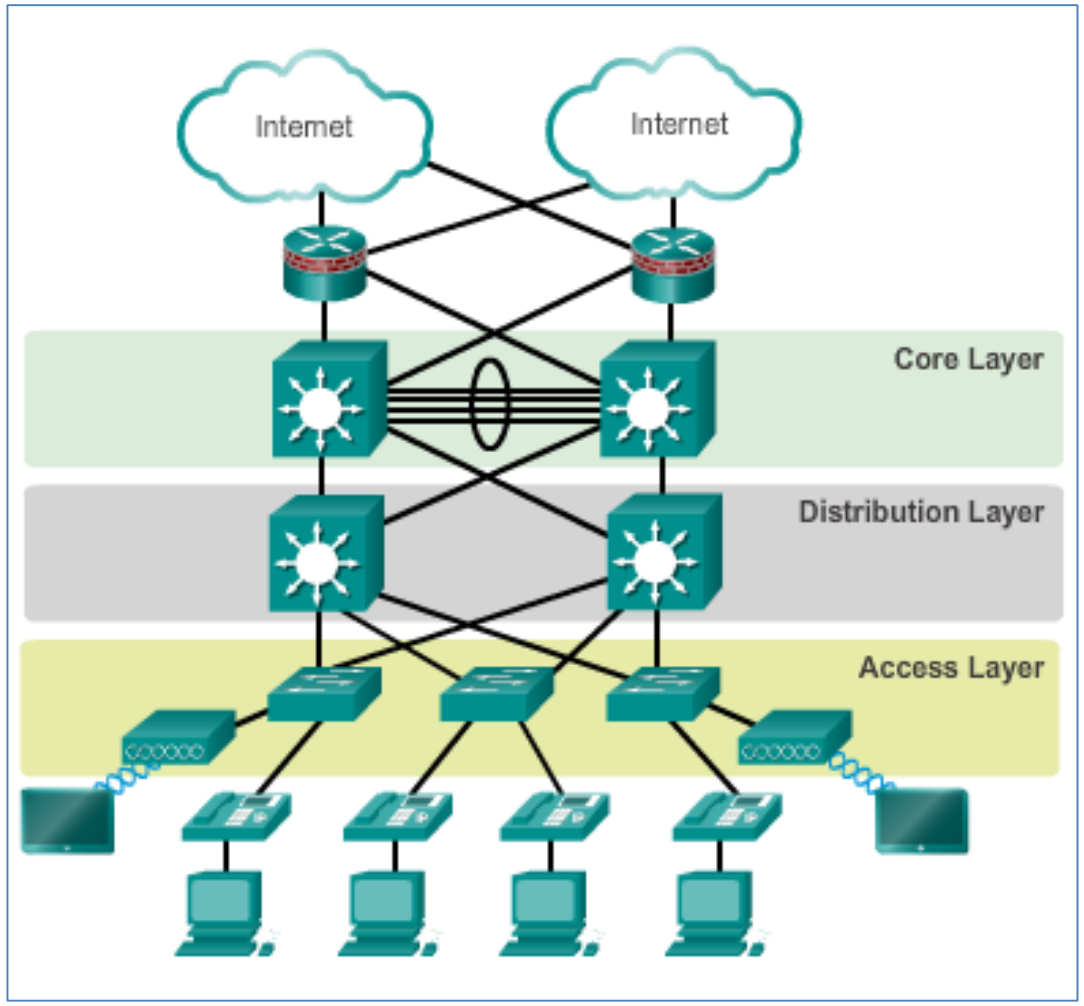
Katedra informačných sietí
FRI, UNIZA

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

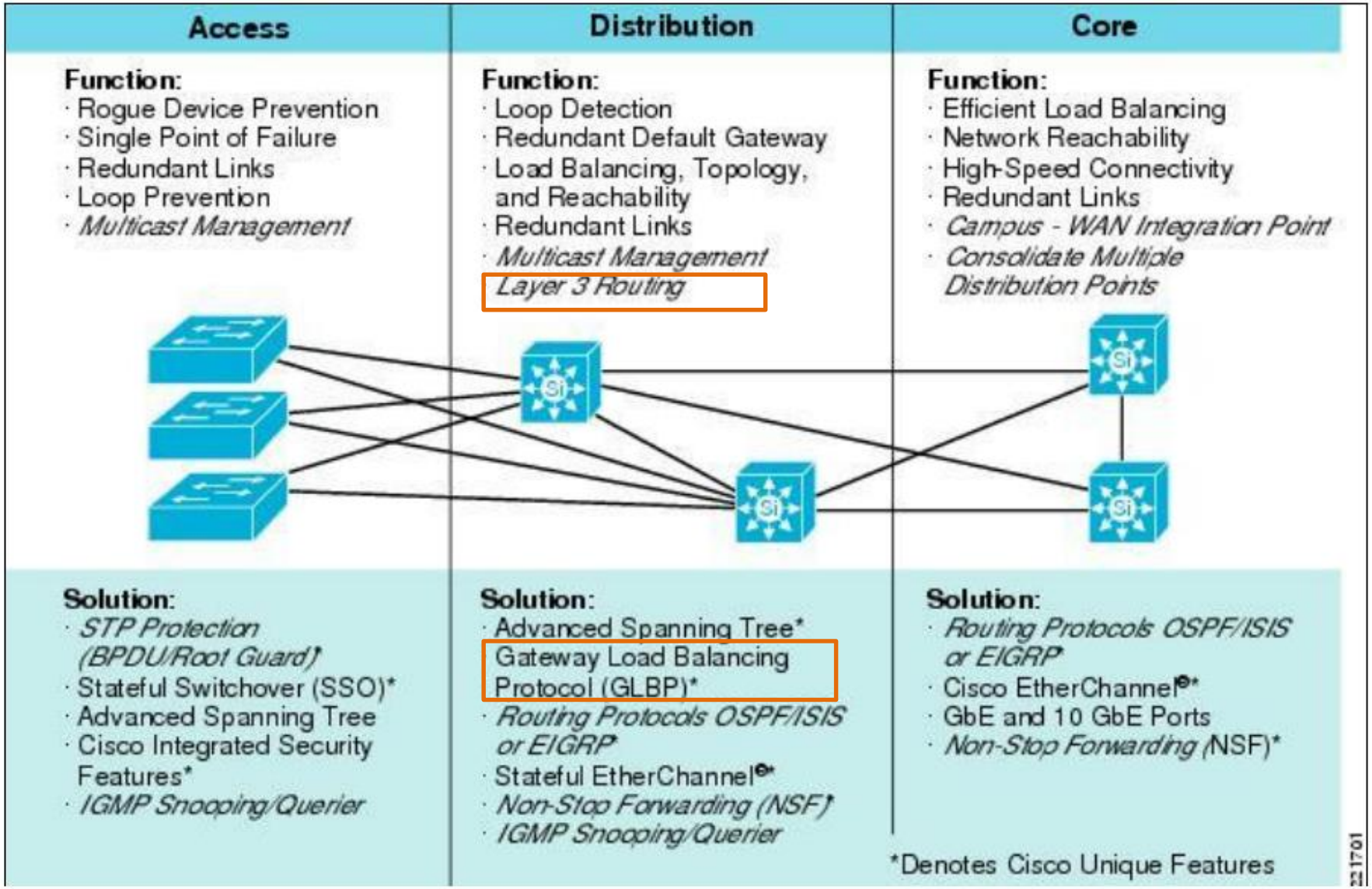
Hierachický model, funkcia prepínača, port-security,

Hierarchický model siete

- Rozdeľuje sieť podľa funkcionality do troch vrstiev
- **Access**
  - Poskytuje prostriedky na prístup do siete
  - Riadi kto môže komunikovať cez sieť **port-security**
  - Definuje bezpečnostnú hranicu
  - Rieši prevenciu proti slučkám **Rapid-PVST**
- **Distribution**
  - Agreguje dáta z prístupovej vrstvy
  - Optimalizuje smerovanie medzi nimi **interVLAN rout.**
  - Riadi tok dát (smerovacie a ACL politiky)
  - Musí byť vysokorýchlostná a redundantná **FHRP**
- **Core**
  - Tvorí **vysokorýchlostnú** chrbticu siete
  - Musí zvládať spracovávať veľké objemy dát a veľmi rýchlo
  - Agreguje dáta od distribučných prepínačov
  - Musí byť **vysokodostupná** a **redundantná**
  - Musí umožňovať load-balancing pre nás zatiaľ **RIP**



Hierarchický model siete (2)

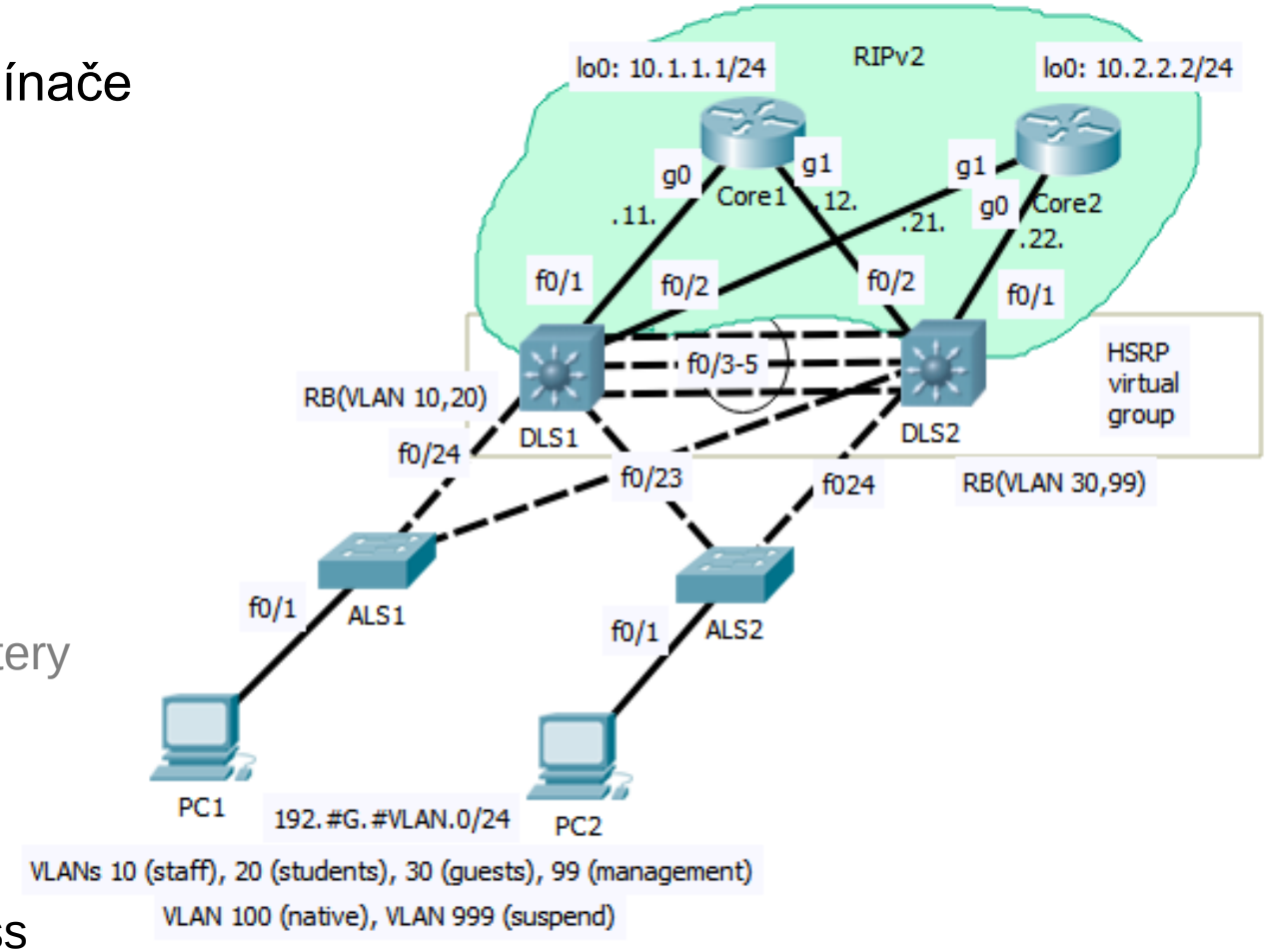


Vlastnosti dobre navrhnutej siete

- **Škálovateľnosť (Scalability)**
  - Ľahká a bezproblémová rozšíriteľnosť siete pri jej raste
- **Redundancia (Redundancy)**
  - Zabezpečenie vysokej dostupnosti (availibilty) a spoľahlivosti prenosovej cesty
- **Výkonnosť (Performance)**
  - Zohľadnenia prenosových nárokov používateľov a aplikácií
    - „Nech každý dostane to čo potrebuje“
  - Agregácia liniek a vysoko rýchlostné spracovávanie a prepínanie dát
- **Bezpečnosť (Security)**
  - Zabezpečenie siete na rôznych úrovniach
    - Bezpečnosť portov, prístupové pravidlá a pod.
- **Manažovateľnosť (Manageability)**
  - Zjednodušený manažment siete pri jasne definovaných pravidlách, dodržanie konzistentnosti konfiguračných politík naprieč sieťou
- **Udržovateľnosť (Maintainability)**
  - Modulárne siete s jasne definovanou funkcionalitou sa ľahko udržujú

Prepínače pre jednotlivé vrstvy

- Na prístupovú vrstvu Cisco odporúča prepínače
  - Catalyst 2960 (L2 prepínač)
  - Catalyst 3560, 3750 (L3 prepínače)
  - Malé/stredné: 2960-X, Veľké: 3850-X
- Na distribučnú vrstvu sa hodia prepínače
  - Catalyst 3560, 3750, 4500 (L3 prepínače)
  - Malé/stredné: 3850-X, Veľké:4500-X
- Na chrbticu sa odporúčajú prepínače
  - Catalyst 4500, 6500, prípadne high-end routery
  - Malé/stredné/veľké: 6800
- Špeciálne pre dátové centrá má Cisco osobitný rad prepínačov
  - Nexus 200, 3000, 5000 – Data center Access
  - Nexus 5000, 7000

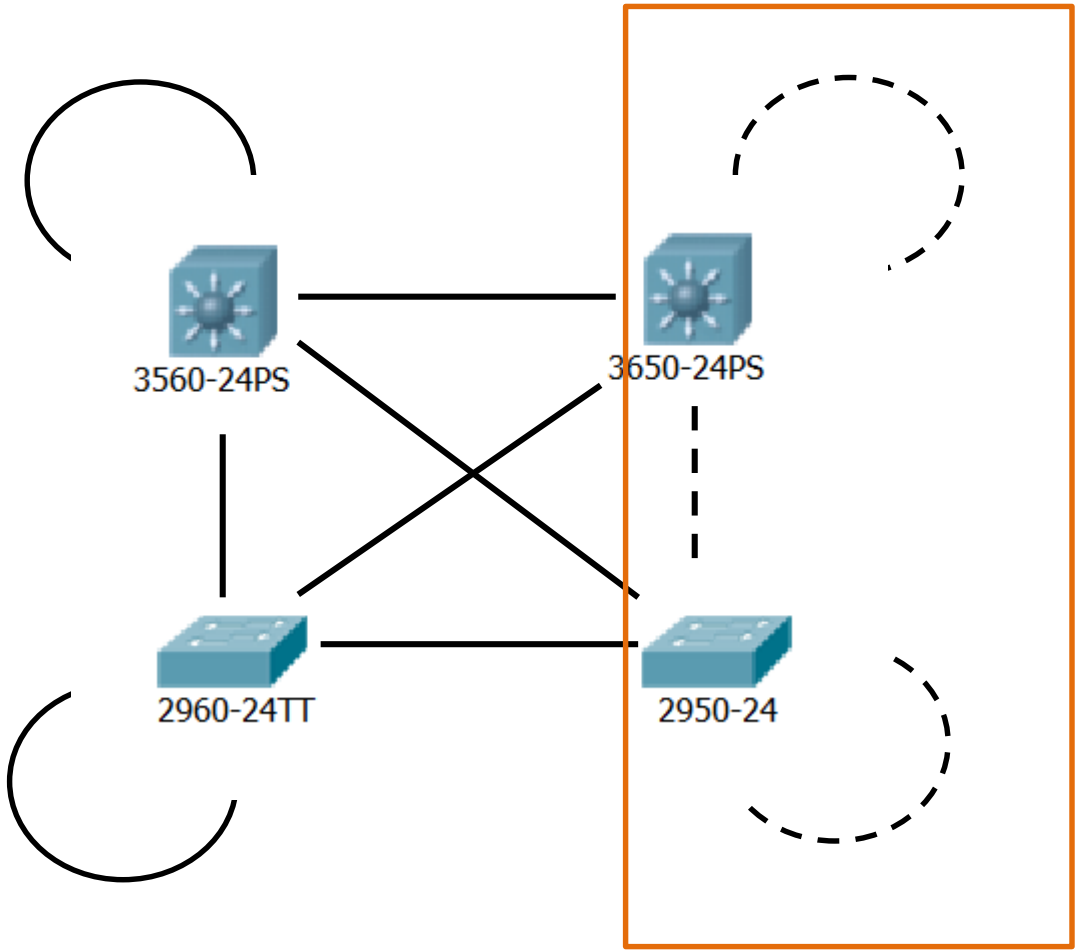


Funkcia auto-MDIX

- Príslušné typy káblov (priamy/krížený) bolo v minulosti potrebné dodržiavať pri pripojení k zariadeniam.
- Dnes ale tento problém rieši **auto-MDIX**
  - *automatic medium-dependent interface crossover*.
- Keď je povolená (na rozhraní), automaticky deteguje požadovaný typ káblového prepojenia a vhodne ho nakonfiguruje.
- Ak ju používam, rýchlosť aj duplex musia byť nastavené na automatické vyjednanie ba oboch stranách:
  - T.j. **auto** (autonegotiate)
- Overenie:

```
switch# show controllers ethernet-controller gigabitEthernet 0/1 phy | include Auto-MDXI
```

Kedy sa nespoliehať na mdix-auto?



Základná konfigurácia portov prepínača

```
Switch(config)# interface gig 3/1
Switch(config-if)# description Printer in Bldg A, room 213
! Switch(config-if)# speed {10 | 100 | 1000 | auto}
Switch(config-if)# speed auto
! Switch(config-if)# duplex {auto | full | half}
Switch(config-if)# duplex auto
```

- Ak je aspoň jeden z týchto parametrov ponechaný na auto, na porte zostáva bežať autonegociácia
  - V „capabilities“, ktoré port ohlasuje, sú len tie alternatívy, ktoré zahŕňajú fixne nastavený parameter
- Ak sú oba parametre nastavené fixne, autonegociácia sa na viacerých typoch Catalyst switchov vypína
  - Dôsledkom je, že ak sa druhá strana spolieha na autonegociáciu, rýchlosť odhadne z kanálového kódovania a duplex nastaví na half (fallback hodnota)
  - Možnosť veľmi nepríjemných problémov kvôli nezhode duplexu
  - Je rozdiel „vypnutá autonegociácia“ a „autonegociácia, ktorá uvádza iba jedinú alternatívu“
  - Ak je vypnutá autonegociácia, nefunguje ani auto-MDIX
  - Praktická skúsenosť: 3560V2 nevypínajú autonegotiation, iné modely switchov (2960) áno – poučenie: ak je potrebné nastaviť rýchlosť a duplex fixne, najlepšie je to urobiť na oboch koncoch linky súčasne

Show interfaces status

```
switch# show interface status

Port      Name               Status       Vlan       Duplex     Speed  Type
Fa0/1                        connected    1          a-full     a-100  10/100BaseTX
Fa0/2                        connected    1          a-full     a-100  10/100BaseTX
Fa0/3                        connected    1          a-full     a-100  10/100BaseTX
Fa0/4                        notconnect   1          auto       auto   10/100BaseTX
Fa0/5                        notconnect   1          auto       auto   10/100BaseTX
Fa0/6                        notconnect   1          auto       auto   10/100BaseTX
Fa0/7                        notconnect   1          auto       auto   10/100BaseTX
Fa0/8                        connected    1          a-full     a-100  10/100BaseTX
Fa0/9                        notconnect   1          auto       auto   10/100BaseTX
Fa0/10                       notconnect   1          auto       auto   10/100BaseTX
```

Overenie stavu prepínača

show interface TYP X/Y

```
Sw-FRI-3560-A213#sh interfaces gigabitEthernet 0/3
GigabitEthernet0/3 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 001b.8f8f.de03 (bia
001b.8f8f.de03)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 4000 bits/sec, 6 packets/sec
     2830675 packets input, 185209120 bytes, 0 no buffer
     Received 4199 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     15980351 packets output, 1277847091 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

Pripojenie staro-nového prepínača do živej siete

Nový = ešte tam nebol
Staro = má nezmazanú konfiguráciu

Osvedčený postup:

1. nezapájať káble, iba konzolu
2. startup-config – ak neprázdny, zmaž
   - show start
   - erase startup
3. vlan.dat – ak existuje, zmaž
   - show vlan (alebo) show flash
   - delete vlan.dat
4. reload – iba ak bolo treba niečo mazať
5. nastaviť prepínač do VTP transparent módu
6. káblovanie

```
Switch# show startup-config
 .... MAZ-LEN-AK-TU-NIECO-JE ....
Switch# erase startup-config
Erasing the nvram filesystem will remove all
configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
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)
! .... MAZ-LEN-AK-TU-NIECO-JE .... :
Switch# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch# reload
Switch(config)# vtp mode transparent
```

Prepínač už zapojený v živej sieti

- Ako vrátiť rozhranie do východzieho stavu?

```
Switch (config)# default interface NAZOV X/Y
```

- Čo keď zmazané VLAN (vlan.dat) sa nám neustále nanovo objavujú na prepínači (znovu naučením)?

```
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)# no vlan ID_VLANY
Switch(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```

Funkcie port security

- Funkcia Port Security umožňuje na porte
  - Obmedziť počet zariadení, ktoré môžu byť pripojené k jednému rozhraniu prepínača
    - Definovaním maxima MAC adries vyskytujúcich sa na porte
  - Definovať zoznam bezpečných MAC adries staníc, ktoré smú byť pripojené k danému rozhraniu prepínača
    - Uviesť kto je bezpečný
    - Alebo nechať rozhodnúť prepínač
  - Definovať, čo sa stane, ak dôjde k porušeniu niektorého z týchto bezpečnostných pravidiel
    - Tzv. violation
    - Stanica, ktorej MAC nie je v zozname bude „*nejako*“ obmedzená

Port Security

Ktoré a koľko adries je bezpečných?

- Bezpečné adresy môžu byť troch druhov:
  - **Static secure MAC**: manuálne nakonfigurovaná adresa
    - Nachádza sa v konfigurácii aj v CAM tabuľke
    - Po reštarte prepínača sa opätovne načíta z uloženej konfigurácie
  - **Dynamic secure MAC (dynamic learning)**: dynamicky získaná adresa z CAM
    - Nachádza sa len v CAM tabuľke
    - Po odpojení portu alebo reštarte prepínača sa stráca
  - **Sticky secure MAC (sticky learning)**: hybrid medzi statickou a dynamickou adresou
    - Získava sa dynamicky, no prepínač automaticky vygeneruje záznam do bežiacej konfigurácie
    - Nachádza sa v konfigurácii aj v CAM tabuľke
    - Po reštarte prepínača sa opätovne načíta z uloženej konfigurácie
- Zároveň je na porte možné definovať maximálny počet bezpečných adries
  - Statické adresy sa započítavajú do počtu bezpečných adries
  - Prepínač automaticky pridá každú novú neznámu MAC adresu do zoznamu bezpečných adries ako *dynamickú* resp. *sticky*
  - Ak by sa však pridaním novej adresy prekročil maximálny počet bezpečných adries, nastáva tzv. porušenie bezpečnosti (security violation)

Reakcia na porušenie - Violation Modes

- Na bezpečnostné porušenie možno zareagovať trojakým spôsobom
  - **Protect**: rámec s nepovolenou MAC adresou sa zahodí
  - **Restrict**: rámec s nepovolenou MAC adresou sa zahodí a zároveň sa incident zaznamená (hláška na konzolu, syslog, SNMP trap...)
  - **Shutdown**: port sa pri prijatí rámca s nepovolenou MAC adresou automaticky uvedie do stavu err-disabled

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

Konfigurácia

- Port Security sa konfiguruje individuálne na prepínaných portoch
- Odporúčaný postup:
  - Port nastaviť do režimu „access“ alebo „trunk“
    - Nevyhnutné – Port Security nie je podporovaná na dynamických portoch
  - Nastaviť maximálny povolený počet MAC adries
    - Nepovinné, predvolený počet je 1
  - Definovať statické bezpečné adresy, prípadne sticky learning
    - Nepovinné, default je dynamic learning
  - Určiť reakciu pri porušení bezpečnosti
    - Nepovinné, predvolená reakcia je shutdown
  - Určiť spôsob expirácie bezpečných adries
    - Nepovinné. Bez dodatočného nastavenia statické a sticky adresy neexpirujú vôbec, dynamické expirujú až pri odpojení portu
  - Aktivovať port security
    - Nevyhnutné a často prehliadnuté! (`switchport port-security`)

Konfigurácia a kontrola Port Security

```
Sw(config)# interface fa0/2
Sw(config-if)# switchport mode access
Sw(config-if)# switchport port-security maximum 5
Sw(config-if)# switchport port-security mac-address 001c.2320.3a28
Sw(config-if)# switchport port-security violation restrict
Sw(config-if)# switchport port-security aging time 10
Sw(config-if)# switchport port-security
```

```
Sw# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/2              5            3                  0         Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 8192
```

Konfigurácia a kontrola Port Security

```
Sw# show port-security address
           Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    01c.2320.3a28     SecureConfigured              Fa0/2         -
   1    00e0.4c3b.b787    SecureDynamic                 Fa0/2         8
   1    0200.0000.0001    SecureDynamic                 Fa0/2         8
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 8192
```

Konfigurácia a kontrola Port Security

```
Sw# show port-security interface fa0/2
Port Security                   : Enabled
Port Status                     : Secure-up
Violation Mode                  : Restrict
Aging Time                      : 10 mins
Aging Type                      : Absolute
SecureStatic Address Aging      : Disabled
Maximum MAC Addresses           : 5
Total MAC Addresses             : 3
Configured MAC Addresses        : 1
Sticky MAC Addresses            : 0
Last Source Address:Vlan        : 00e0.4c3b.b787:1
Security Violation Count        : 0
```

Porty v stave „Error Disabled“

- Vtedy keď je na porte nastavená akcia pri narušení na shutdown a narušenie nastane
- Port je vtedy v skutočnosti shutdown-utý
- Prepínač túto zmenu oznámi cez konzolové správy:

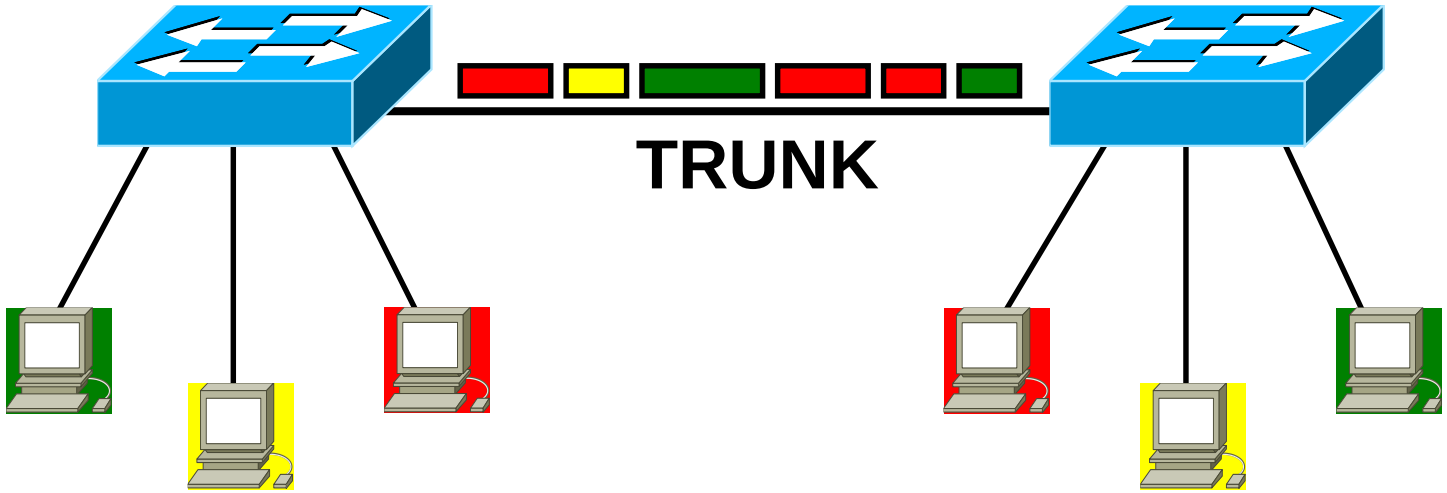
```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

VLANs, trunks, DTP, VTP

Trunking vo VLAN

- **Riešenie**:
  - Použiť na prepojenie dvoch prepínačov jeden spoj, cez ktorý sa budú prenášať rámce zo všetkých VLAN
  - Ako potom ale rozlíšiť, do ktorej VLAN konkrétny rámec prenášaný týmto spojom patrí?
  - rámce sa budú značkovať
- Jedná sa o tzv. **trunking** (spôsob multiplexovania)
  - Pojmy „trunk“ a „trunking“ používa spoločnosť Cisco, iní výrobcovia môžu túto istú funkciu nazvať inak (napr. **tagging** alebo **tagged ports**)
- Trunk porty teda slúžia na prepojenie prepínačov tak, aby sa VLAN mohli súvisle rozprestierať nad viacerými prepínačmi a pritom aby nestratili svoju izolovanosť

Trunking vo VLAN



- Porty pripojené k počítačom: **prístupové** (**access**) porty
  - Patria do jednej konkrétnej VLAN danej konfiguráciou
  - Nepoužívajú označovanie rámcov, pretože nie je potrebné
- Porty prepájajúce prepínače: **trunk** porty
  - Patria do všetkých existujúcich VLAN
  - Používajú označovanie rámcov na rozlíšenie VLAN, do ktorých patria

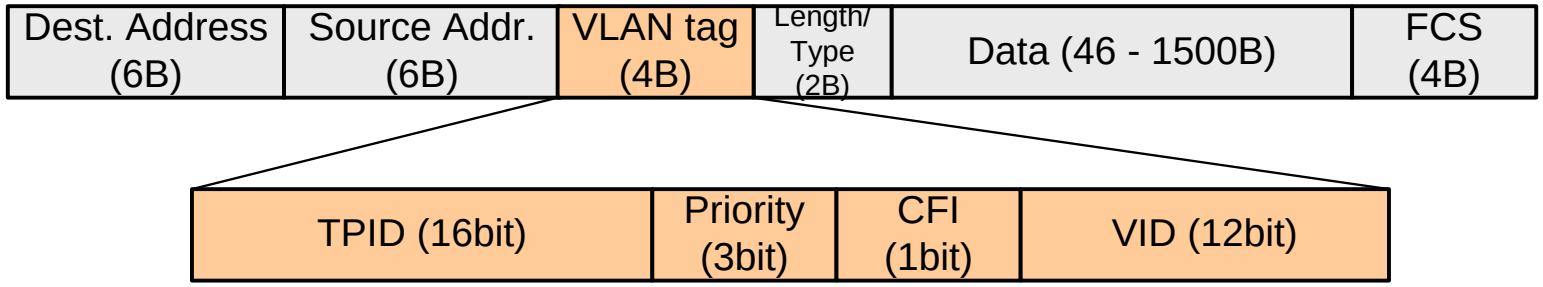
Trunk protokoly

- Existuje niekoľko spôsobov označovania, do akej VLAN rámec prenášaný trunkovým prepojom patrí
- **ISL (Inter-Switch Link)**
  - Proprietárny protokol spoločnosti **Cisco**
  - Rámce prechádzajúce trunk prepojom sa zabalia do nového rámca s prídavnou hlavičku s informáciou o VLAN
    - Celý pôvodný rámec sa balí do nového rámca – forma **tunelovania**
    - Formát pridanej hlavičky je technicky **SNAP**, pre obyčajné ethernetové prepínače sa javí ako multicastový rámec
    - Bežné prepínače budú rámec šíriť ako **multicast**, t.j. chovajú sa z pohľadu ISL ako zdieľaný segment
    - Prídavná hlavička a nový kontrolný súčet pridajú spolu **30B** ku každému rámcu

Trunk protokoly

- **IEEE 802.1Q**
  - **Otvorený** štandard, široko podporovaný výrobcami sieťových zariadení aj operačných systémov
  - Zachováva **základnú** štruktúru ethernetového rámca
    - Značkovaný rámec je plne kompatibilný s bežnými ethernetovými rámcami
  - Do tela rámca sa vkladá **4B značka**, tzv. tag
    - Nejedná sa o obaľovanie rámca do novej hlavičky
  - Dovoľuje použiť 4094 rôznych VLAN
  - Rozširuje Ethernet o možnosť priority rámcov

Formát značky 802.1Q



- **TPID (Tag Protocol Identifier)**: 16 bitov
  - Má povahu poľa EtherType
  - Obsahuje konštantnú hodnotu **0x8100**, ktorá informuje, že tento rámec je značkovaný
- **Priority**: 3 bity
  - Vyjadruje prioritu rámca v rozsahu 0-7
  - Toto prioritné značkovanie sa niekedy nazýva aj **Class of Service** (CoS marking) podľa IEEE 802.1p
- **CFI (Canonical Format Indicator)**: 1 bit
  - Používané len v non-Ethernet sieťach (Token Ring)
  - Vyjadruje, či adresy v rámci sú/nie sú v tzv. kanonickom formáte (poradie bitov v bajte od Least Significant bit po Most Significant bit)
  - 802.1Q-2011 predefinoval CFI na **Discard Eligible Indicator** (info, že rámec môže v prípade nutnosti byť zahodený prednostne)
- **VID (VLAN Identifier)**: 12 bitov
  - Identifikuje VLAN, do ktorej rámec patrí
  - 4096 možných VLAN (0-4095)

Typy VLAN na prepínačoch Cisco

Podľa spôsobu použitia:

- **Default VLAN**: synonymum pre VLAN1
  - Vždy existujúca VLAN
  - Nemožno ju zmazať, premenovať, prečíslovať
  - Je automaticky použitá ako natívna VLAN na trunk portoch a ako access VLAN na prístupových portoch
- **Native VLAN**
  - VLAN, ktorá na trunku ako jediná nepoužíva značky
  - Implicitne je to VLAN1

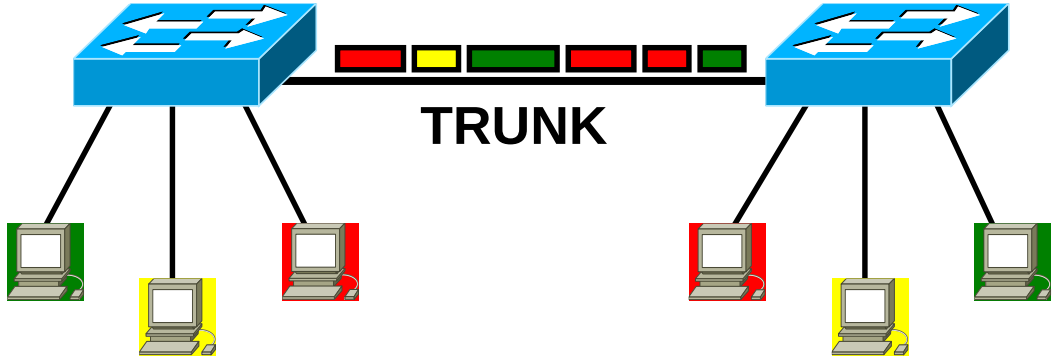
```
Switch# show vlan brief

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
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

- **Access VLAN** resp. **Data VLAN**
  - Konkrétna jedna VLAN, do ktorej je zaradený prístupový port
- **Voice VLAN**
  - Prídavná (auxiliary) VLAN na prístupových portoch, v ktorej sa prenášajú dáta z a do IP telefónu, ak je k portu pripojený
- **Management VLAN**
  - VLAN, pre ktorú je nakonfigurovaný aj `interface VLAN`
  - V tejto VLAN má prepínač svoju vlastnú IP adresu (manažment)

Vyhradené čísla VLAN v 802.1Q

- Zo 4096 možných VLAN (0-4095) sú niektoré VLAN štandardom vyhradené
- **VLAN 0**
  - Vyjadruje, že tag nesie užitočnú informáciu len o **priorite** (CoS a DEI), avšak odosielateľ neuvádza, do akej VLAN patrí
  - Umožňuje koncovým staniciam vyznačovať prioritu v rámcoch bez toho, aby vedeli alebo rozumeli, čo sú VLAN a do akej patria
  - Rámec s tagom pre VLAN 0 patrí do predkonfigurovanej **VLAN portu**, ktorým vošiel (t.j. ako keby ani nemal 802.1Q tag)
- **VLAN 4095**
  - Číslo VLAN, ktoré sa nikdy nesmie objaviť v tagu
  - Výrobcovia prepínačov môžu toto číslo **interne** vo vnútri prepínača využiť pre svoje účely s istotou, že nebude kolidovať s reálnou VLAN

Prenos rámcov v 802.1Q



- Rámec prijatý na prístupovom porte bude spracovaný v zodpovedajúcej prístupovej VLAN tohto portu
- Rámec prijatý na trunk porte bude spracovaný vo VLAN podľa značky, no ak značka chýba resp. ak VID=0, v natívnej VLAN
- Rámec odoslaný prístupovým portom nebude značkovaný
- Rámec odoslaný trunk portom bude obsahovať značku VLAN, do ktorej patrí, s výnimkou natívnej VLAN – rámce v natívnej VLAN sa na trunku odošlú bez značky

Pomôcka pri rozbehu trunk portov – DTP

- Pri úvodnej konfigurácii novej prepínanej siete môže dôjsť k problémom, keď navzájom prepojené prepínače nepoužívajú na spoločnej linke ten istý režim portu (jeden je access, druhý je trunk)
- Cisco na svojich prepínačoch používa protokol **Dynamic Trunk Protocol**, ktorého úlohou je zariadiť, aby navzájom prepojené porty používali ten istý režim, ak je to možné
- DTP pomáha pri úvodnom rozbehu siete, ale nie je vhodný na trvalú prevádzku
  - Režimy portov access/trunk majú byť stanovené „natvrdo“ konfiguráciou, nie je vhodné spoliehať sa na automatické dojednanie
- **Predvolený** režim portov na Cisco prepínačov je **dynamický** režim (prispôsobujúci sa druhej strane)

Režimy portov na Cisco prepínačoch

- S ohľadom na podporu DTP môžu porty na Cisco prepínačoch byť v niektorom z nasledujúcich režimov
  - **`switchport mode dynamic desirable`** (Catalyst 2950, 3550)
    - Port sa vie prispôsobiť druhej strane (dynamický port)
    - Port preferuje režim trunk, ohlasuje ho pomocou DTP
  - **`switchport mode dynamic auto`** (Catalyst 2960, 3560)
    - Port sa vie prispôsobiť druhej strane (dynamický port)
    - Port preferuje režim access, ohlasuje ho pomocou DTP
  - **`switchport mode trunk`**
    - Port sa nevie prispôsobiť druhej strane (statický port)
    - Svoj režim trunk ohlasuje pomocou DTP
  - **`switchport mode access`**
    - Port sa nevie prispôsobiť druhej strane (statický port)
    - Na tomto porte je DTP úplne vypnuté (neodosiela ani neprijíma)

Režimy portov na Cisco prepínačoch

- Výsledný prevádzkový (operational) stav portov je daný kombináciou ich konfiguračných (administrative) stavov
  - Dynamic desirable + Dynamic desirable = Trunk
  - Dynamic desirable + Dynamic auto = Trunk
  - Dynamic auto + Dynamic auto = Access
  - Dynamic (akýkoľvek) + Trunk = Trunk
  - Dynamic (akýkoľvek) + Access = Access
  - Trunk + Trunk = Trunk
  - Access + Access = Access
  - Trunk + Access = PROBLEM

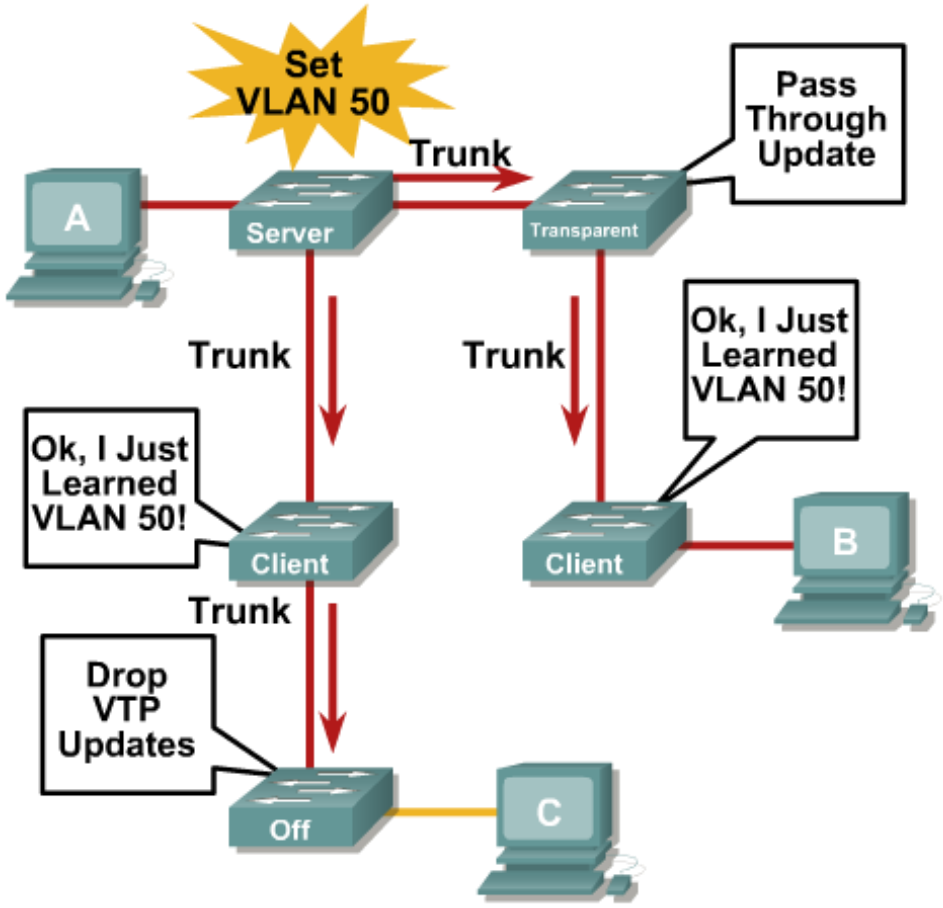
	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

Odporúčania pre nasadzovanie VLAN

- Presunúť nepoužité porty do osobitnej nepoužívanej VLAN
  - Táto VLAN môže byť nakonfigurovaná ako tzv. suspendovaná, v ktorej je akákoľvek komunikácia zakázaná
  - Nepoužité porty sa rovnako odporúča úplne vypnúť
- Vytvoriť osobitnú manažmentovú VLAN, odlišnú od akejkoľvek inej existujúcej VLAN
  - Členmi tejto VLAN budú len prepínače, nie koncové stanice
  - Prístup z iných VLAN bude riešený cez smerovač
- Zmeniť natívnu VLAN na trunk portoch na osobitnú VLAN odlišnú od akejkoľvek inej existujúcej VLAN
  - Členom tejto natívnej VLAN nebude vôbec nikto
  - Predchádzanie útokom pomocou dvojitého značkovania
- Pre vzdialený manažment povoliť iba SSH, deaktivovať Telnet
- Na trunk portoch po ich konfigurácii a rozbehu deaktivovať DTP
- Neponechávať žiadne porty v (predvolenom) dynamickom režime
- **Vyhýbať sa akémukoľvek používaniu VLAN1**

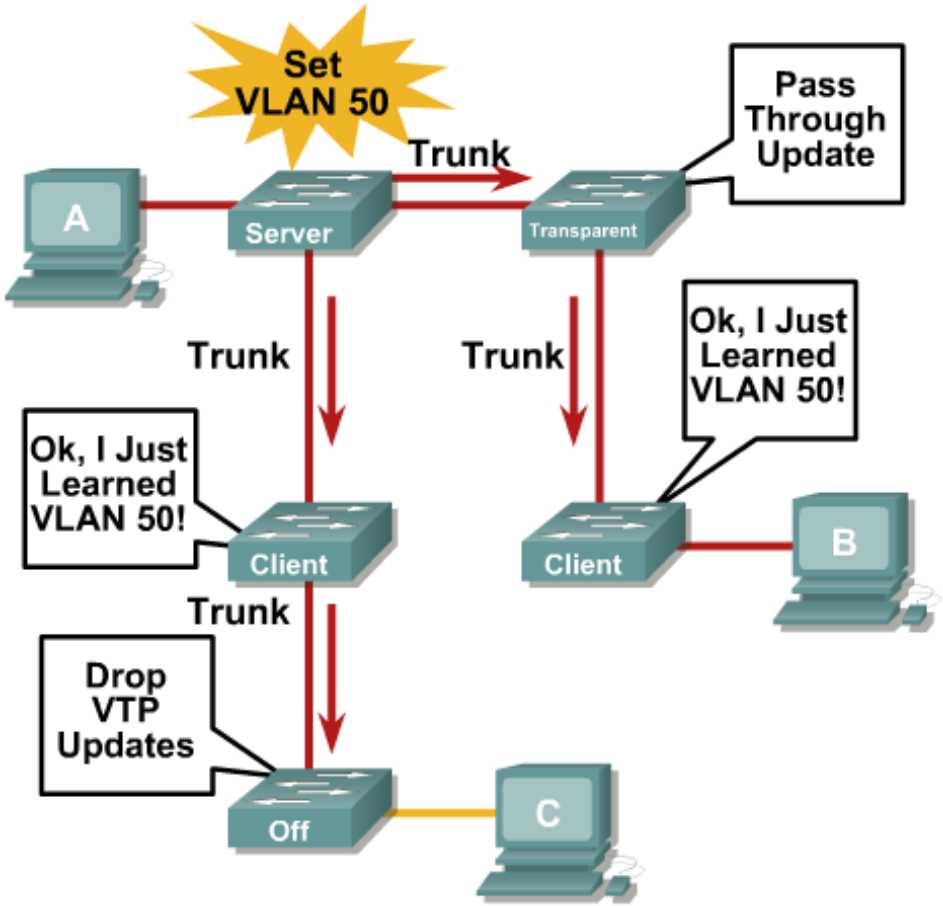
Výhody VTP

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



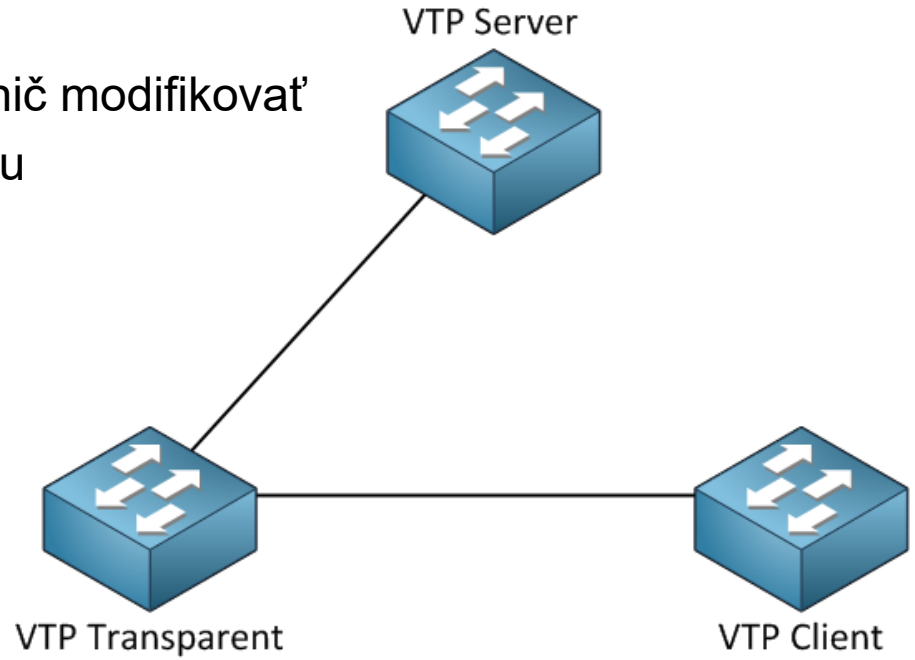
Virtual Trunking Protocol (VTP)

- 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



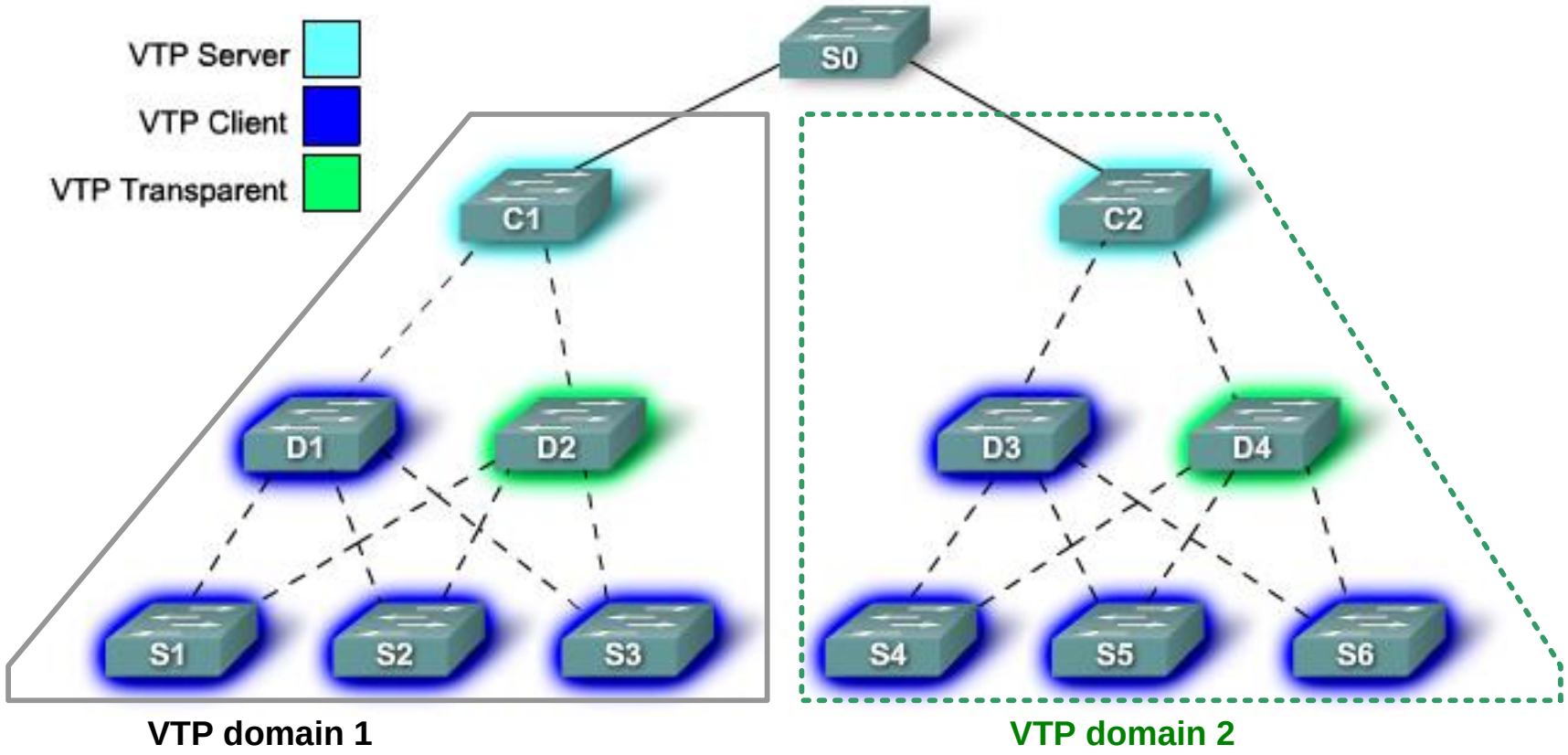
VTP módy

- **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)

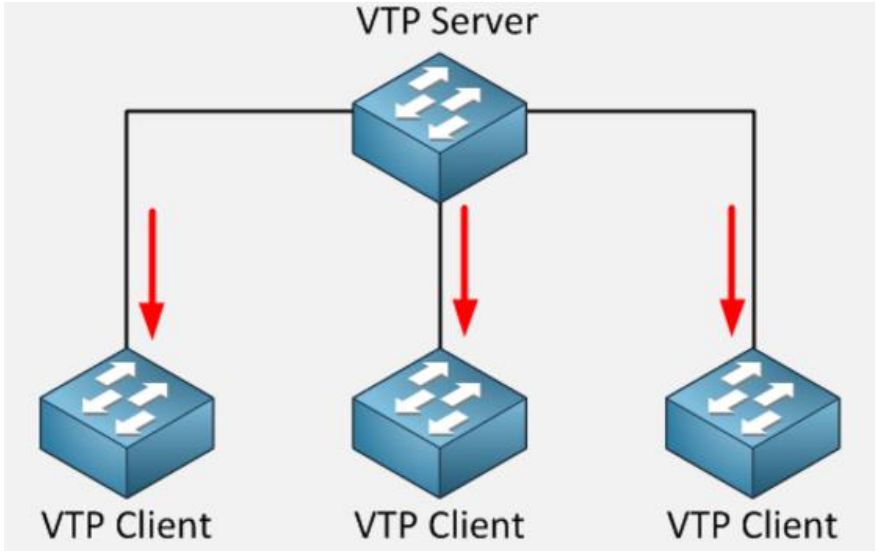


VTP doména

- 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
- Pri tom 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-ách, 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 subset advertisements

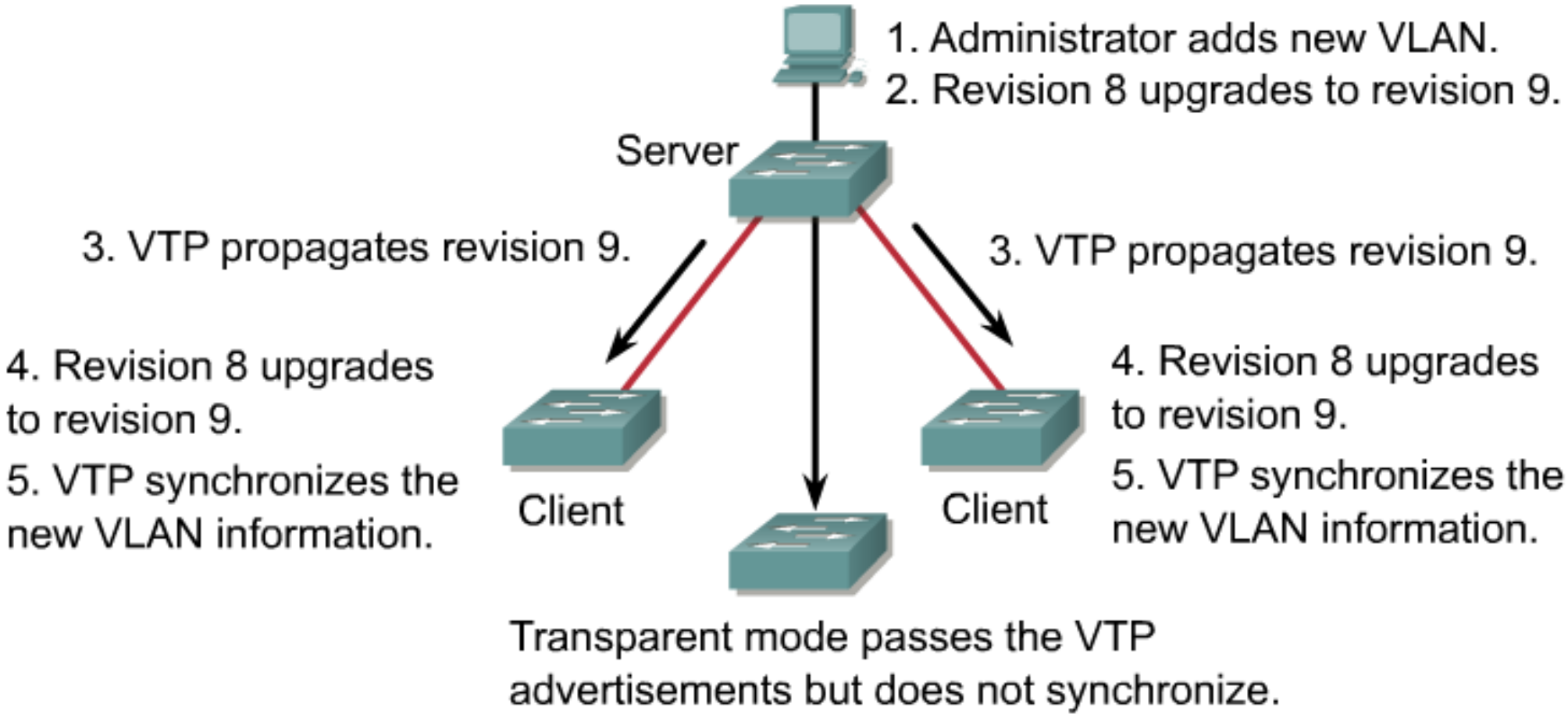
VTP správa

- 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**
  - **Version** – Verzia VTP, buď VTP 1, VTP 2 or VTP 3. Cat2960 podporuje VTP 1 a VTP 2. 1 a 2 sú navzájom nekompatibilné.
  - **VTP Message Type –** Summary Adv., Subset Adv., Adv. Request, ..
  - **Domain name –** Identifikuje VTP doménu prepínača.
  - **Domain name length** – Dĺžka doménového mena.
  - **Configuration revision number** – Aktuálne číslo revízie updatu.

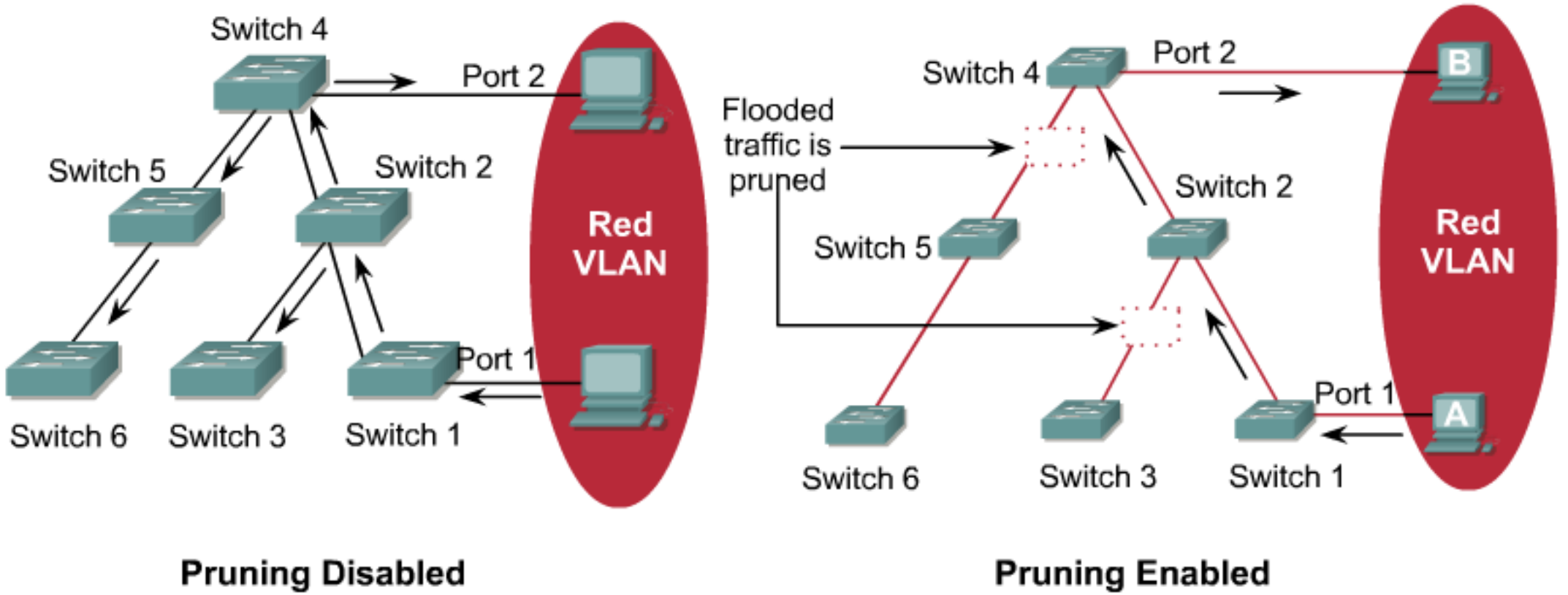
- **Telo**
  - Obsahuje fixné info:
    - VTP domain name
    - Identita prepínača posielajúceho správu, a časovú značku
    - MD5 otlačok konfiguračných parametrov VLAN
    - Formát rámca: ISL or 802.1Q
  - Info pre každú konfigurovanú VLAN:
    - VLAN IDs (IEEE 802.1Q)
    - VLAN name
    - VLAN type
    - 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.

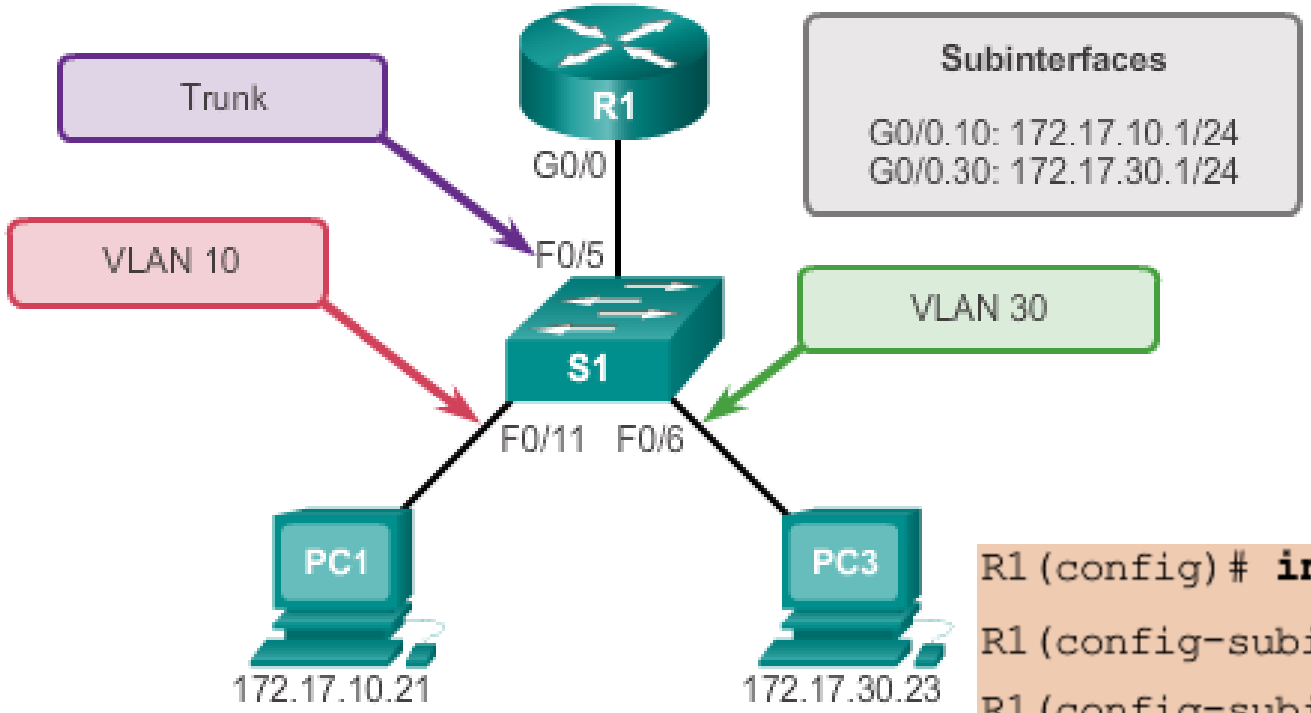
VTP pruning

- 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



InterVLAN routing

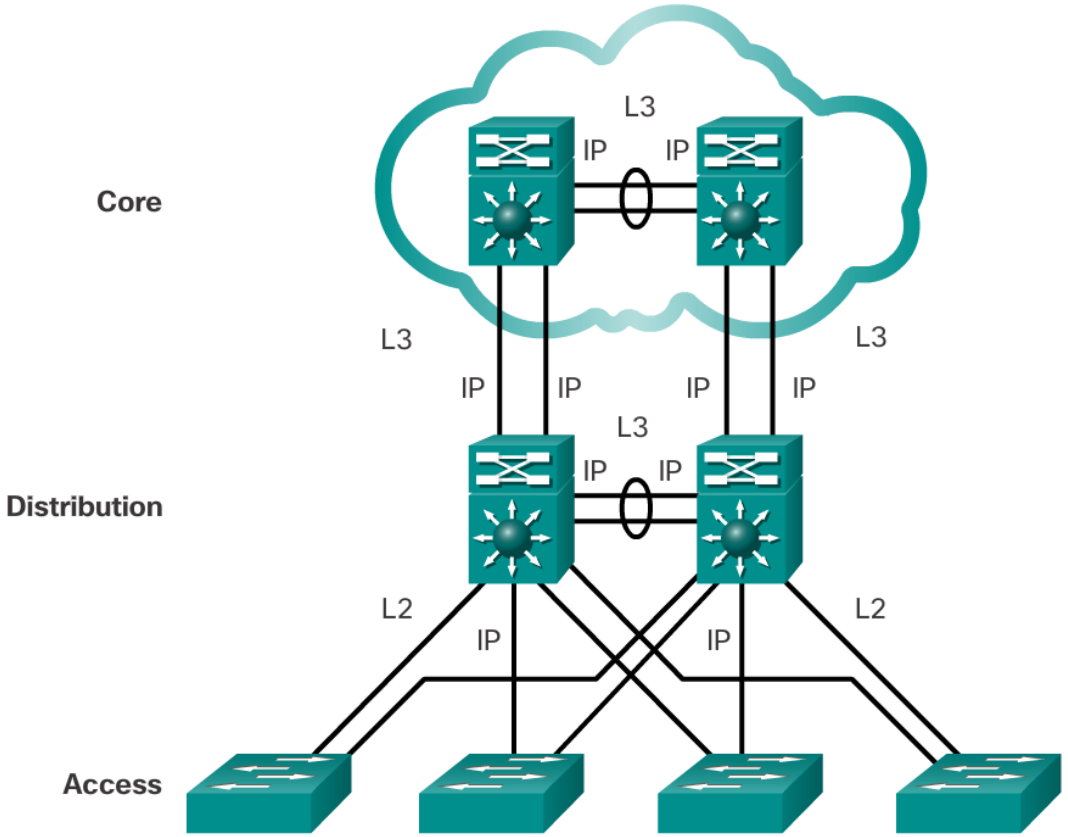
Smerovanie medzi VLAN pomocou router-on-stick




```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
```

Použitie MLS na smerovanie medzi VLAN

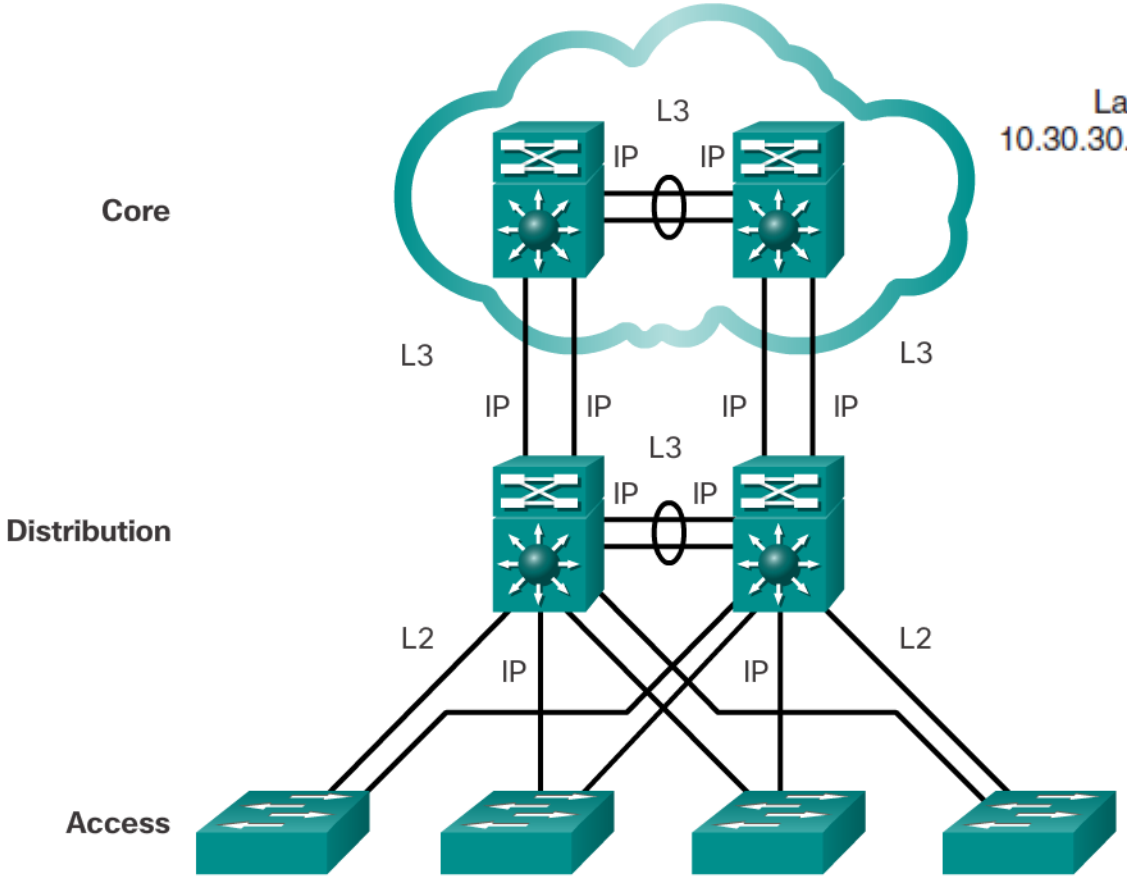
- V hierarchickom modeli prepínanej siete (access, distribution, core) sa MLS prepínače umiestňujú často do **distribučnej** a **chrbticovej** časti
  - **VLAN** sú vytvorené na prístupových a distribučných prepínačoch
  - **Medzi VLAN** sa smerovanie realizuje na distribučných prepínačoch
  - **Navonok** sa činnosť MLS prepínačov a samostatných smerovačov nedá rozoznať, okrem výkonu
  - MLS majú významne **vyššiu prenosovú kapacitu**
  - Mnohé **high-end** smerovače sú v skutočnosti MLS prepínače

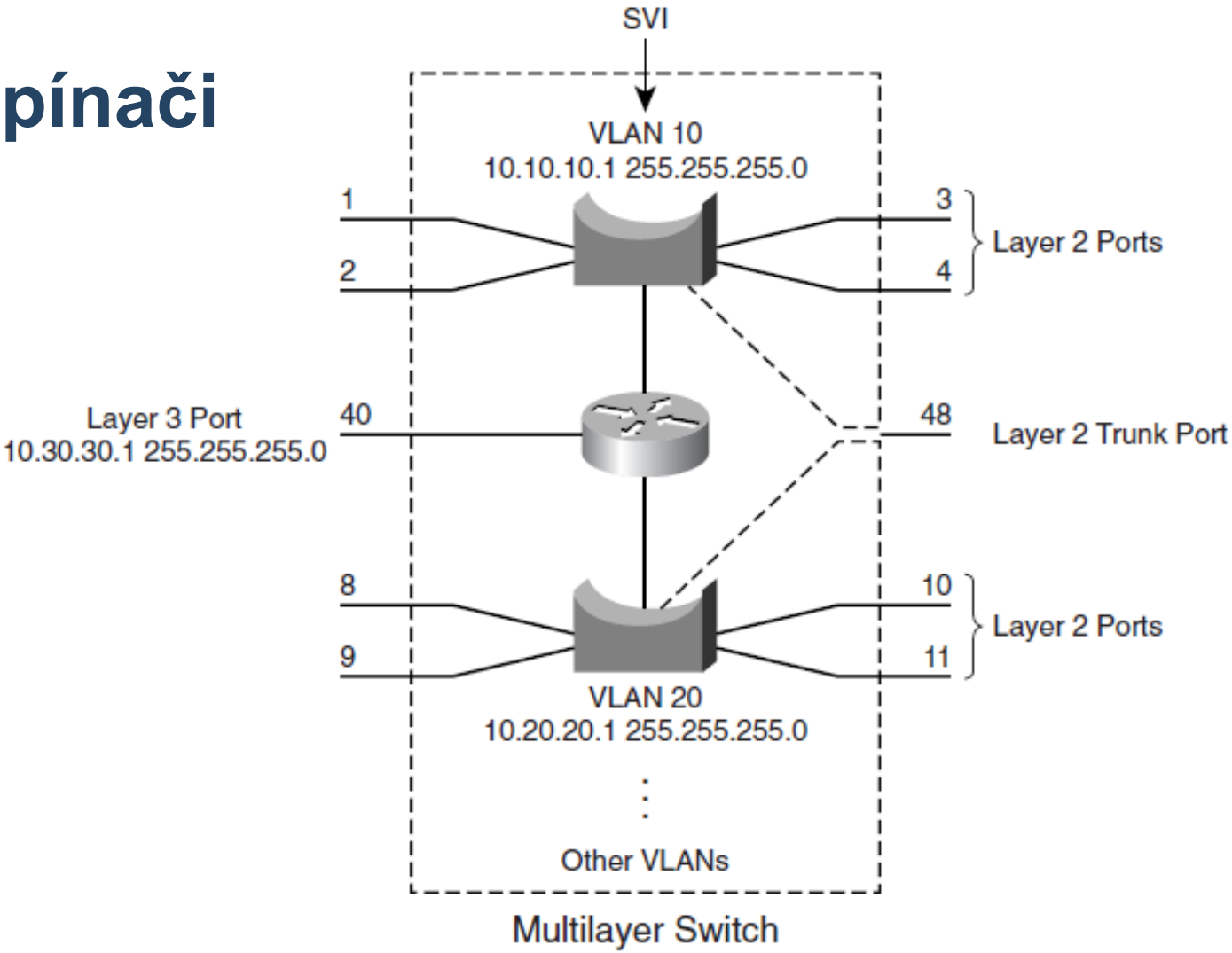


Smerované rozhrania na MLS

- Smerovanie pomocou smerovačov typu router-on-stick je funkčné a použiteľné, ale zároveň málo výkonné
- Rádovo **vyššiu priepustnosť** i **operatívnosť** ponúkajú tzv. multilayer switches (MLS)
  - Prepínače, ktoré vo svojich špecializovaných HW obvodoch vedia robiť funkcie prepínania aj smerovania zároveň
- MLS používajú dva druhy smerovaných rozhraní
  - Switched Virtual Interface – **SVI** (zväčša distribučný switch k prístupovému)
  - Fyzické smerované rozhrania – **routed** (zväčša medzi core a distribution)
- SVI je jednoducho `interface VLAN X`
  - Jedná sa o virtuálne rozhranie, ktoré prepája vnútorný smerovač MLS prepínača s konkrétnou VLAN
  - Implicitne je vytvorené rozhranie vo VLAN 1, ostatné SVI rozhrania môžeme podľa ľubovôle vytvárať či odstraňovať
  - Na rozdiel od L2 switchov, kde má zmysel vytvárať spravidla iba jedno takéto rozhranie, MLS switche môžu mať pre každú VLAN samostatné SVI
  - SVI je rozhraním smerovača v MLS pripojeným do danej VLAN siete

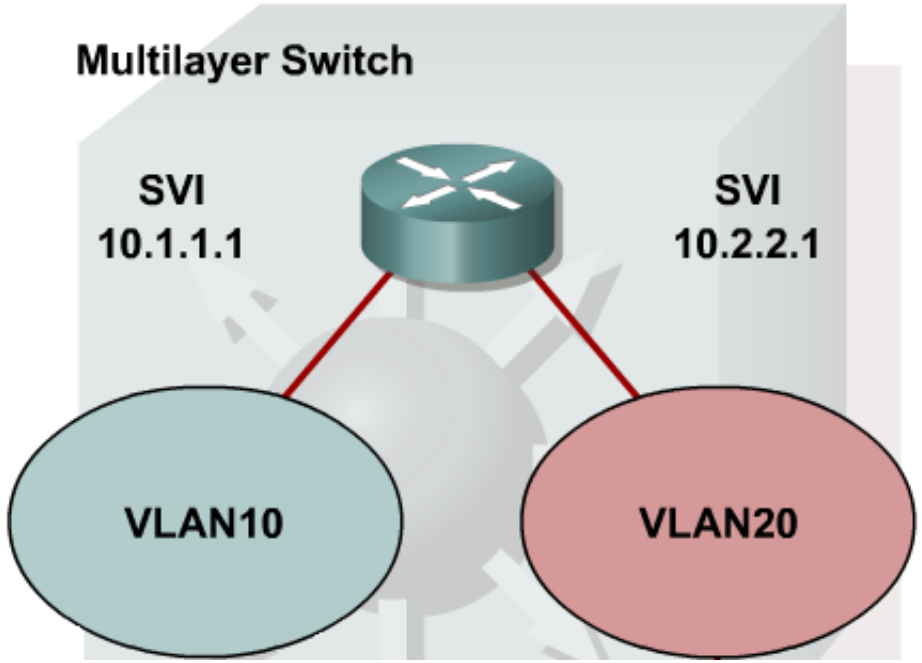
Typy portov na MLS prepínači





SVI rozhrania na MLS

- Príkaz `ip routing` aktivuje podporu pre L3 switching
  - Môžu byť potrebné i dodatočné príkazy
- Po zadaní tohto príkazu je možné na MLS pracovať ako na routeri
  - Smerovacia tabuľka
  - Smerovacie protokoly




```
Switch(config)# ip routing
Switch(config)# vlan 10,20
Switch(config-vlan)# exit
Switch(config)# int vlan 10
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# int vlan 20
Switch(config-if)# ip address 10.2.2.1 255.255.255.0
```

Multi-Layer switching (MLS)

- Multilayer switching je pojem pre prepínanie datagramov na rôznych vrstvách OSI
  - **Layer 1** – nie je switching: Prenos a zosilnenie signálu
  - **Layer 2 switching**: Prenos rámcov (určujúca je L2 hlavička)
    - Hardware based bridging
  - **Layer 3 switching**: Prenos paketov (určujúca je L3 hlavička)
    - Hardware based routing
  - **Layer 4 switching**: Prenos segmentov (určujúca je L3 + L4 hlavička)
  - **Layer 7 switching**: Prenos aplikačných dát (určujúci je ich obsah)
- Rozdiel medzi switchingom a routingom?
  - Routing je obvykle softvérový - CPU
  - Switching je realizovaný s hardvérovou podporou – ASIC
- Multilayer switche
  - Switche s podporou prepínania na viacerých vrstvách súčasne
  - Rozšírene používané v Campus net. dizajne

MLS Cisco prepínače na L3

- Môžu používať tri módy prepínania:
  - Process-based switching
    - Bežný softvérový routing
  - Fast switching - Route caching
    - Alternatívne názvy: *NetFlow LAN switching, flow-based or demand-based switching, „route once, switch many“*
    - Prvý paket ako PBS, ďalšie cez cache
  - Cisco Express Forwarding (CEF) – topology based switching
    - Sw/hw, centralizované/distribuované
    - Forwarding Information Base (FIB)
      - Routing TCAM or L3 forwarding table
      - „otlačok“ smerovacej tabuľky
    - Adjacency table (L2 info)
      - L2 next hop rewrite info

●Show ip cef [detail]

●show adjacency ...

STP a jeho varianty

STP umožňuje

- Prepínače komunikujú cez špeciálne STP rámce (BPDU - Bridged Protocol Data Unit) za účelom:
  1. **krok**: Volia Root Bridge (RB)
     - Referenčný bod stromu, je len jeden
  2. **krok**: Volia ROOT ports
     - Porty najbližšie k Root-ovy
  3. **krok**: Určujú Designated porty a non-Designated pre každý segment
- Výsledkom je bezslučková (LOOP FREE) topológia
  - Ktorá dokáže aktívne prehodnocovať aktuálnu topológiu a reagovať na zmeny v sieti
  - Jedna topológia pre celú prepínanú sieť, alebo pre všetky VLAN v nej
- Každý prepínač si pamätá posledné najlepšie BPDU

BPDU rámce

Bytes	Field
2	Protocol ID
1	Version
1	Message type
1	Flags
8	Root ID
4	Cost of path
8	Bridge ID
2	Port ID
2	Message age
2	Max age
2	Hello time
2	Forward delay

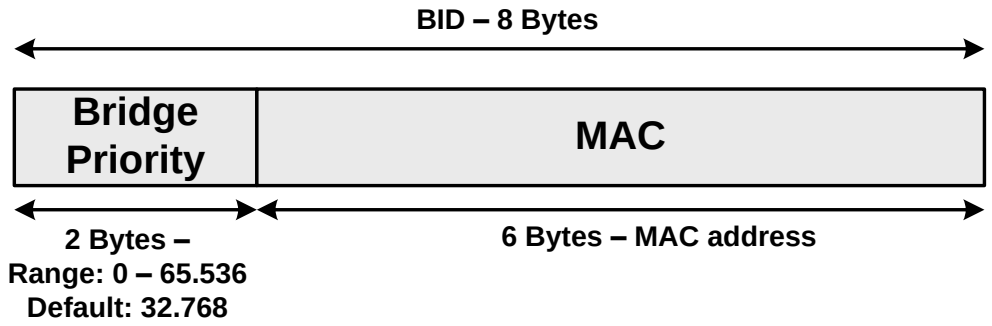
- Dva typy BPDU
  - Configuration BPDU
  - Topology Change Notification (TCN) BPDU
  - Posielané každé 2 sek.

- Kto je root bridge
- Ako ďaleko je root bridge
- Aké je BID prepínača, ktorý poslal BPDU
- Cez ktorý port odosielateľa tento BPDU odišiel.

- **Po zapnutí prepínača Root ID = Bridge ID**

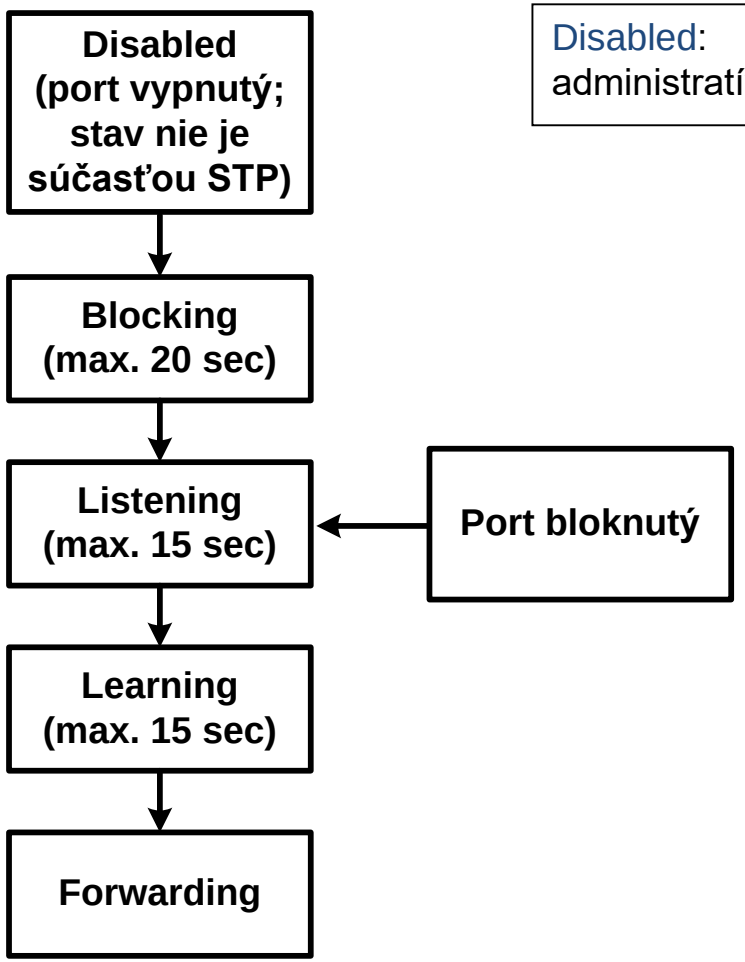
STP Bridge Identity (BID) a Cost

- **Každý prepínač:**
  - Je identifikovaný **BID** (**Bridge ID) (**8 Bajtov)
    - 2B: Priority
      - Môže nastaviť administrátor
      - Default: 32768
    - 6B: MAC adresa
      - MAC adresa prepínača
  - Každý port prepínača:
    - **Má pridelený identifikátor** (**Port Identifier**)
      - Jedinečný v rámci prepínača
    - **Má pridelenú cenu (Path Cost)**
      - Na základe rýchlosti rozhrania
    - **Má pridelenú prioritu portu (Port Priority)**
      - **Def. 128**



Link speed	Cost (Revised IEEE spec)	Cost (Previous IEEE spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

Stavy portov



Disabled:
administratívne down

Blocking: Prijíma BPDU, neprijíma dátové rámce. Neposiela BPDU.

Ostáva v ňom Max Age timer (20sec.). Zistenie Root BID a úloh portov.

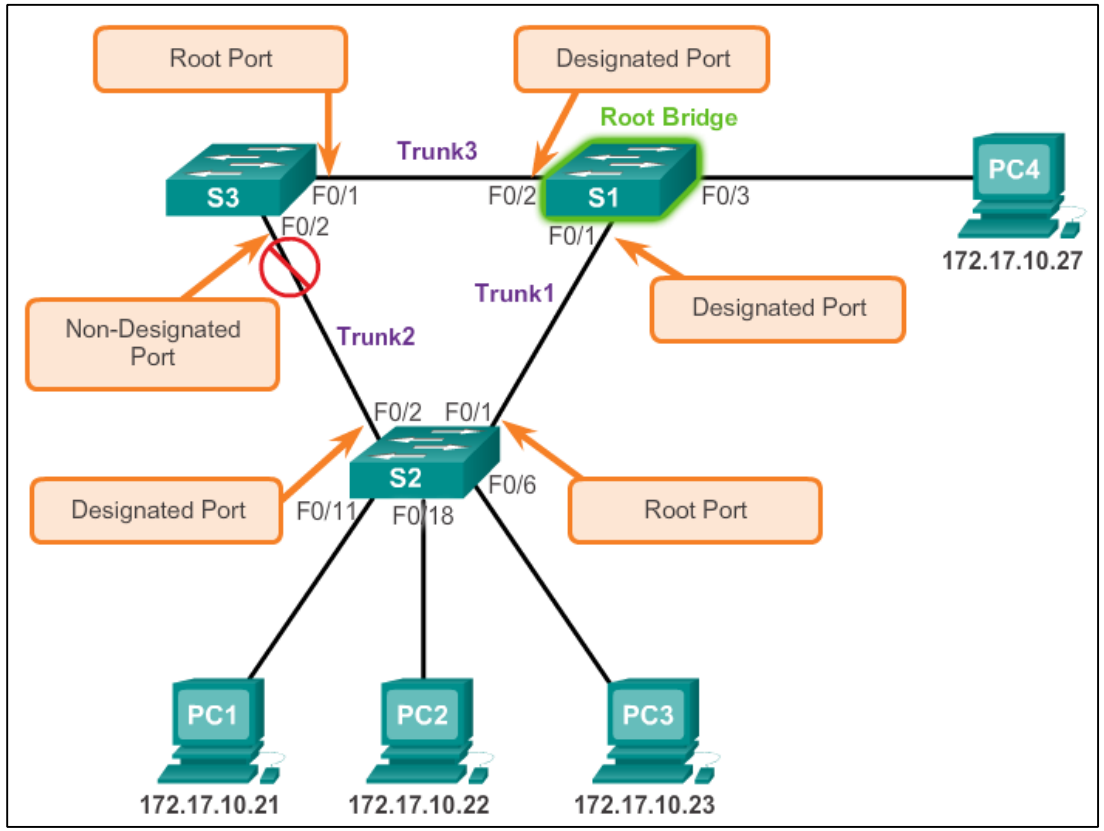
Listening: Prijíma, spracováva a preposiela BPDU (info. že port je pripravený pracovať v aktivnej topo), neprijíma dátové rámce, neučí sa MAC adresy

Learning: Spracováva BPDU, neposiela dátové rámce, učí sa však MAC adresy (buduje Bridging table)

Forwarding: Spracováva BPDU, posiela, prijíma dátové rámce, učí sa MAC adresy

Pozn. Def. stav po oživnutí portu je listening

Role portov v STP topológii



Rola	Popis
Root Port	Port na non-root prepínačoch. Je to port na najkratšej ceste k Root Bridge. Existuje len jeden Root Port pre prepínač.
Designated Port	Existuje aj na RB aj na non-RB. Je to port, ktorý forwarduje data smerom k RB. Na RB všetky porty sú Designated. Na non-RB len jeden per segment, ak viac prepínačov musí byť voľba.
Non Designated Port	Port v stave BLOCKING, neforwarduje žiadne uživ. dáta.
Disabled Port	Port ktorý je SHUT DOWN.

STP časovače

Hello Time	Čas medzi dvomi BPDU poslanými cez port. Default je 2 s. Možné hodnoty <1, 10> sek.
Forward delay	Čas strávený v Listening a Learning stave. Def. Je 15 sek. Možné hodnoty <4, 30> sek.
Maximum age	Čas, na ktorý si prepínač per port ukladá najlepšie prijaté BPDU. Def. je 20, možné hodnoty <6, 40> sek. Ak do jeho uplynutia neprijaté BPDU – iniciovaná nová voľba RB.

Rozhodovací proces používaný pri porovnávaní BPDU

- STP stavia svoju činnosť na schopnosti porovnať dvojicu BPDU a vyhlásiť, ktoré je lepšie (superior) a ktoré je horšie (inferior)
- BPDU sa porovnávajú v tomto poradí parametrov:
  - 1 – Root Bridge ID (má dve časti!)
  - 2 – Root Path Cost
  - 3 – Sender Bridge ID (má dve časti!)
  - 4 – Sender Port ID (má dve časti!)
  - 5 – Receiver Port ID (má dve časti; porovnáva sa len výnimočne)
- Parameter N sa porovnáva len vtedy, ak sú všetky predošlé parametre zhodné
- Lepšie je to BPDU, v ktorom sa pri danom poradí porovnávania parametrov nájde prvýkrát nižšia hodnota

Prvý krok - voľba Root bridge (RB)

- Výber RB ovplyvní dátový tok v prepínanej sieti
- Každý prepínač po zapnutí začne posielať STP rámce (BPDU) so svojim BID
  - Defaultne predpokladá, že RB je on sám
  - Rozposlané všetkým prepínačom
- Ak nejaký iný prepínač:
  - Má nižšie BID ako je uvedené v prijatom BPDU rámci, rámec prepínač zahodí
  - Má vyššie BID, poznačí si lepšie BID a rámec pošle ďalej
- RB sa stane prepínač s najnižšou BID
  - Stane sa Root-om siete (začiatkom STP stromu)
    - Ovplyvňuje dátové toky v LAN
  - Defaultne je nastavená rovnaká priorita, rozhoduje sa na základe MAC adresy
    - Prioritu môže zmeniť admin a ovplyvniť tak voľbu RB

STP činnosť – ďalej ...

- **Root bridge** (RB)
  - Po voľbe je v sieti len jeden RB
  - Je počiatkom počítaného STP stromu
    - Od RB do každého segmentu siete je len jedna cesta
    - Všetky redundantné cesty, ktoré nebudú súčasťou STP stromu sú blokované
  - Všetky porty RB sú zvyčajne designated portami
    - Špeciálny prípad je slučka sám na seba
      - Tam sú niektoré blokované
  - Začne vysielať BPDU s cost = 0
- **Ďalšie kroky**
  - Určenie najkratšej cesty k RB (Root Path Cost), „root“ portov, určenie „designated“ prepínačov a „designated portov“

Skonvergované STP

- Po prebehnutí STP algoritmu
  - Loop free topológia
  - Jeden Root bridge per L2 net.
  - Jeden root port per non-root bridge.
  - Jeden designated port per segment.
  - Každý non-designated port je nepoužívaný (blokovaný).

STP – konvergencia

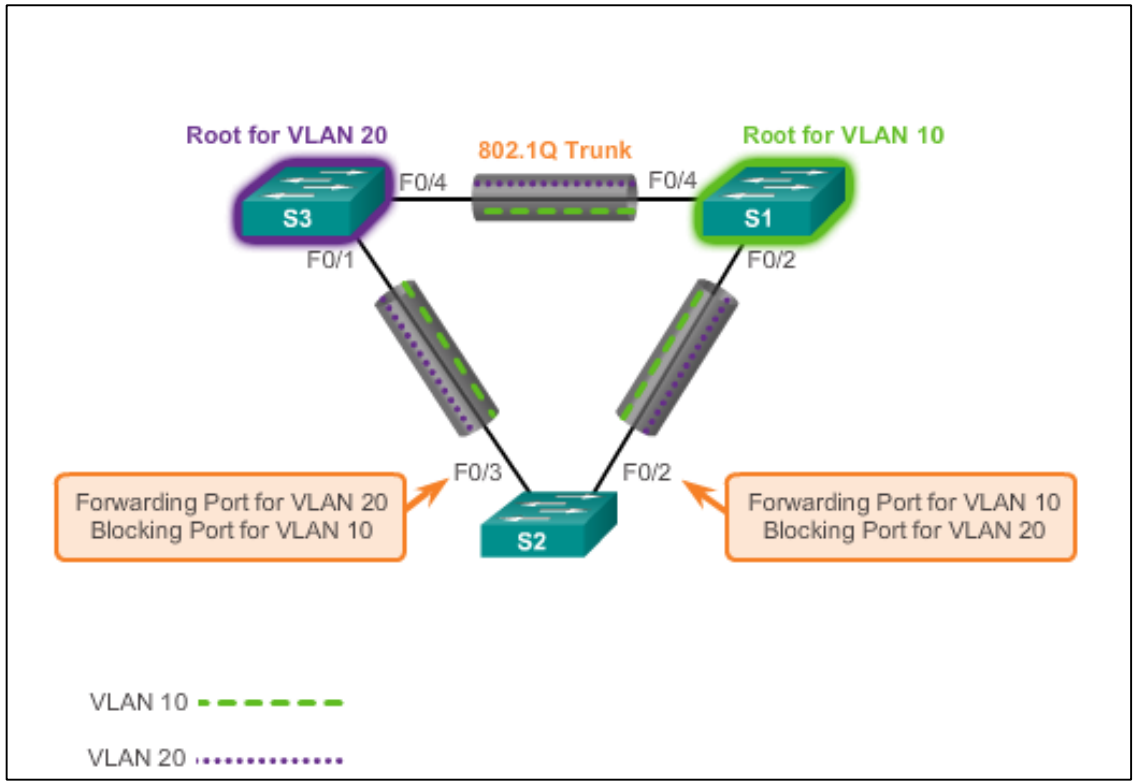
- Konvergencia
  - Keď všetky prepínače majú porty buď vo forwarding or blocking stavoch
    - BPDU sú neustále posielané
- STP proces sa spúšťa:
  - Pri zmene topológie
    - Pridanie, odobratie prepínača v sieti
    - Pridanie, odobratie linky v sieti
    - Zmena stavu portu up na down a naopak
      - Aj takého kde je PC!!!!!!
    - Strata konektivity s root bridge
  - Časté prepočty STP môžu viesť k slučkám
- STP konvergencia
  - Trvá od 30 do 50 sekúnd
    - Pre radius 7 prepínačov
    - V niektorých prípadoch ťažko akceptovateľné

Implementácie STP Cisco-m

- IEEE štadardy
  - Spanning Tree Protocol: IEEE802.1D-1998
  - Rapid Spanning Tree: IEEE 802.1w (IEEE 802.1D-2004)
  - Multiple STP (MSTP): IEEE 802.1s
- Cisco terminológia a riešenia
  - IEEE802.1D = Common STP (CST)
    - Jeden STP strom pre všetky VLAN
  - PVST (Per Vlan Spanning Tree)
    - Jeden STP strom pre každú VLAN
    - Podpora ISL trunking, + Cisco vylepšenia BackboneFast, UplinkFast, PortFast
  - PVST+ (Per Vlan Spanning Tree)
    - Jeden STP strom pre každú VLAN
    - Kompatibilita na 802.1D, + Cisco vylepšenia BackboneFast, UplinkFast, PortFast
  - Rapid PVST+
  - MSTP

Protocol	Standard	Resources Needed	Convergence	Tree Calculation
STP	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
Rapid PVST+	Cisco	Very high	Fast	Per VLAN
MSTP	802.1s Cisco	Medium or high	Fast	Per Instance

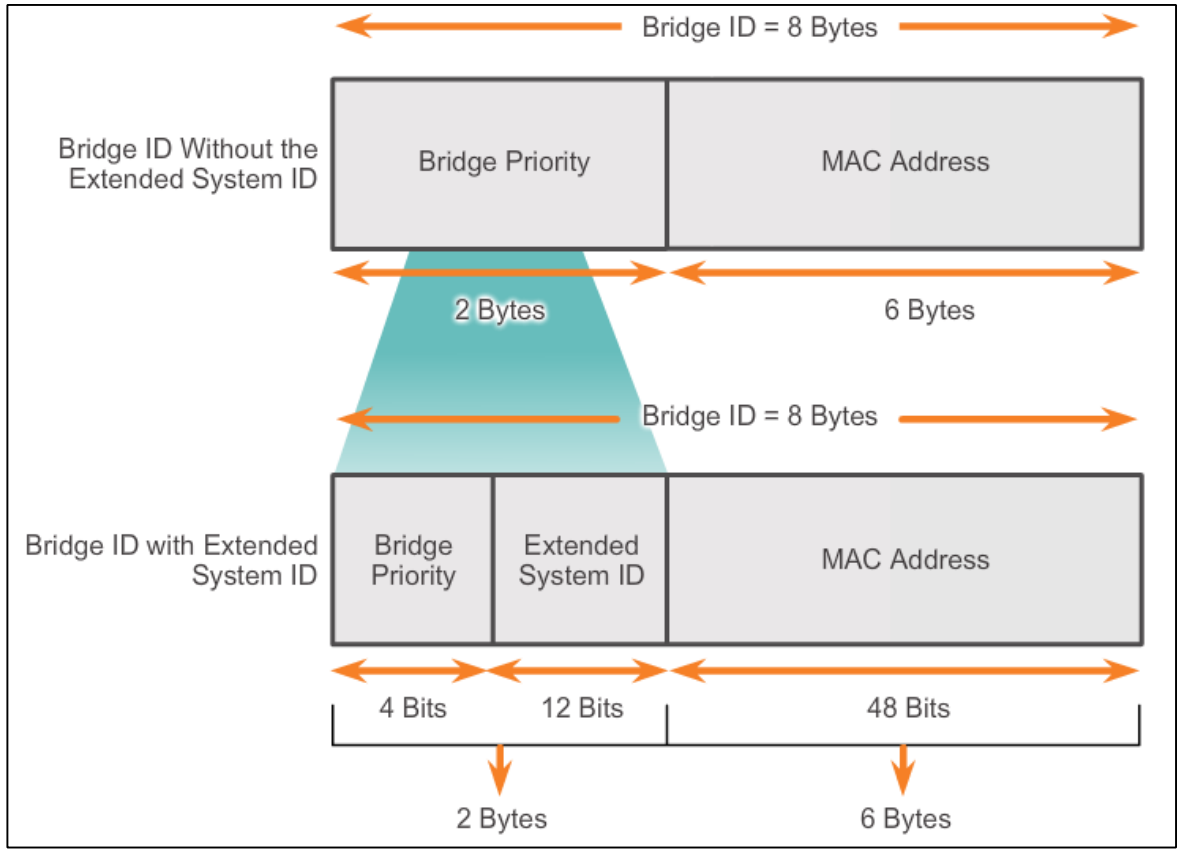
PVST+



- PVST+
  - sieť prevádzkuje nezávislé inštancie STP stromu pre každú VLAN zvlášť
  - je možné aplikovať load balancing
    - Optimalizácia distribúcie tokov
  - Problém s výkonom pri veľa VLAN

Extended System ID and PVST+ Operation

- Potreba zabezpečiť jedinečné BID pre každú VLAN a strom
- `BID Priority = Priority + VLAN_ID`

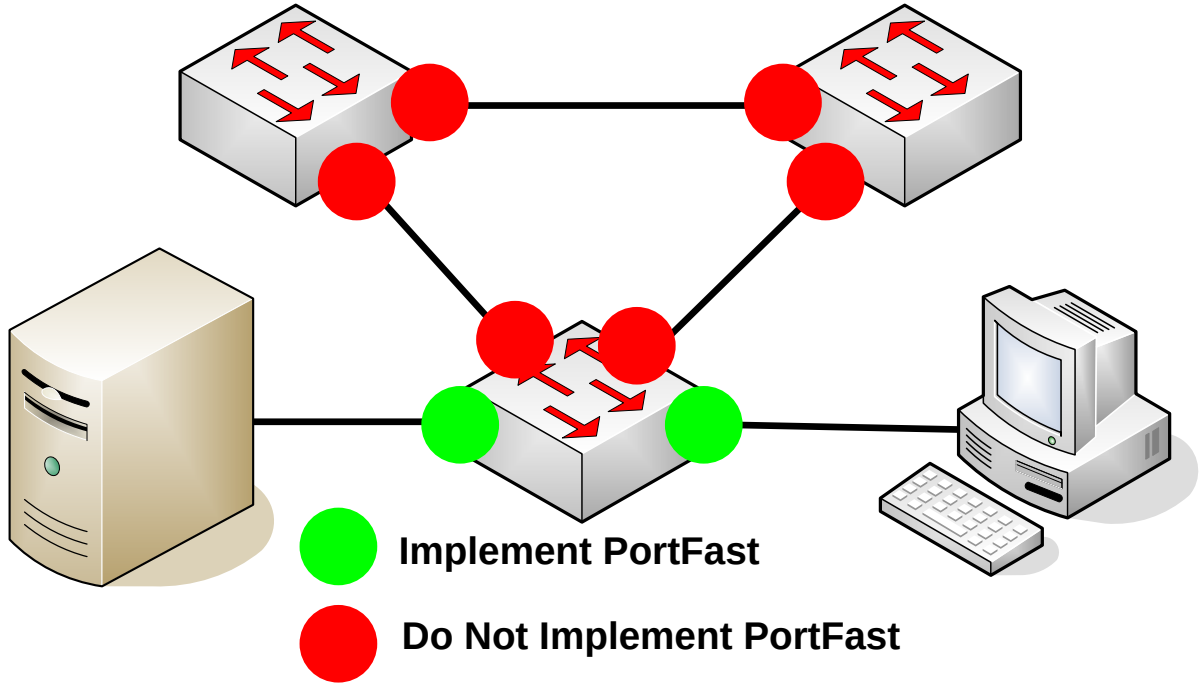


Default nastavenie na Catalyst-e

Feature	Default Setting
Enable state	Enabled on VLAN 1
Spanning-tree mode	PVST+ (Rapid PVST+ and MSTP are disabled.)
Switch priority	32768
Spanning-tree port priority (configurable on a per-interface basis)	128
Spanning-tree port cost (configurable on a per-interface basis)	1000 Mb/s: 4, 100 Mb/s: 19, 10 Mb/s: 100
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mb/s: 4, 100 Mb/s: 19, 10 Mb/s: 100
Spanning-tree timers	Hello time: 2 seconds Forward-delay time: 15 seconds Maximum-aging time: 20 seconds Transmit hold count: 6 BPDUs

Cisco vylepšenia STP

- Port Fast
  - Minimalizuje čas prechodu
  - Vhodné len na Access porty
  - Ak rozhranie s konfigurovaným PortFast príjme BPDU, spanning tree zhodí port do blocking stavu pomocou techniky **BPDU guard**.



Rapid Spanning Tree (RSTP)

- Urýchľuje prepočítavanie spanning-tree stromu pri zmenách topológie
  - Evolúcia STP 802.1d
  - Definovaný ako IEEE 802.1w
    - Dnes je zahrnutý do štandardu IEEE 802.1D-2004
    - Spätne kompatibilný s STP
  - Konvergencia od 1 do max. 15 sekúnd
  - Preferovaná voľba do full duplex prepínaného prostredia
    - Pri half-duplex rýchlosť nie je výrazne lepšia
  - Nasadenie tam, kde STP konvergencia je pomalá
  - Nepoužíva STP časovače, je proaktívny

Odlišnosti STP od RSTP

- Mení definíciu stavov portov (len tri stavy)
- Mení definíciu rolí portov (nové)
  - Zavádza Edge porty.
    - Rýchly prechod do Forwarding
    - Niečo ako PortFast vlastnosť
- Mení definíciu typov liniek
- Používa také isté BPDU ako STP
  - Len Version = 2
  - Proaktívne správanie
  - Posiela každý prepínač, nie len RB ako v STP
  - Proposal / Agreement mechanizmus
- Dokáže spolupracovať s STP na jednej sieti
  - RSTP port ktorý príjme BPDU verzie 1 začne pracovať ako STP port

Pozn. Def. stav po oživnutí portu je designated discarding

Zmena stavov portov

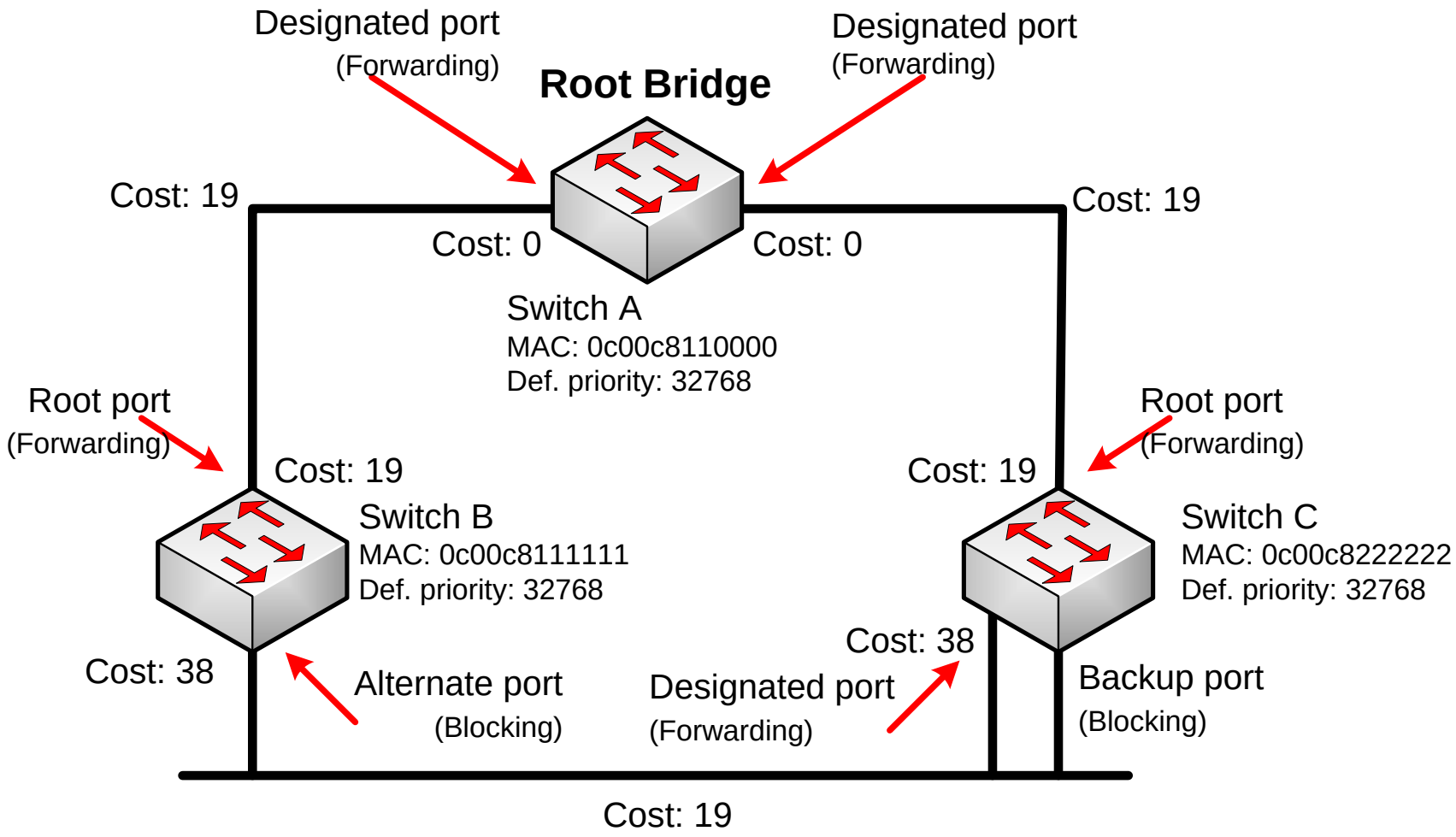
STP (802.1D) Port State	RSTP (802.1w) Port State	Is Port Included in Active Topology?	Is Port Learning MAC Addresses?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	Yes	No
Learning	Learning	Yes	Yes
Forwarding	Frowarding	Yes	Yes

- RSTP stavy portov
  - Discarding (ako blocking/listening v STP)
    - Nepreposiela dátové rámce
  - Learning (ako v STP)
    - Buduje MAC tabuľky prepínača aby zbytočne nešíril neznáme unicastové rámce na všetky porty.
  - Forwarding (ako v STP)
    - Preposiela dátové rámce.

Zmena definície rolí portov

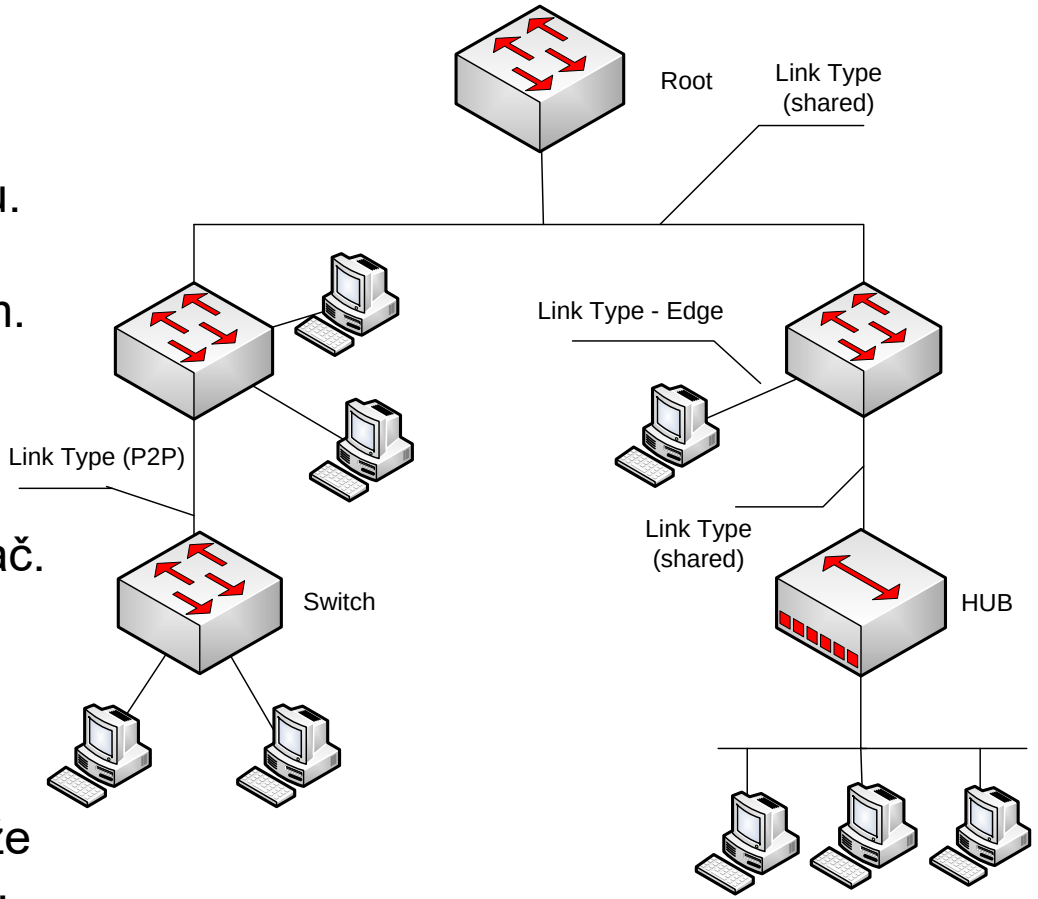
Rola portu	Popis
Root port	Port na každom nonroot prepínači, ktorý je vybratý ako najbližšia cesta k Root Bridge (RB). Na každom nonroot prepínači môže byť len jeden root port. Root port je v stave Forwarding v ustálenej aktívnej topológii.
Designated port	Každý segment má aspoň jeden designated port. V ustálenej aktívnej topológii, prepínač s portom designated prijíma rámce na segmente, ktoré sú určené pre RB. Designated port pracuje v stave Forwarding. Na non-RB len jeden per segment, ak viac prepínačov musí byť voľba.
Alternate port	Port prepínača, ktorý je alternatívnou cestou k RB. Alternate port je v stave discarding v ustálenej aktívnej topológii. Alternate port je prítomný na nondesignated prepínačoch a dovoľuje prechod na designated port ak aktuálny designated port zlyhá.
Backup port	Port na designated prepínači s redundantnou linkou do segmentu, kde je prepínač **Designated**. Backup port ma vyššie port ID ako designated port na designated prepínači. Backup port je v stave blocking v ustálenej aktívnej topológii.
Edge port	Port, na ktorom sa nepredpokladá pripojenie iného prepínača (len koncová stanica). Prechádza okamžite po aktivácii do Forward stavu. Odpovedá PortFast. Zmeny na ňom negenerujú Topo Changes. Objavenie PBDU – zmena na bežný port.

Zmena definície rolí portov oproti STP



Zmena typov liniek

- Typ linky predurčuje aktívnu úlohu v RSTP
- **Edge port**
  - Nepredpokladá sa. Že by mohol spraviť slučku.
  - Prechádza priamo do Forward stavu.
  - Pri príjme BPDU sa stáva bežným STP portom.
- **Non-Edge linky**:
  - **Point-to-point**:
    - Port pracuje v móde full-duplex. Predpokladá sa, že tento port bude pripojený na iný prepínač.
    - Môže prechádzať priamo do Forward
    - `spanning-tree link-type point-to-point`
  - **Shared Port:**
    - pracuje v móde half-duplex. Predpokladá sa, že tento port bude pripojený na zdieľané médium, na ktoré môže byť pripojených viacero prepínačov.
    - Musí prejsť celým STP procesom



BPDU v2 – Flag Byte využitie

- Posielané každé 2s.
  - Posiela každý prepínač (aj keď je root stratený), nielen ROOT
- Používa sa ako keepalive mechanizmus:
  - Tri chýbajúce BPDU = aging MAC tab. + indikácia zmeny topológie
- Bity 0 a 7 sú použité na TCN a na acknowledgement (ACK), ako v 802.1D
- Bity 1 a 6 sú používané na **proposal a agreement proces**
  - **Zrýchlenie konvergencie**
- Bity 2-5 enkódujú úlohy a stavy portov ktorým patrí BPDU

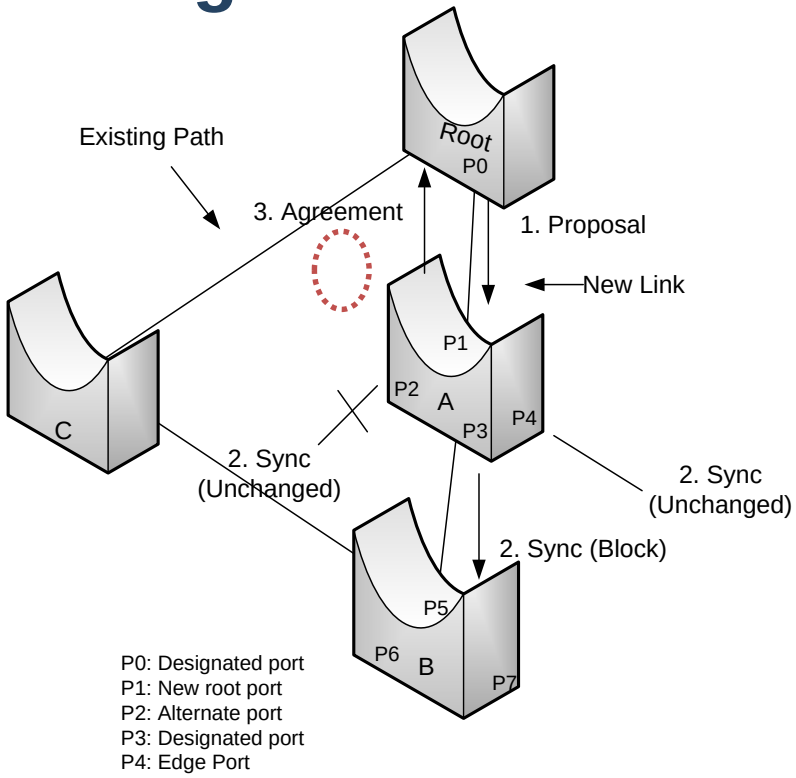
RSTP Version 2 BPDU

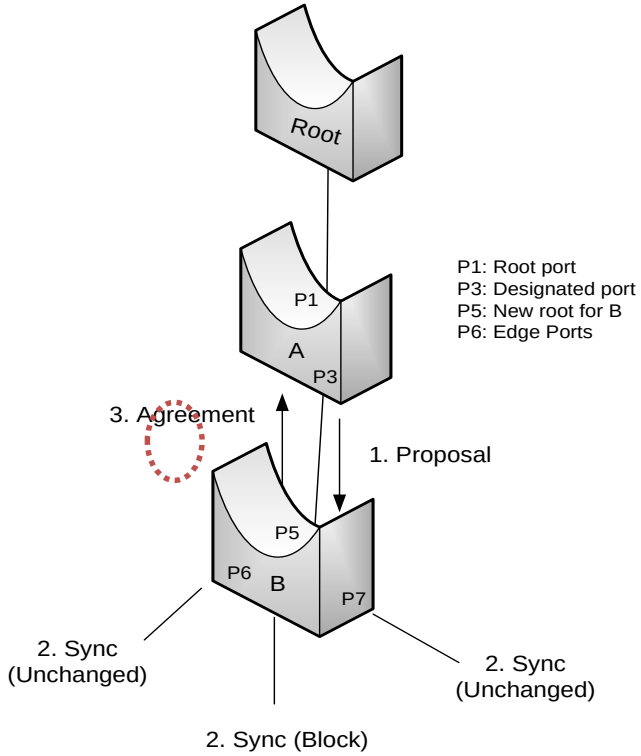
Field	Byte Length
Protocol ID=0x0000	2
Protocol Version ID=0x02	1
BPDU Type=0X02	1
Flags	1
Root ID	8
Root Path Cost	4
Bridge ID	8
Port ID	2
Message Age	2
Max Age	2
Hello Time	2
Forward Delay	2

Flag Field

Field Bit	Bit
Topology Change	0
Proposal	1
Port Role Unknown Port Alternate or Backup Port Root Port Designated Port	2-3 00 01 10 11
Learning	4
Forwarding	5
Agreement	6
Topology Change Acknowledgment	7

Zrýchlenie konvergencie – Propoposal / Agreement mechanizmus





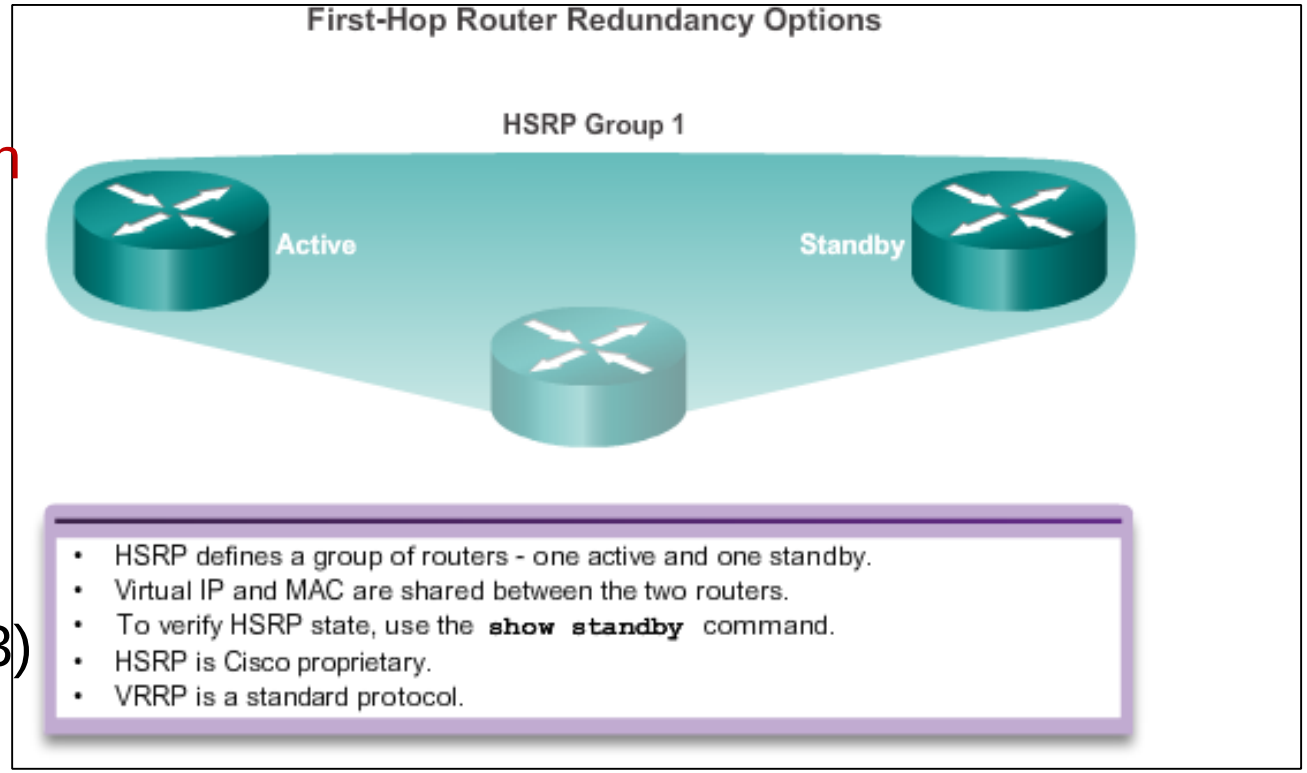
- Použitý vo fáze kedy **je designated port v discarding or learning stave**
  - Spôsobí urýchlenie konvergencie na link-by-link báze
- Možné len pre edge porty a point-to-point linky
- **Sync stav**
  - bloknuté všetky non-edge porty, aby sa predišlo slučke

Mechanizmy zálohovania brán

First Hop Redundancy Protocols

Riešenia pre FHRP

- ICMP Router Discovery Protocol (IRDP)
  - RFC1256, ICMP správy Router Advertisement + Router Solicitation
- Hot Standby Router Protocol (HSRP)
  - Cisco HSRP IPv4 (v1) aj IPv6 (v2)
- Virtual Router Redundancy Protocol version 2 (VRRPv2)
  - IETF riešenie, IPv4 (v2) aj IPv6 (v3)
- Gateway Load Balancing Protocol (GLBP)
  - Cisco GLBP for IPv6
  - Vylepšené funkcie oproti HSRP



Hot Standby Router Protocol (HSRP)

- HSRP poskytuje:
  - Zoskupovanie smerovačov do grúp tvoriacich virtuálny router
  - Redundanciu brán zdieľaním **virtuálnej IP** a **MAC adresy** medzi redundantnými routrami v grupe
    - Každý router má svoju reálnu IP a reálnu MAC adresu!!!!
  - Routre v grupe si nakonfigurované adresy prenášajú medzi sebou pomocou HSRP protokolu na Mcast adrese **224.0.0.2** s použitím UDP portu 1985 (HSRPv1) a 224.0.0.102/FF02::66 vo verzii3
    - Routre musia mať L2 vzájomnú konektivitu (tá istá LAN/VLAN)
- Koncové hosty sú nakonfigurované s **IP adresou Virtuálneho routra**
- Počet grúp
  - Od 0 po 255 (až 4096 vo verzii3)
  - Reálne na Catalyst 16
  - Grupa má len lokálny význam per interface

Hot Standby Router Protocol (HSRP)

- HSRP protokol definuje tzv. „*standby group*“, ktorá obsahuje:
  - Active router
    - Nositeľ identity virtuálneho routera (vMAC, vIP)
    - Je zodpovedný za obsluhu paketov posielaných na identitu virtuálneho smerovača
    - V HSRP grupe je vždy iba jeden Active router
      - Buď prvý nabbotovaný, alebo pri preempcii sten s najvyššou prioritou
  - Standby router
    - Záložný router pre Active (podobne ako DR a BDR v OSPF)
    - Ak Active router prestane pracovať, Standby router preberie na seba vMAC a vIP
    - V HSRP grupe je vždy najviac jeden Standby router
      - Buď druhý nabootovaný alebo s druhoy najvyššou prioritou
  - Other routers
    - Ostatné smerovače v HSRP grupe, ktoré nie sú ani Active ani Standby. Monitorujú dostupnosť Active a Standby routerov.
      V prípade potreby vedia prejsť do roly Standby a následne Active.
  - Virtual router
    - Celá standby group v vIP a vMAC
- ***Preemption*** je schopnosť iného routera prevziať na seba úlohu Active routera, aj keď aktuálny Active stále žije, avšak jeho priorita je menšia než priorita na Standby
  - Štandardne je preempcia vypnutá, v takej situácii Standby preberie na seba úlohu Active len vtedy, keď Active úplne odíde

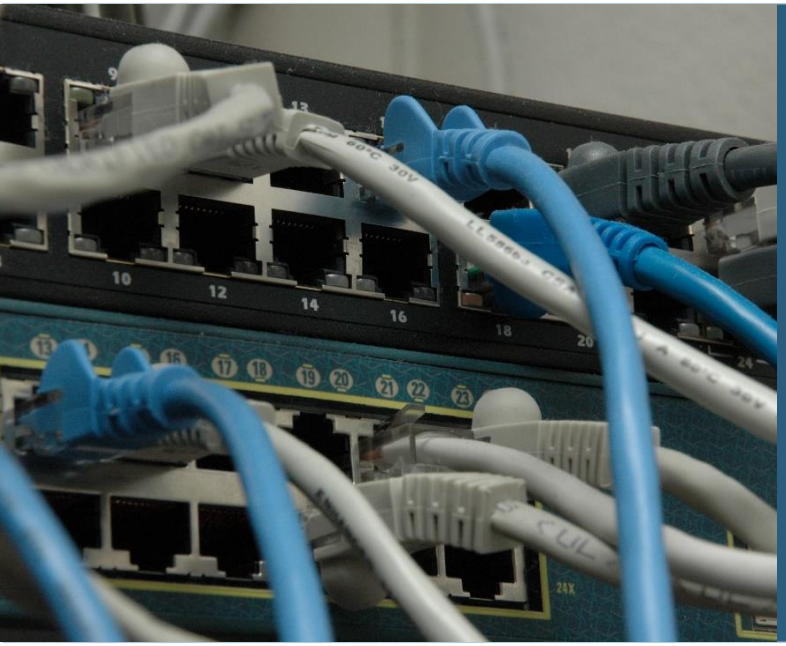
HSRP troubleshooting

- Väčšina chýb sa týka:
  - Nefungujúca konektivita medzi Active/Standby
    - Následok
      - Obaja sú Active
      - Problém s trackovním stavu
  - Nefungujúca voľba Active
    - Zistiť prioritu a zapnutie „preempt“
- Riešenie
  - Over konektivitu
  - Over správnosť konfigurácie (konfigurácia rovnakého rozhrania, rovnaká vIP, vhodné a nerovnaké logické IP adresy s toho istého segmentu, rovnaké číslo HSRP grupy)

- Riešenie:
  - `Debug standby packets`
  - `Debug standby packets terse`

Iné riešenia

- VRRP
  - Štandardizovaná IETF RFC 2338 alternatíva k HSRP (Cisco™)
  - VRR Group (na routri je možných až 255 grúp)
    - Reprezentovaná virtuálnou IP a MAC adresou
    - Jeden **Virtual Master** router (v HSRP Active)
      - Môže mať takú istú reálnu IP ako sa použije **virtuálna** – vtedy vyhráva voľbu na Master ten router, ktorého IP je použitá ako virtuálna
        - Priority 255 (def. 100, vyčlenenie z voľby 0)
      - Ak sa používa len virtuálna IP
        - Prebieha voľba na základe priority
      - MAC adresa virtual routra je **0000.5e00.01*xx*,** kde *xx* je dvojčíselné hexa číslo VRRP grupy
    - Jeden alebo viac **backup routrov** (v HSRP jeden Standby, zvyšok Listen)
- GLBP
  - Vylepšenie HSRP a VRRP o lepší manažment zdrojov neaktívnych routrov v grupe
    - Ak chcem dosiahnúť lepšie vyťaženie viacerých routrov pri HSRP a VRRP = manuálna konfigurácia load balance
    - napr. rozložením Active routrov pre viaceré virtual IP
  - GLBP umožňuje
    - Použitie viacerých "*Forwarders*"(GW) paralelne na smerovanie dát
    - Automatický výber GW
    - Automatický failover medzi použitými GW
    - Ľahšia konfigurácia využitia zdrojov ako pri HSRP a VRRP
    - Load sharing lepší ako pri HSRP a VRRP
      - Redundantné linky využívané paralelne
      - HSRP a VRRP používajú na smerovanie len jeden z uplinkov,
      - ostatné nevyužité kým sa nepoužije nejaká Load Balance finta

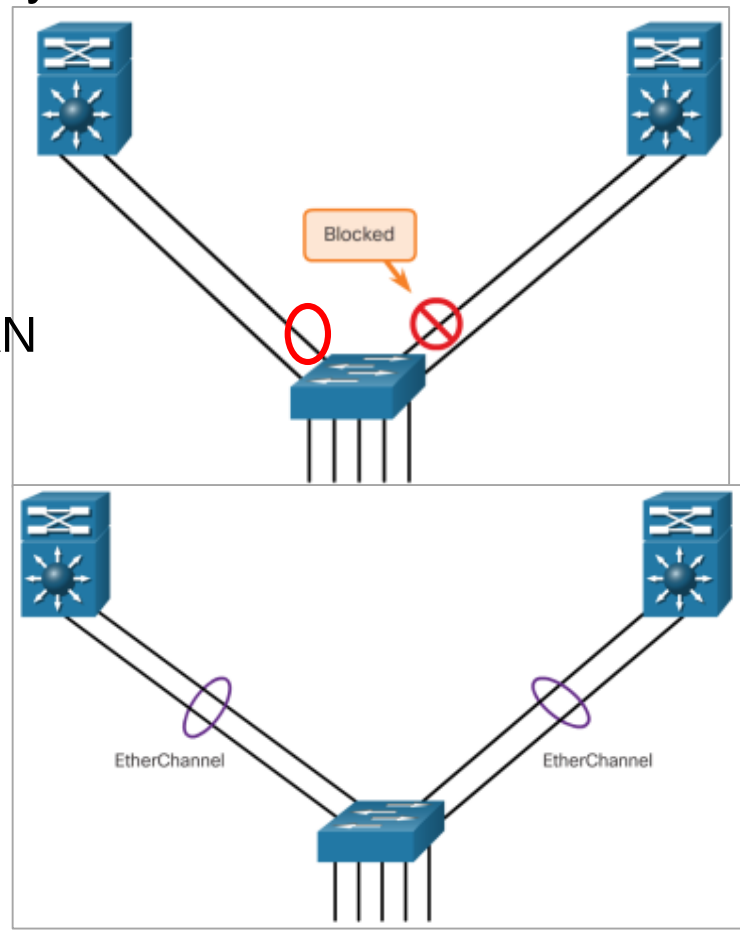


Agregácia liniek

Link aggregation, Etherchannel, ChannelBonding
apod.

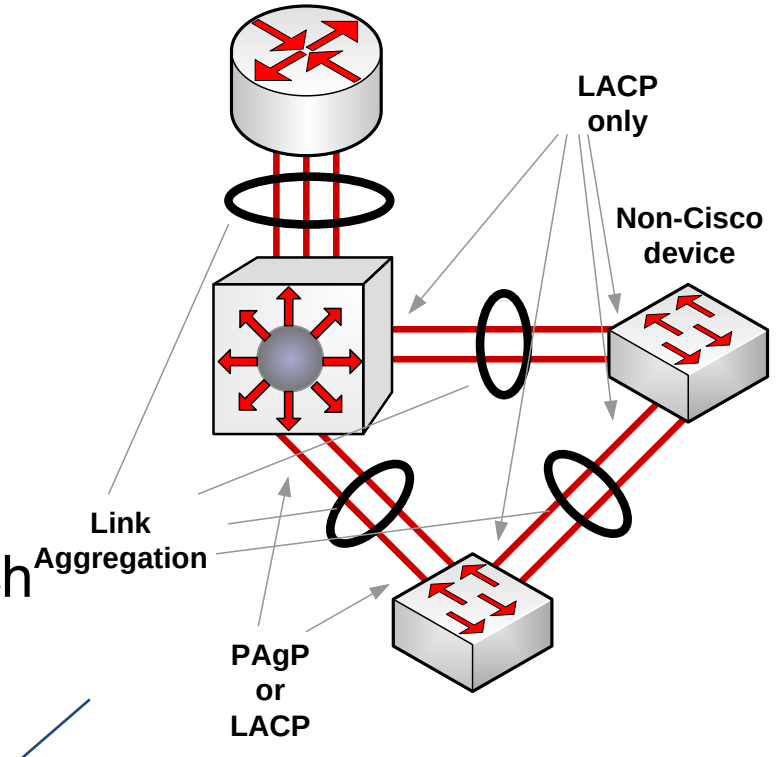
Link Aggregation cez EtherChannel

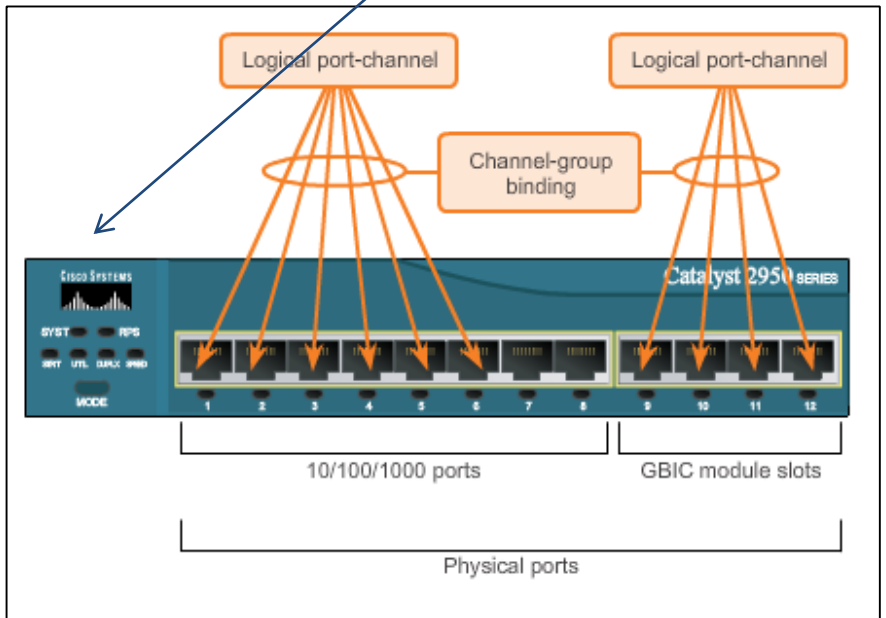
- Technológia umožňujúca **logicky zgrupovať** fyzické prepínané porty do niekoľkonásobne výkonnejšieho prenosového kanála
- Poskytuje väčšiu priepustnosť
  - Vytvára logické porty vysokých rýchlostí
  - Switch-switch, switch-router, switch-server
  - Môžem združovať od 2 do 8 fyzických portov do jedného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



Implementácie agregácie linky

- EtherChannel využíva podporný signalizačný protokol na zostavenie združených kanálov
  - Overenie, či všetky linky idú k tomu istému zariadeniu
  - Overenie, či na susednom zariadení sú porty združené
  - Overenie, či schopnosti a vlastnosti portov dovoľujú z nich vytvoriť spoločný kanál
- **PAgP** (Port Aggregation Protocol):
  - Cisco proprietárny
  - Správy každých 30s
- **LACP** (Link Aggregation Protocol):
  - IEEE štandard 802.3ad
- Oba protokoly sú rovnocenné
  - avšak nie kompatibilné





EtherChannel PAgP a LACP módy

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

Nastavenia režimov

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

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

Podmienky na vytvorenie EtherChannel

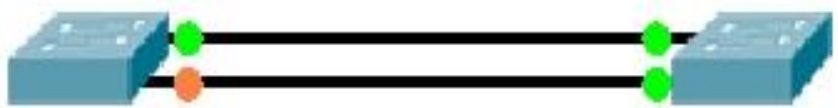
- Vytvorenie EtherChannel má nasledujúce obmedzenia pre porty, ktoré ho budú tvoriť:
  - Všetky porty rovnakú rýchlosť
  - Všetky porty rovnaký duplex
  - EtherChannel sa nevytvorí ak jeden z portov je SPAN (switched port analyzer)
  - Všetky porty priradené do rovnakých VLAN or musia byť trunk
  - Ak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

Distribúcia prevádzky nad Etherchannel – Load Balance

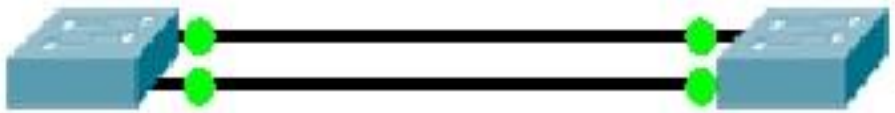
- EtherChannel nedistribuuje rámce na princípe round-robin obsluhy
  - Riziko doručenia rámcov v nepôvodnom poradí
- Používa niektorú distribučnú politiku (závislú od platformy a používateľa)
- Load balancing môže byť založené na nasledujúcich kritériách:
  - src-mac: Source MAC address
  - dst-mac: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

EtherChannel a Spanning-tree

- Dve redundantné linky bez EtherChannel-u
  - len jedna linka je FWD, ostatné bloknuté



- EtherChannel linka je STP vnímaná ako jedna linka
  - Všetky fyzické porty môžu pracovať a nie sú blokované STP



Odporúčania pre konfiguráciu a troubleshooting

- Všetky rozhrania by mali mať rovnaké parametre a konfiguráciu
- Odporúča sa využiť najprv dynamickú negociáciu založenia cez LACP/PAGP
  - LACP preferované – IEEE štandard
- A potom spraviť statickú konfiguráciu
- Ak sa robia zmeny, je dobré zhodiť port-channel, vykonať zmeny a potom nahodiť
- Poučenie z cvičení
  - Ak padne portchannel do errdisable or je down (typicky problém s STP)
  - Odstrániť konfiguráciu a začať nanovo

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť!

Ohodnoť našu CNA na google:

- https://goo.gl/maps/BAnFvQKYCBpffcEX7

Vytvorené v rámci projektu KEGA 011STU - 4/2017.