



Virtuálne LAN siete, smerovanie medzi nimi a ich škálovanie (VTP, DTP, extended VLAN, L3 prepínanie)

PS1 – prednáška 4 (RSE kapitola 6, SN kapitola 2)

Katedra informačných sietí
FRI, UNIZA



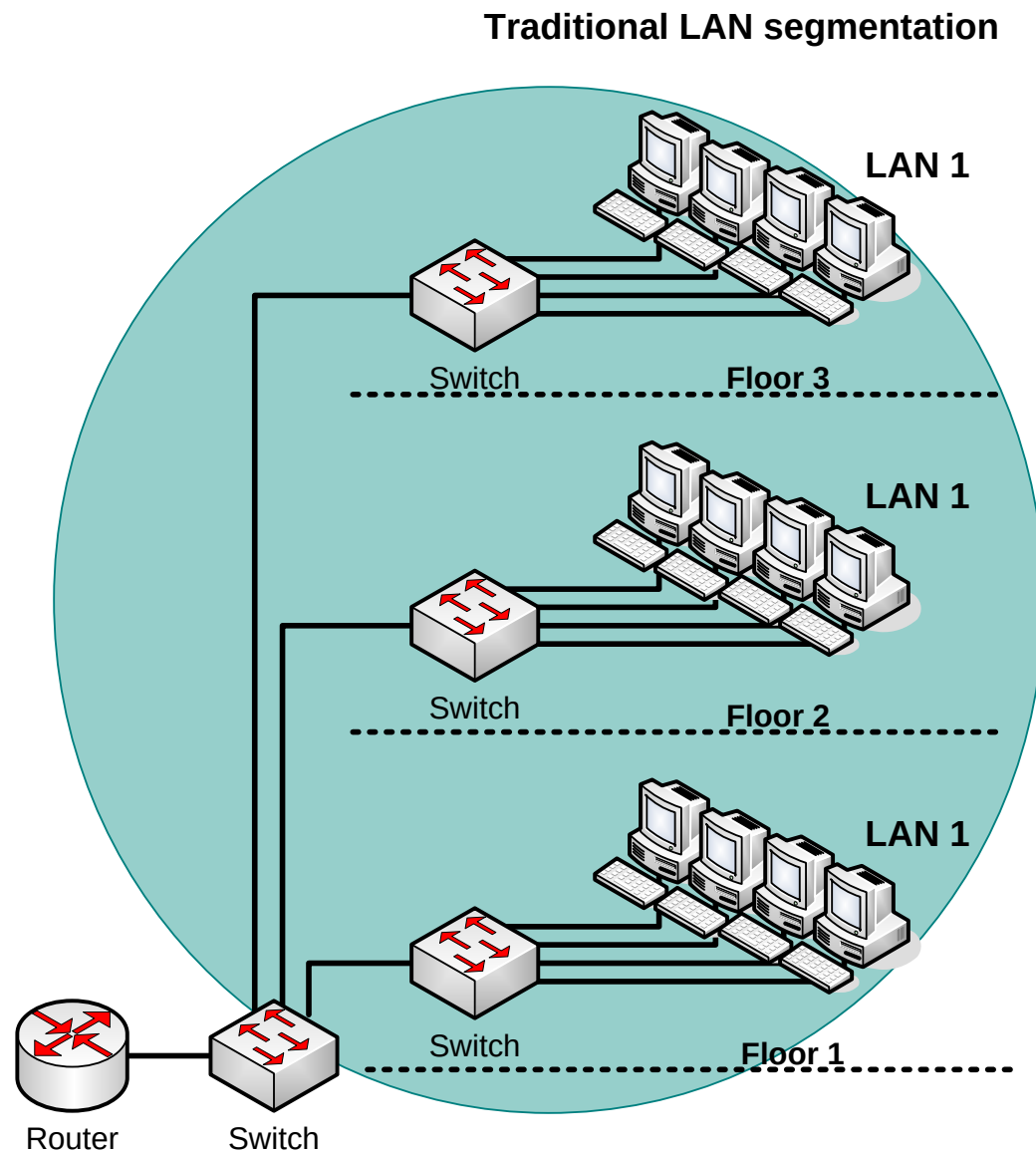
Úvod do VLAN sietí a trunkingu

RSE kapitola 6: VLANs a interVLAN routing

Motivácia pre virtuálne LAN siete

Situácia z praxe:

- V budove je zapojená štruktúrovaná kabeláž, každá miestnosť má niekoľko zásuviek
- Všetky zásuvky sú vyvedené do spojovacích panelov v rozvádzačoch
- Je potrebné vytvoriť nezávislé siete pre:
 - Vedenie podniku
 - Pracovníkov podniku
 - Hostí



Motivácia pre virtuálne LAN siete

Riešenie 1:

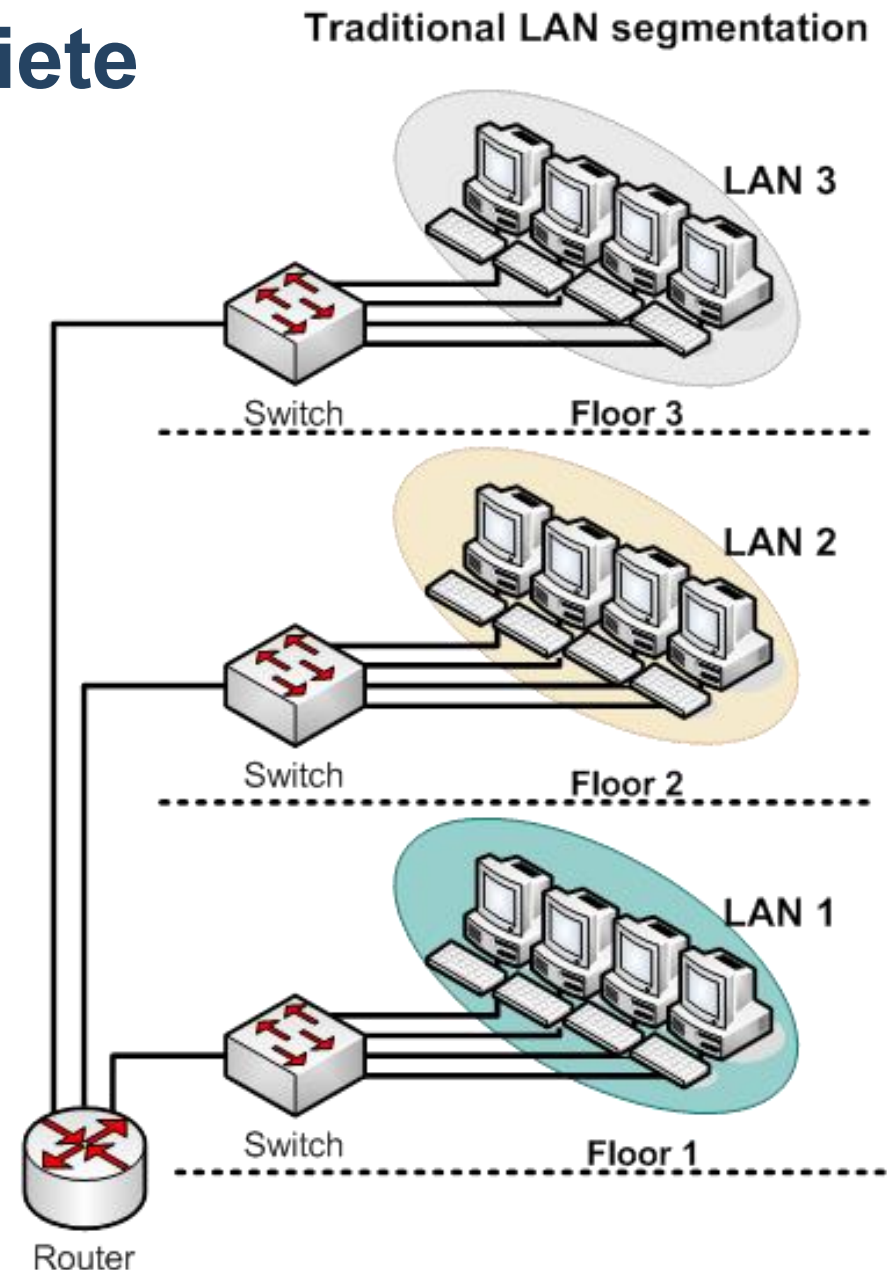
- Zapojiť zásuvky do samostatných prepínačov tak, aby každá sieť mala vlastný prepínač
- Prepínače podľa potreby prepojiť so smerovačmi

+ Výhody:

- Fyzická nezávislosť
- Každá sieť má vlastnú nezdieľanú prenosovú kapacitu

- Nevýhody:

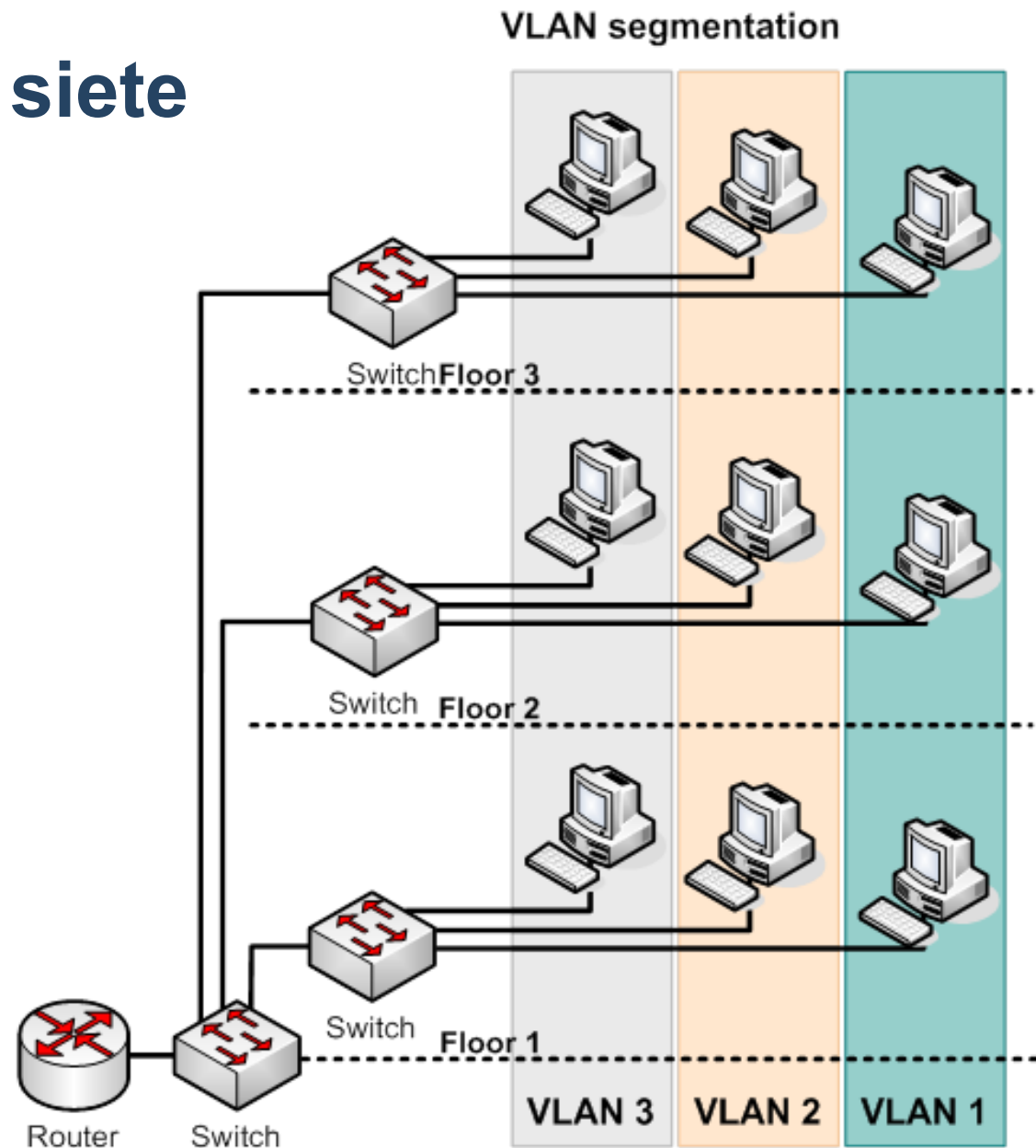
- Neefektívne využitie zdrojov
- Malá operatívnosť pri zmenách



Motivácia pre virtuálne LAN siete

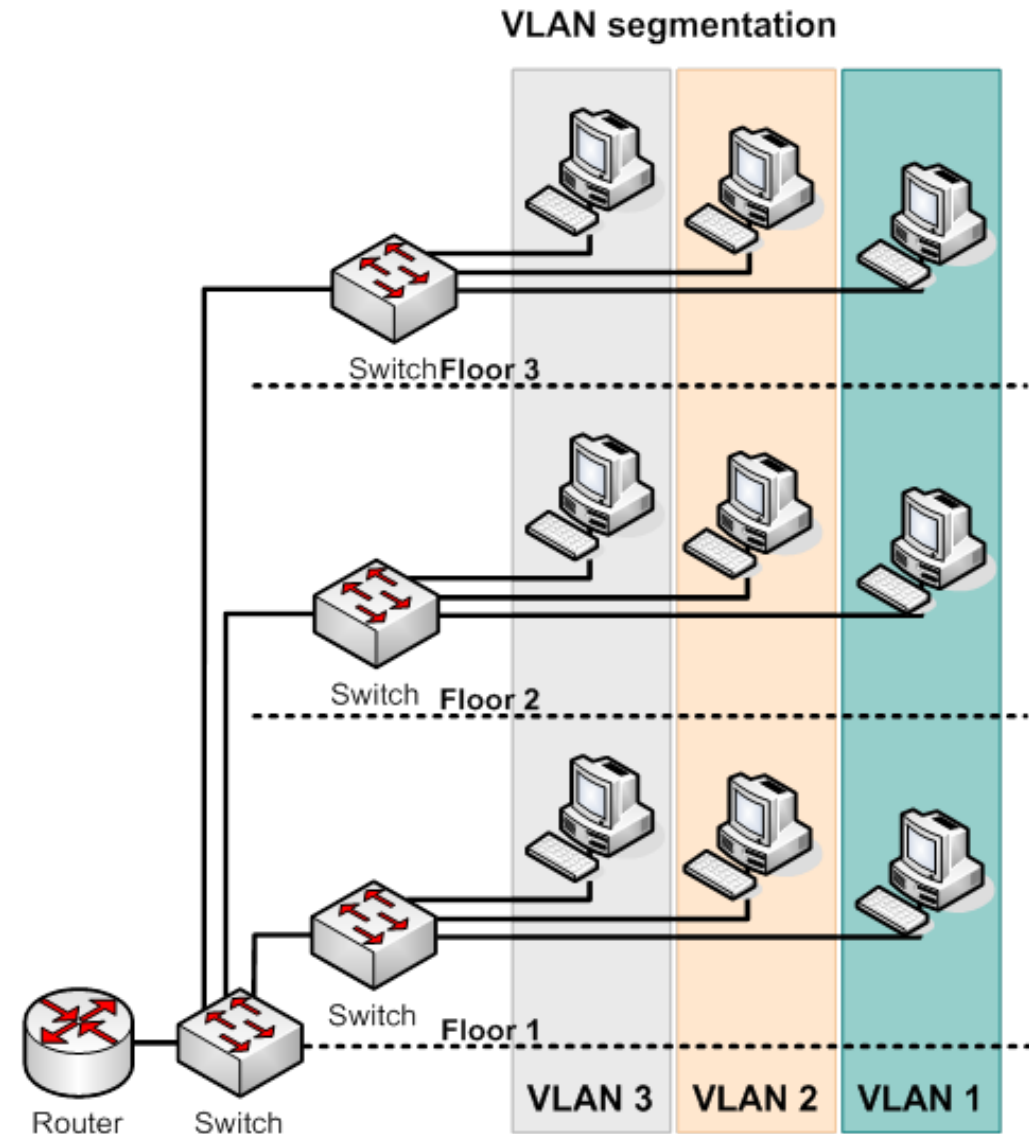
Riešenie 2:

- Zapojiť všetky zásuvky do spoločného prepínača
 - Porty prepínača konfiguračne zadeliť do samostatných izolovaných skupín, tzv. virtuálnych LAN
 - Podľa potreby zriadiť smerovanie medzi týmito skupinami
- Nevýhody:
- Porucha jedného prepínača sa môže dotknúť viacerých skupín
 - Kapacita prepínačov sa delí medzi všetky skupiny
- + Výhody:
- Množstvo, odhalíme neskôr ☺

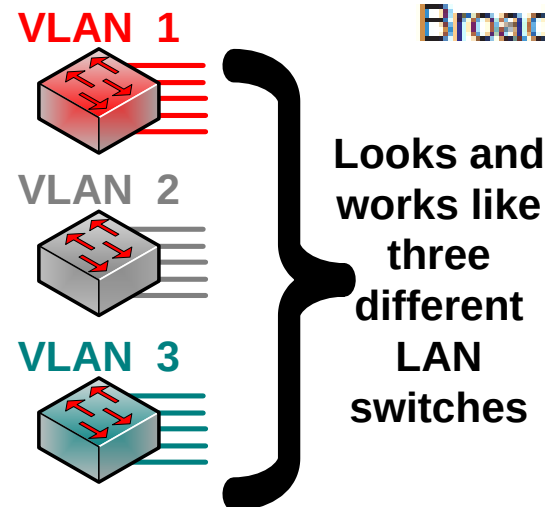
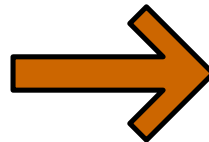
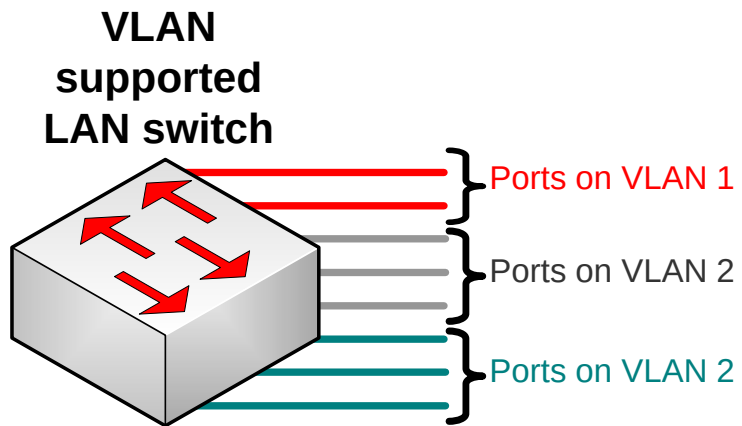
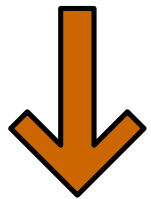
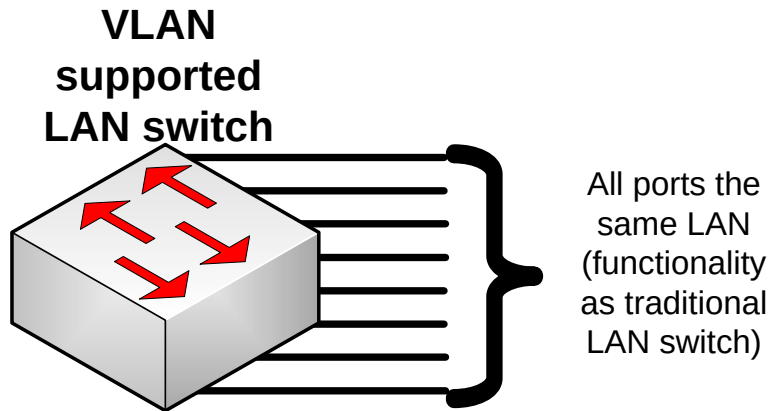


Ethernet – Virtuálne LAN

- Virtuálna LAN (VLAN) je nezávislá izolovaná broadcastová doména vytvorená logikou prepínača
 - Skupina portov, ktoré smú medzi sebou komunikovať bežným prepínaným spôsobom
 - Rámec prijatý v istej VLAN môže byť odoslaný iba iným portom v tej istej VLAN
 - Porty v rôznych VLAN od seba prepínač úplne izoluje
 - Fyzická LAN a VLAN sú z pohľadu koncových staníc nerozlíšiteľné
 - 1 VLAN $\approx$ 1 IP sieť



Princíp VLAN



Prepínacia tabuľka (CAM)

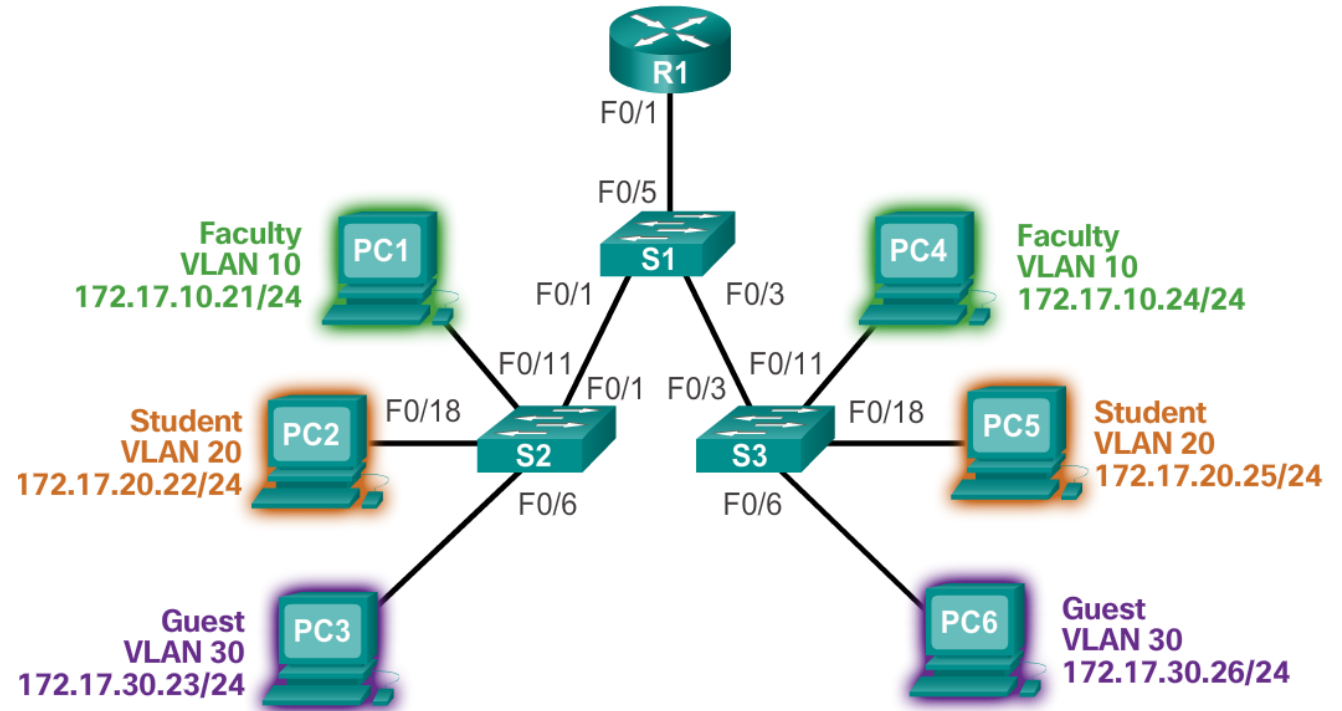
Forwarding Table

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

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

Výhody použitia VLAN

- Nesporná flexibilita
 - Jednoduché premiestňovanie staníc medzi VLAN
 - Jednoduché pridávanie staníc do konkrétnych VLAN
 - Jednoduchá zmena konfigurácie VLAN
- Predpoklady pre vyššiu bezpečnosť
 - Izolácia prevádzky vo VLAN
 - Jednu veľkú broadcastovú doménu rozbijem na viac menších
 - Lepšia kontrola nad komunikáciou
 - Použitie smerovačov
- Šetrenie finančných prostriedkov na infraštruktúru
 - Lepšie využitie prostriedkov prepínačov



Typy VLAN sietí podľa členstva staníc

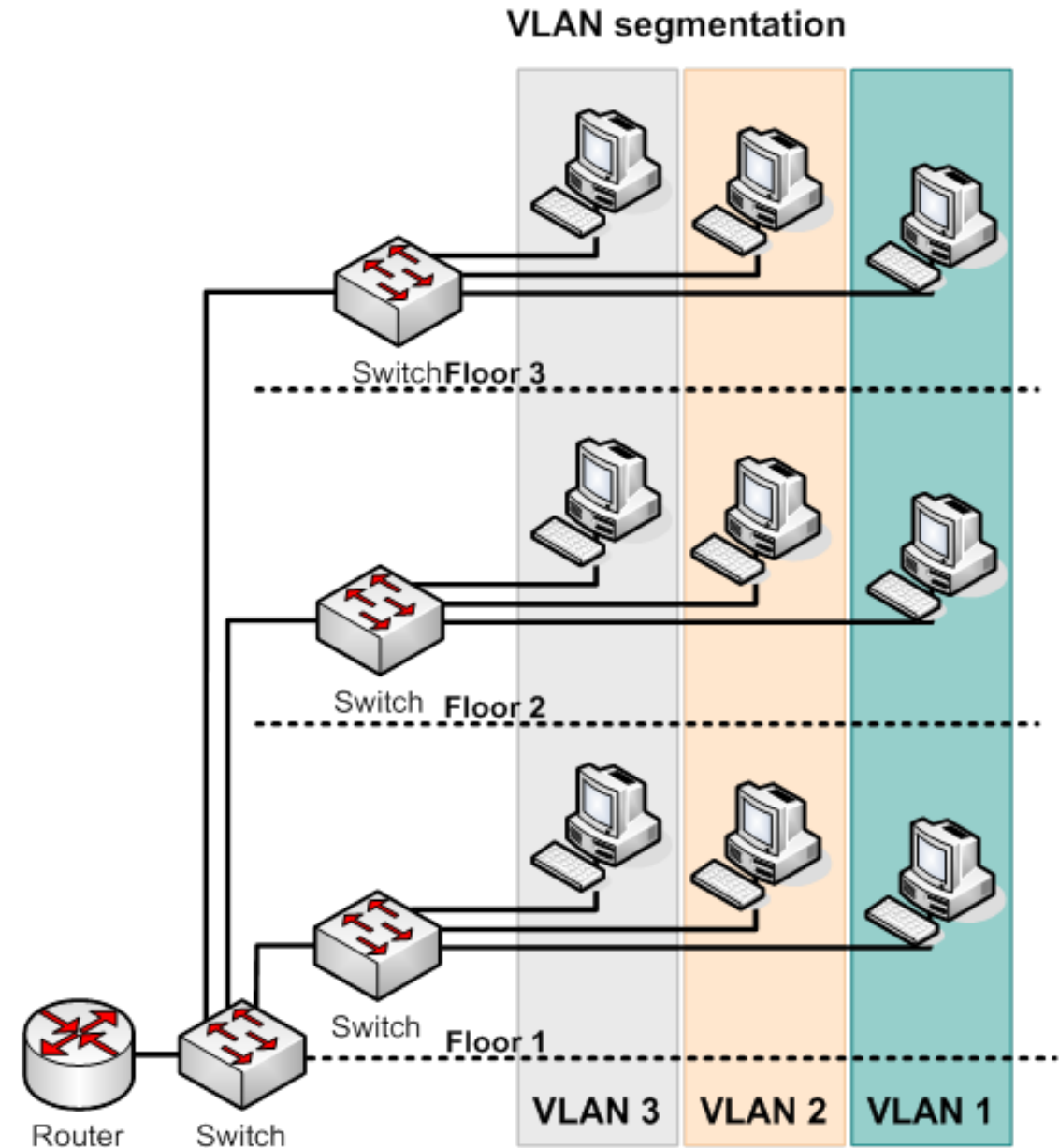
- V praxi existuje niekoľko spôsobov, ktorými sa určuje členstvo staníc vo VLAN
 - Port je staticky konfiguračne priradený do práve jednej konkrétnej VLAN (tzv. **port-based VLANs**)
 - Takýto port sa zvykne nazývať **prístupový (access) port**
 - V súčasnosti najbežnejší spôsob implementácie VLAN sietí
 - Existujú mechanizmy, ktoré na základe zdrojovej MAC adresy rámca alebo autentifikácie používateľa dynamicky zaradia port do istej VLAN
 - Tieto mechanizmy umožňujú používateľovi byť vždy vo svojej domácej VLAN, i keď sa presúva medzi portmi prepínača
 - Členstvo vo VLAN sa dynamicky určuje pre každý rámec individuálne podľa MAC adresy odosielateľa
 - Členstvo vo VLAN sa dynamicky určuje pre každý rámec individuálne podľa obsahu rámca (tzv. **protocol-based VLANs**)

Interná práca prepínača s VLAN

- Implementovanie podpory port-based VLAN z pohľadu logiky switcha je relatívne jednoduché
 - Každá VLAN dostane pri konfigurácii svoje unikátne **číslo**
 - CAM tabuľka (Content Addressable Memory – obvod prepínača ukladajúci MAC adresy) sa rozšíri o stĺpec s číslom **VLAN**
 - Riadok CAM tabuľky bude teda obsahovať informácie v tvare
<VLAN> | <MAC> | <Port>
- Rámec vchádzajúci istým portom bude spracovaný takto:
 - Ak je jeho source 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
 - Ak je **príjemca neznámy** (unknown unicast, m-cast, b-cast), tak čo?
 - rámec bude odoslaný všetkými ostatnými portmi v tej istej VLAN

Motivácia pre trunking

- Predstavme si teraz:
 - Každé poschodie budovy má vlastný prepínač
 - Na každom poschodí sú aj zamestnanci, aj potenciálni hostia s prístupom k sieti
 - Na prepínačoch sú vytvorené príslušné VLAN
 - Ako ich prepojiť, aby napr. VLAN pre host'ov bola súvislá, ale „nepretiekla“ do iných VLAN?



Motivácia pre trunking

- **Riešenie 1:**

- Na každom prepínači vyhradiť v každej VLAN porty na prepojenie s ďalšími prepínačmi
 - Ako by to vyzeralo?

- **Zjavné nevýhody:**

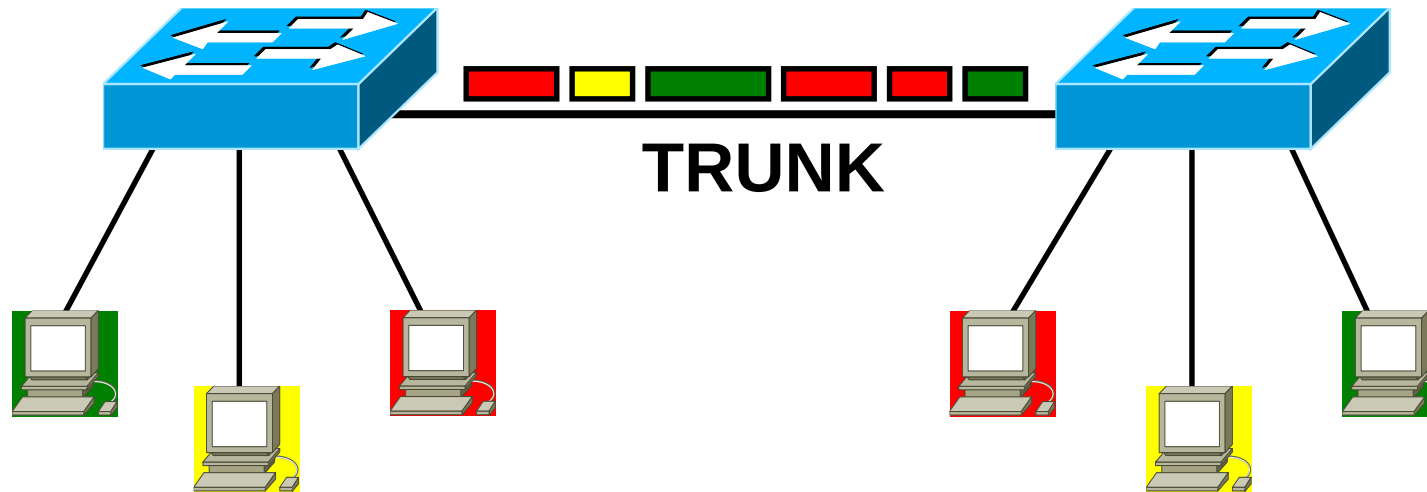
- Je potrebné rezervovať veľké množstvo portov na každom prepínači, veľký počet prepojovacích káblov
- Pri veľkom množstve VLAN a susedných prepínačov nepraktické až nerealizovateľné

Trunking vo VLAN

■ Riešenie 2:

- 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 značkovat'
- 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

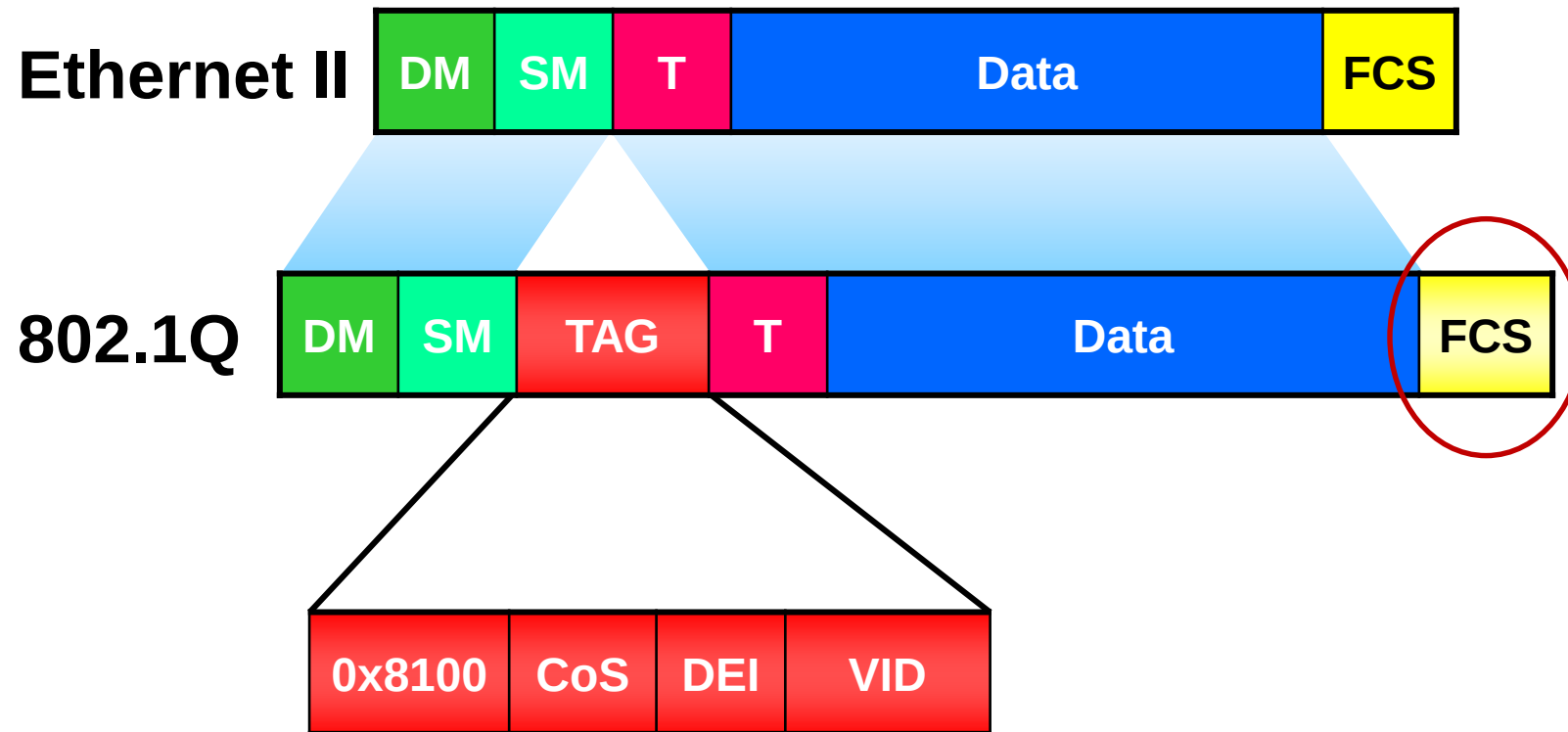
- Existuje niekoľko spôsobov označovania, do akej VLAN rámec prenášaný trunkovým prepojom patrí
- **ISL (Inter-Switch Link)**
 - Proprietárny protokol spoločnosti **Cisco**
 - Rámce prechádzajúce trunk prepojom sa zabalia do nového rámca s prídavnou hlavičkou s informáciou o VLAN
 - Celý pôvodný rámec 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

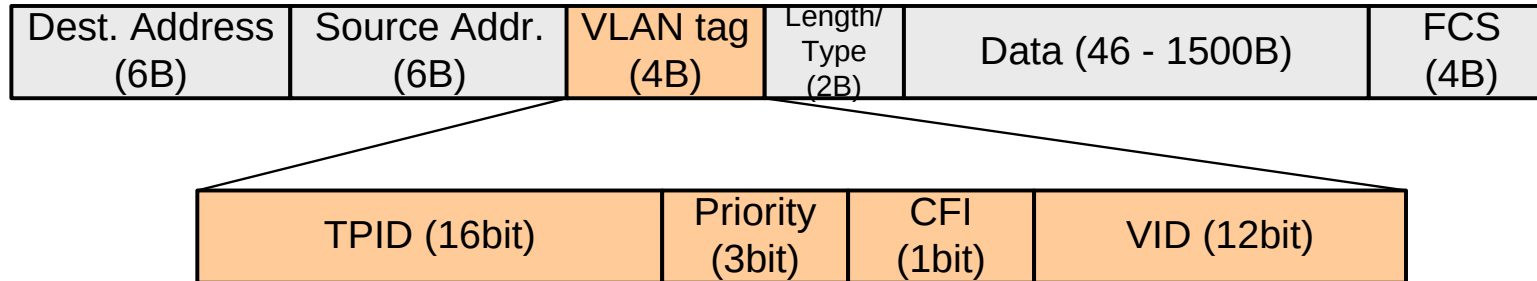
- **IEEE 802.1Q**

- **Otvorený** štandard, široko podporovaný výrobcami sieťových zariadení aj operačných systémov
- Zachováva **základnú** štruktúru ethernetového rámca
 - Značkový 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

Značkovanie rámcov podľa 802.1Q

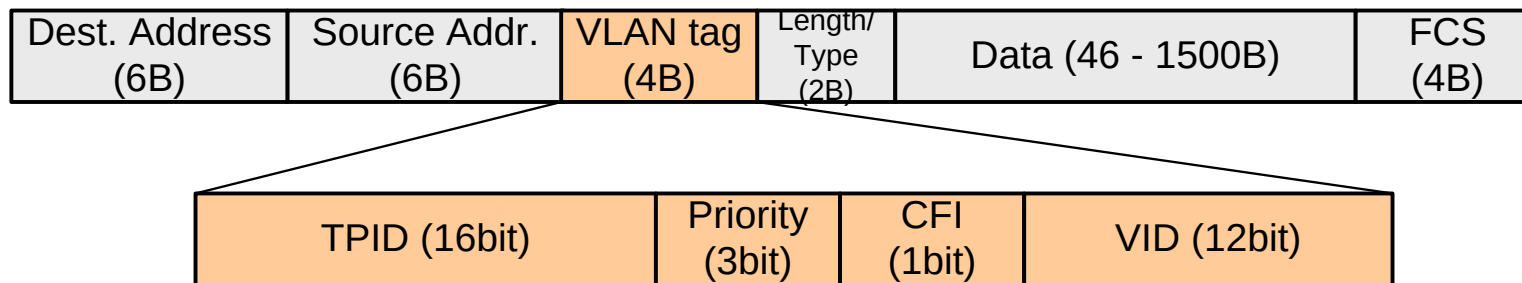


Formát značky 802.1Q



- **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

Formát značky 802.1Q

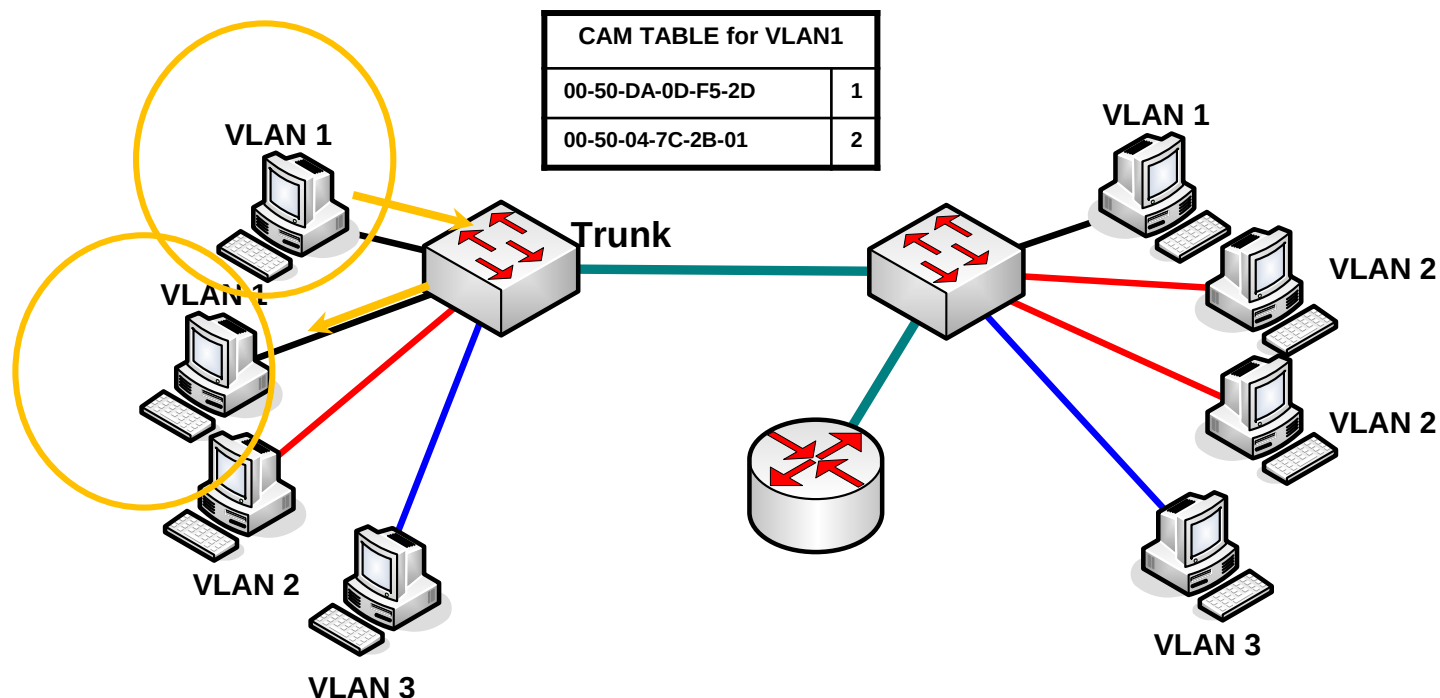


- **CFI (Canonical Format Indicator):** 1 bit
 - Používané len v non-Ethernet sieťach (Token Ring)
 - Vyjadruje, či adresy v rámci sú/nie sú v tzv. kanonickom formáte (poradie bitov v bajte od Least Significant bit po Most Significant bit)
 - 802.1Q-2011 predefinoval CFI na **Discard Eligible Indicator** (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)

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 rámci 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

802.1Q – Intra VLAN komunikácia



Príklad:

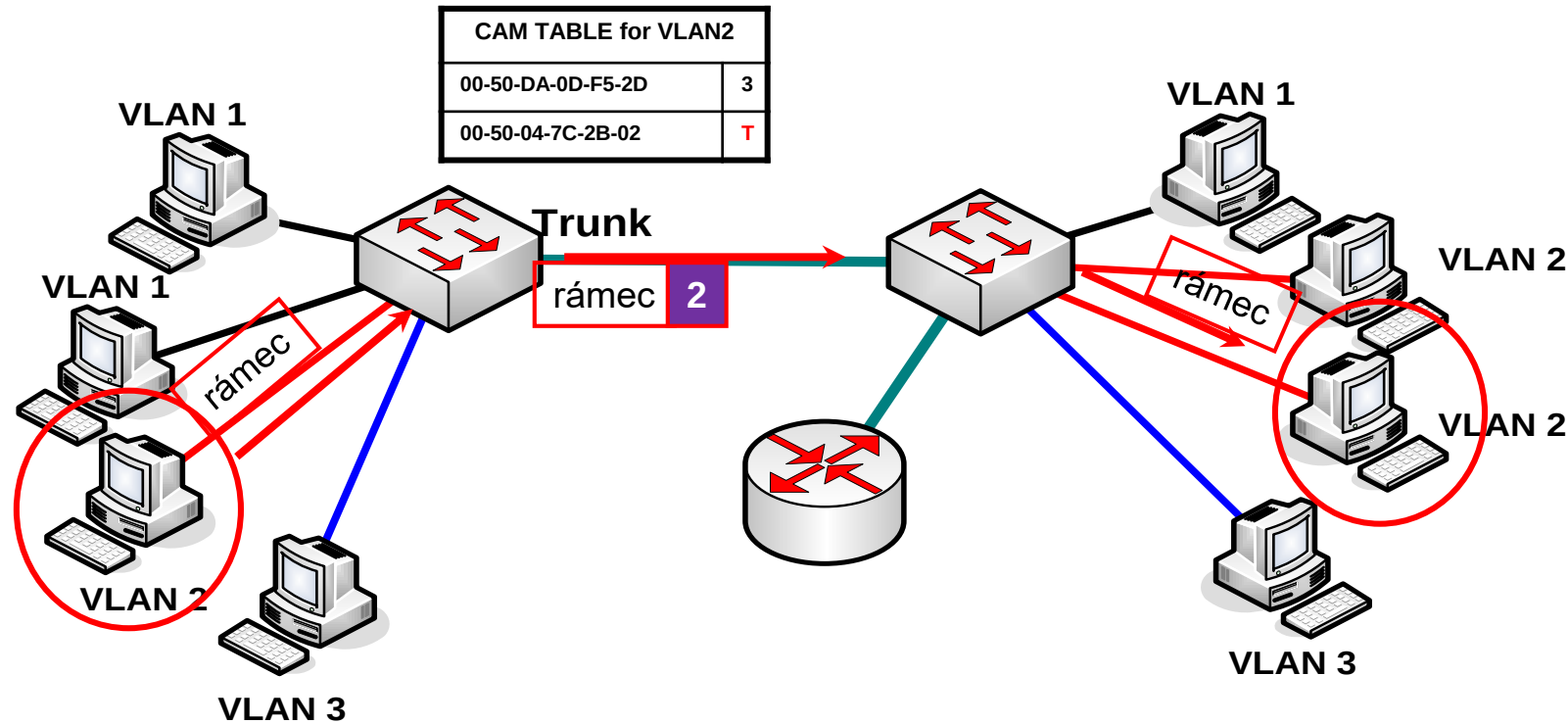
Komunikácia medzi stanicami vo vnútri VLAN (Intra VLAN) na tom istom prepínači

Prepínač prijme rámec na prístupovom porte (**access port**)
Prezrie CAM tabuľku pre VLAN 1
Prepne rámec na výstupný port

Rámec nie je pozmenený (značkový), lebo neprechádza trunk portom!

Rámec je prepnutý ako na bežnom prepínači

802.1Q – Intra VLAN komunikácia



Príklad:

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

Prepínač prijme rámec na prístupovom porte (**access port**)

Prezrie CAM tabuľku pre VLAN 2

Rámec musí byť prepnutý cez trunk

Vloží tag identifikujúci, že rámec je pre VLAN 2

Prepne rámec na trunk port

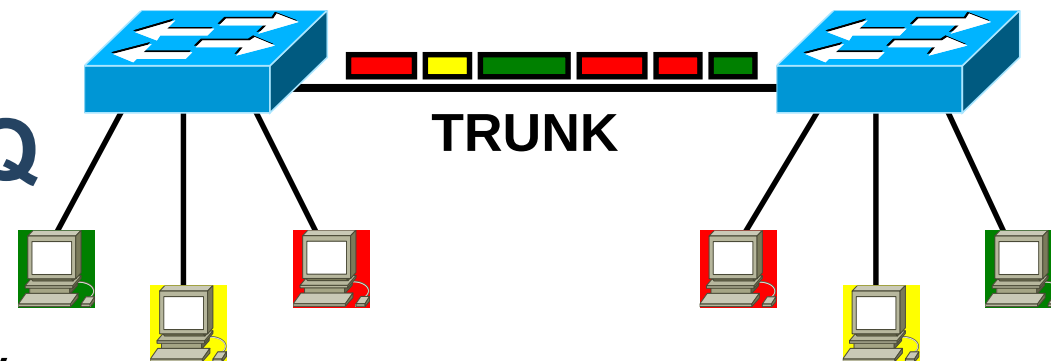
Prijímajúci prepínač prijme rámec

Prezrie CAM tabuľku

Ak cieľová stanica je na jeho porte, odstráni tag a prepne rámec

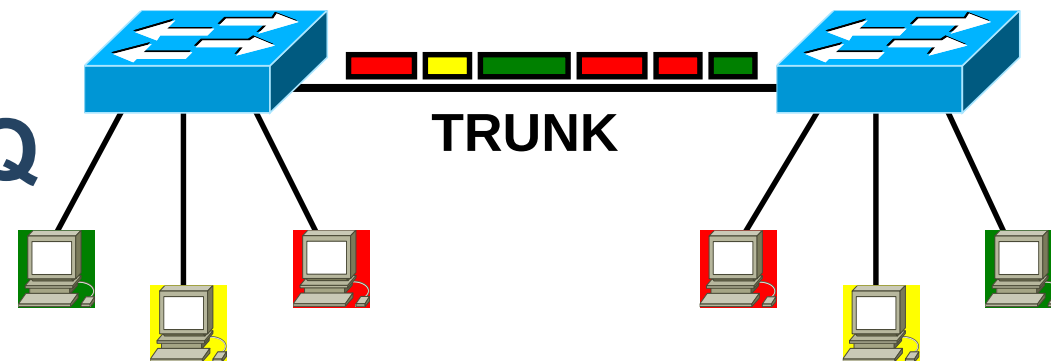
Rámec je pri prechode trunkom označovaný

Koncept natívnej VLAN v 802.1Q



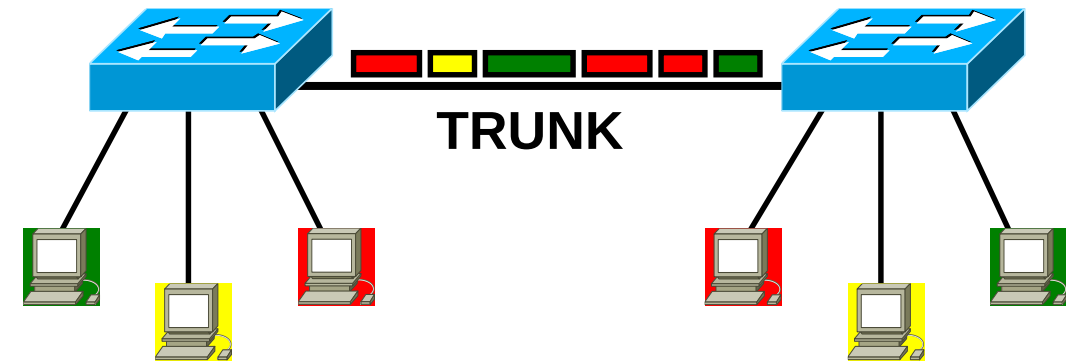
- Na trunk portoch sa teda predpokladá odosielanie a príjem značkových rámcov
- Čo však, ak na trunk port dorazí rámec bez značky?
 - Evidentne sú dve možnosti: rámec zahodiť alebo zaradiť do nejakej „VLAN poslednej možnosti“
 - V IEEE sa rozhodli použiť druhú možnosť
- Každý trunk port v 802.1Q má definovanú tzv. **natívnu VLAN**
 - Natívna VLAN je VLAN, ktorá ako jediná na trunk portoch **nebude** používať **značky**
 - Ak rámec patrí do natívnej VLAN trunk portu, ktorým má odísť, pri odoslaní značku nedostane
 - Ak rámec prijatý na trunk porte neobsahuje značku, bude zaradený do natívnej VLAN tohto portu

Koncept natívnej VLAN v 802.1Q



- Rôzne trunk porty na tom istom prepínači môžu mať nastavené rôzne natívne VLAN
 - Poväčšine to nie je dobrý nápad, ale technicky je to prípustné
- Vzájomne prepojené trunk porty **musia** mať nastavené zhodné natívne VLAN
 - Ak by natívne VLAN na oboch koncoch trunk prepoja boli rôzne, obe natívne VLAN by sa zliali do jednej
- Na väčšine prepínačov je výrobcom prednastavená VLAN 1 ako natívna VLAN
 - Niektorí výrobcovia nepoužívajú pojem „native VLAN“, ale napr. „untagged VLAN“ alebo „primary VLAN ID“

Prenos rámcov v 802.1Q VLAN



- Pozrime sa teraz detailne na proces pridávania a odoberania značky v 802.1Q VLAN sieti
- Sú 4 kombinácie možností doručenia rámca

Vstupný port	Výstupný port
prístupový	prístupový
prístupový	trunk
trunk	prístupový
trunk	trunk

- Výsledný proces je daný kombináciou činností pri prijatí a odoslaní rámca
 - Pri prijatí sa rámec musí zaradiť do vhodnej VLAN
 - Pri odoslaní musí rámec byť označovaný alebo odznačovaný podľa typu výstupného portu a podľa natívnej VLAN

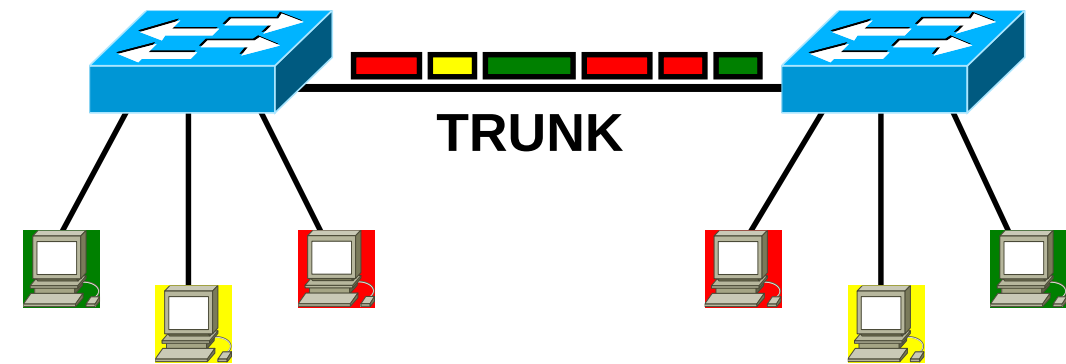
Prijatie rámca

Ak je **vstupný** port **prístupový**, potom...

- Akceptované budú len platné rámce
 - Bez značky
 - Alebo so značkou, kde VID=0
 - Alebo so značkou s rovnakou hodnotou VID, do ktorej je zaradený port
- Rámec bude vždy doručovaný vo VLAN, do ktorej je zaradený port. Predchádzajúci krok je „sanity check“ obsahu rámcov

Ak je **vstupný** port **trunk**, potom...

- Akceptované budú platné rámce so značkou i bez nej
- Rámce bez značky a rámce so značkou s hodnotou VID=0 budú doručované v natívnej VLAN definovanej na porte
- Rámce s ostatnými hodnotami značiek budú spracované vo VLAN podľa hodnoty VID v značke



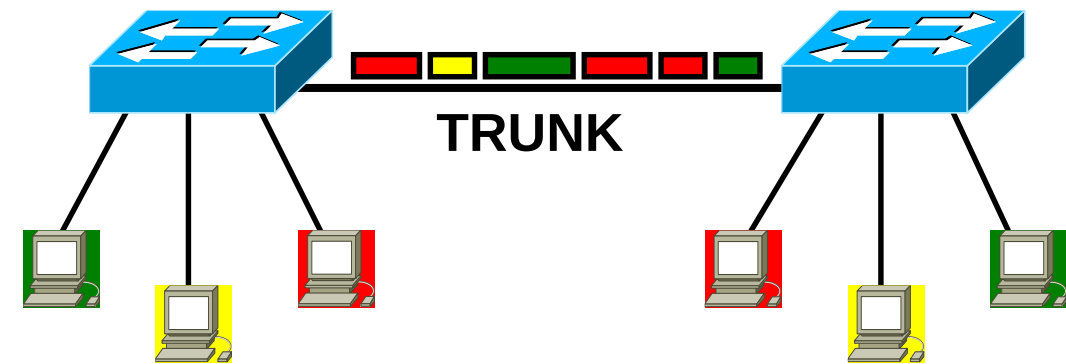
Odoslanie rámca

Ak je **výstupný** port **prístupový**, potom odchádzajúci rámec nemá mať značku

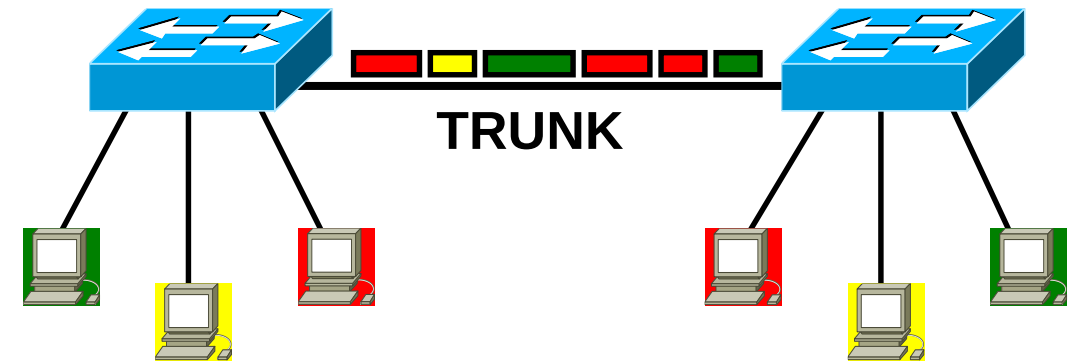
- Ak rámec pri prijatí značku mal, prepínač ju pred odoslaním odstráni
- Ak rámec pri prijatí značku nemal, prepínač značku nepridá

Ak je **výstupný** port **trunk**, potom...

- Odchádzajúci rámec nemá mať značku, ak patrí do VLAN, ktorá je na porte definovaná ako natívna
 - Ak rámec pri prijatí značku mal, prepínač ju pred odoslaním odstráni
 - Ak rámec pri prijatí značku nemal, prepínač značku nepridá
- Odchádzajúci rámec má mať značku, ak patrí do inej VLAN než tej, ktorá je na porte definovaná ako natívna
 - Ak rámec pri prijatí značku nemal, prepínač ju pred odoslaním pridá
 - Ak rámec pri prijatí značku mal, prepínač ju v rámci ponechá



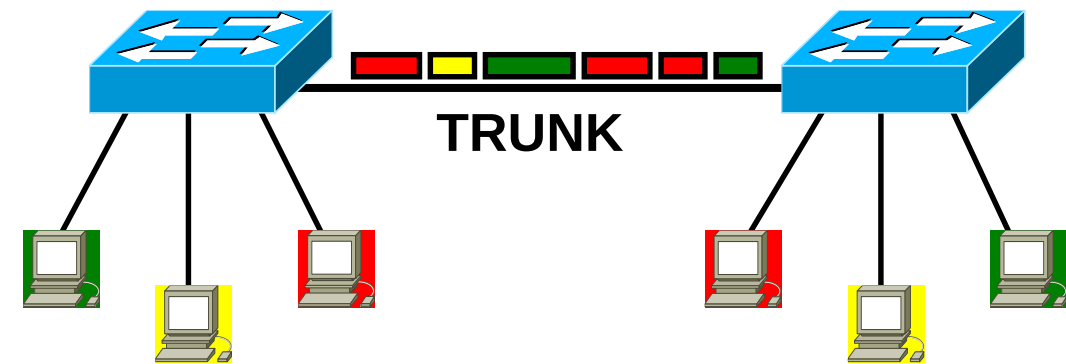
Resumé



- 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

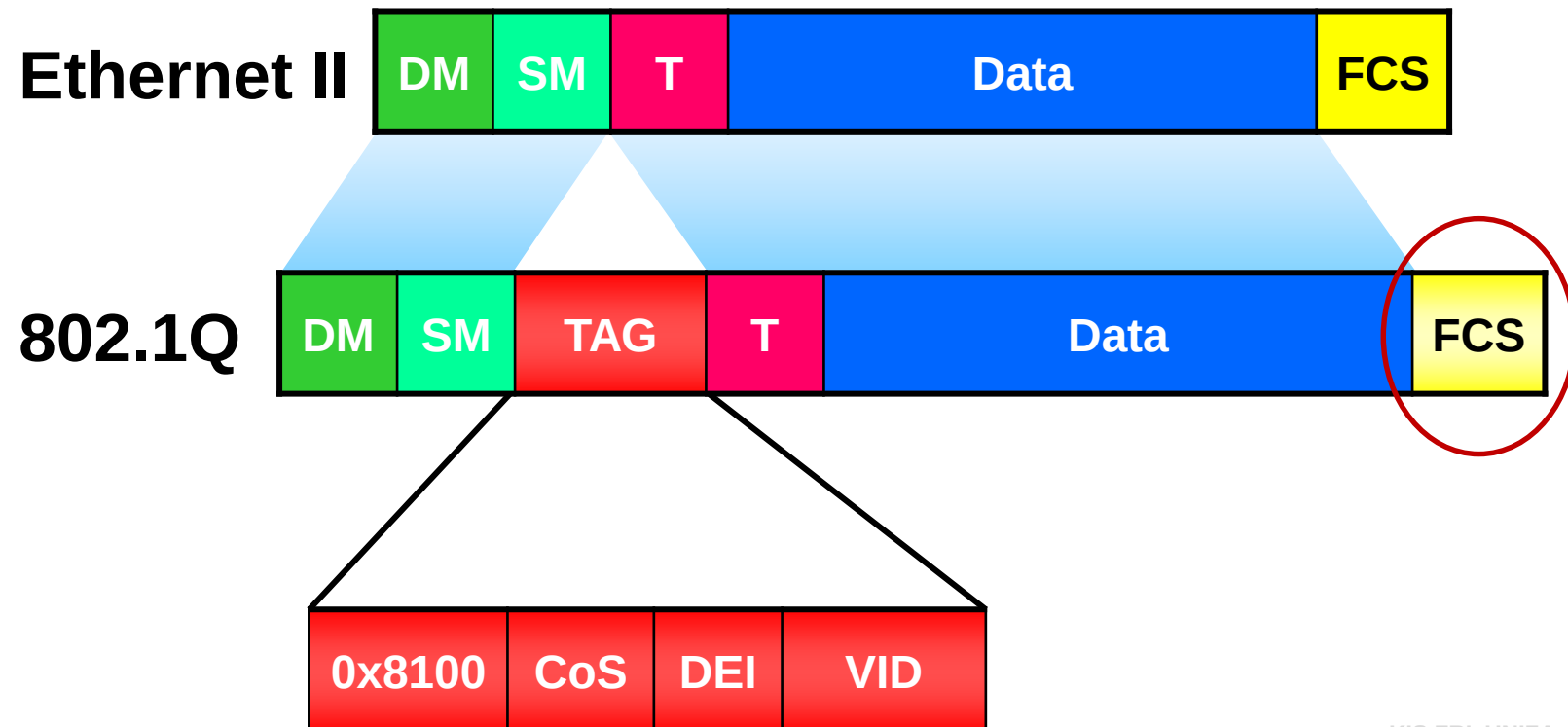
Na uvedomenie si

- Porty prepínača môžu byť dvojaké:
access a **trunk**
 - Prístupový (access) port patrí do jednej konkrétnej VLAN, spravidla neznačuje
 - Trunk port patrí do všetkých VLAN, značuje
- VLAN tag sa pridáva a odoberá len na trunkovom spoji, koncové stanice o značkovaní spravidla nevedia
 - Tagging je primárne vec prepínačov
 - Len výnimočne sa značkované rámce posielajú aj voči koncovým staniciam (napr. pri smerovaní medzi VLAN, virtualizovaných serveroch, IP telefónii apod.)
- Na trunk porte prebieha učenie sa MAC adries rovnako ako na akomkoľvek inom porte
- Rovnaké VLAN musia byť na každom prepínači identicky očíslované



Na uvedomenie si

- Štruktúra **802.1Q** rámca je **kompatibilná** s formátom **Ethernet II**
- Podpora 802.1Q je implementovateľná aj **softvérovo**
- BSD, GNU/Linux bežne podporujú 802.1Q
- **Windows** nemá vlastné ovládače pre 802.1Q, obvykle je podpora VLAN súčasťou špecifického ovládača od konkrétneho výrobcu sieťového adaptéra
- Potenciálny problém: rámce väčšie ako 1518B (tzv. baby jumbo frames – do 1522B)
- Zavedením 802.1Q VLAN sa nezmenšuje počet záznamov v CAM tabuľke prepínačov



Správa VLAN vo väčších sieťach

- Ak sa VLAN rozprestierajú nad viacerými prepínačmi, je potrebné vytvoriť ich na **všetkých** prepínačoch
 - Pri konfigurácii VLAN sa vždy musí definovať jej číslo, voliteľne slovný názov a prípadné ďalšie parametre
 - Udržiavať manuálne tieto nastavenia zhodné na každom prepínači je vo väčšej sieti náročné
- Existujú viaceré **protokoly**, ktorými si prepínače navzájom **synchronizujú databázu VLAN** sietí
 - Cisco: **VTP** (VLAN Trunk Protocol)
 - IEEE: 802.1ak **MVRP** (Multiple VLAN Registration Protocol, jeho predchodcom bol protokol GVRP)
 - **SNMP** (Simple Network Management Protocol)
 - Tieto protokoly neriešia zatried'ovanie portov do konkrétnych VLAN, ale identický zoznam VLAN na prepínačoch v sieti

Typy VLAN na prepínačoch Cisco

- Na Cisco prepínačoch sa VLAN zvyknú označovať rôznymi prívlastkami podľa viacerých kritérií
- Podľa čísla VLAN:
 - **Normal range VLANs**: VLAN v rozsahu **1-1005**
 - Podporované na všetkých prepínačoch
 - Prenášané protokolom VTP, ak je použitý
 - Informácia o nich je **vždy** uložená vo **flash:vlan.dat** a **môže** byť aj v running-config
 - **Extended range VLANs**: VLAN v rozsahu **1006-4094**
 - Podporované na novších prepínačoch
 - Prenášané iba protokolom VTPv3 (len veľmi nové prepínače)
 - Informácia o nich je uložená v **running-config**, iba pri VTPv3 aj vo flash:vlan.dat

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
- **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)

```
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	



Dynamic Trunking Protocol

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 prepínačoch je **dynamický** režim (prispôsobujúci sa druhej strane)

Režimy portov na Cisco prepínačoch

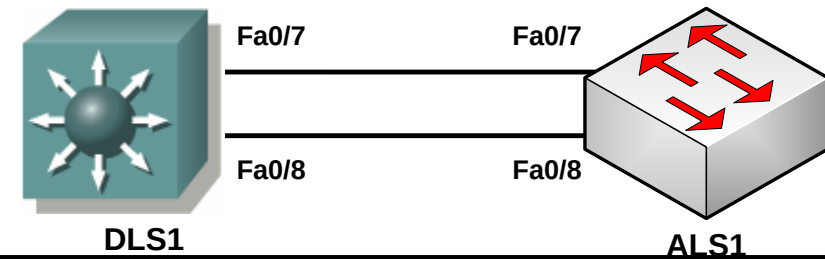
- S ohľadom na podporu DTP môžu porty na Cisco prepínačoch byť v niektorom z nasledujúcich režimov
 - **switchport mode dynamic desirable** (Catalyst 2950, 3550)
 - Port sa vie prispôbiť druhej strane (dynamický port)
 - Port preferuje režim trunk, ohlasuje ho pomocou DTP
 - **switchport mode dynamic auto** (Catalyst 2960, 3560)
 - Port sa vie prispôbiť druhej strane (dynamický port)
 - Port preferuje režim access, ohlasuje ho pomocou DTP
 - **switchport mode trunk**
 - Port sa nevie prispôbiť druhej strane (statický port)
 - Svoj režim trunk ohlasuje pomocou DTP
 - **switchport mode access**
 - Port sa nevie prispôbiť 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

DTP – statik trunk vs dynamic auto



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

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

```
DLS1#sh int fa 0/7 switchport
```

```
Name: Fa0/7
```

```
Switchport: Enabled
```

```
Administrative Mode: trunk
```

```
Operational Mode: trunk
```

```
Administrative Trunking Encapsulation: dot1q
```

```
Operational Trunking Encapsulation: dot1q
```

```
Negotiation of Trunking: On
```

```
Access Mode VLAN: 1 (default)
```

```
Trunking Native Mode VLAN: 1 (default)
```

```
Administrative Native VLAN tagging: enabled
```

```
Voice VLAN: none
```

```
Administrative private-vlan host-association: none
```

```
Administrative private-vlan mapping: none
```

```
Administrative private-vlan trunk native VLAN: none
```

```
Administrative private-vlan trunk Native VLAN tagging:
enabled
```

```
Administrative private-vlan trunk encapsulation: dot1q
```

```
Administrative private-vlan trunk normal VLANs: none
```

```
Administrative private-vlan trunk associations: none
```

```
Administrative private-vlan trunk mappings: none
```

```
Operational private-vlan: none
```

```
Trunking VLANs Enabled: ALL
```

```
Pruning VLANs Enabled: 2-1001
```

```
ALS1#sh int trunk
```

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

```
ALS1#sh int fa 0/7 switchport
```

```
Name: Fa0/7
```

```
Switchport: Enabled
```

```
Administrative Mode: dynamic auto
```

```
Operational Mode: trunk
```

```
Administrative Trunking Encapsulation: dot1q
```

```
Operational Trunking Encapsulation: dot1q
```

```
Negotiation of Trunking: On
```

```
Access Mode VLAN: 1 (default)
```

```
Trunking Native Mode VLAN: 1 (default)
```

```
Administrative Native VLAN tagging: enabled
```

```
Voice VLAN: none
```

```
Administrative private-vlan host-association: none
```

```
Administrative private-vlan mapping: none
```

```
Administrative private-vlan trunk native VLAN: none
```

```
Administrative private-vlan trunk Native VLAN tagging:
enabled
```

```
Administrative private-vlan trunk encapsulation: dot1q
```

```
Administrative private-vlan trunk normal VLANs: none
```

```
Administrative private-vlan trunk associations: none
```

```
Administrative private-vlan trunk mappings: none
```

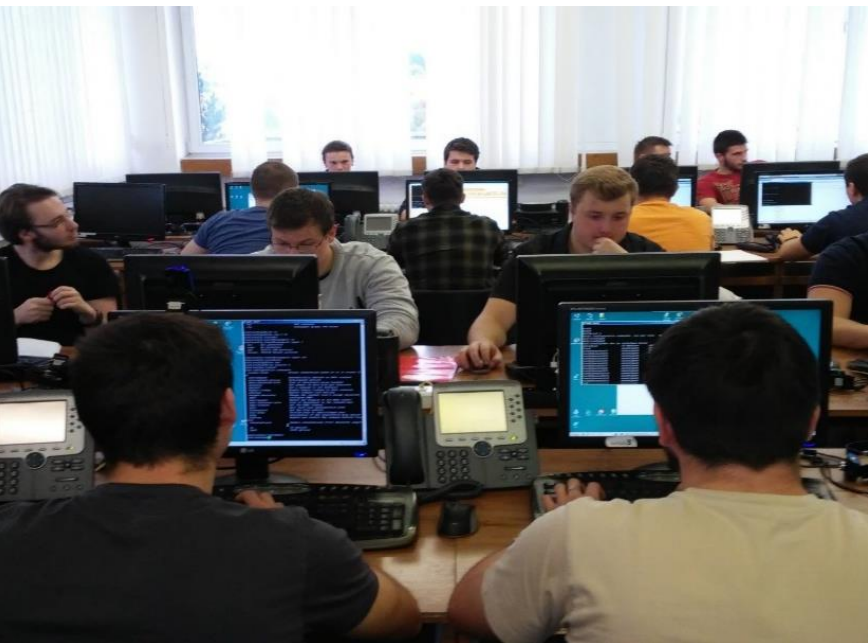
```
Operational private-vlan: none
```

```
Trunking VLANs Enabled: ALL
```

```
Pruning VLANs Enabled: 2-1001
```

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**



Príkazy na overenie a zmenu nastavení VLANs

Zobrazenie VLAN databázy

```
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	

- Default VLAN
- Management VLAN
- Native VLAN
- User/Data VLANs
- Black Hole VLAN
- Voice VLAN

- All ports assigned to VLAN 1 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.

Zmena príslušnosti portu do VLAN

```
S1# config t
S1(config)# int fa0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# 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, Fa0/12, 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
20	student	active	Fa0/11
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```
S1#
```

Zmazanie VLANy

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh 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, Fa0/12, 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	

Overenie VLAN info

```
S1# show interfaces vlan 20
vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia
001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, 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 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Konfigurácia trunk portu

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
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 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Zmena trunku na access port

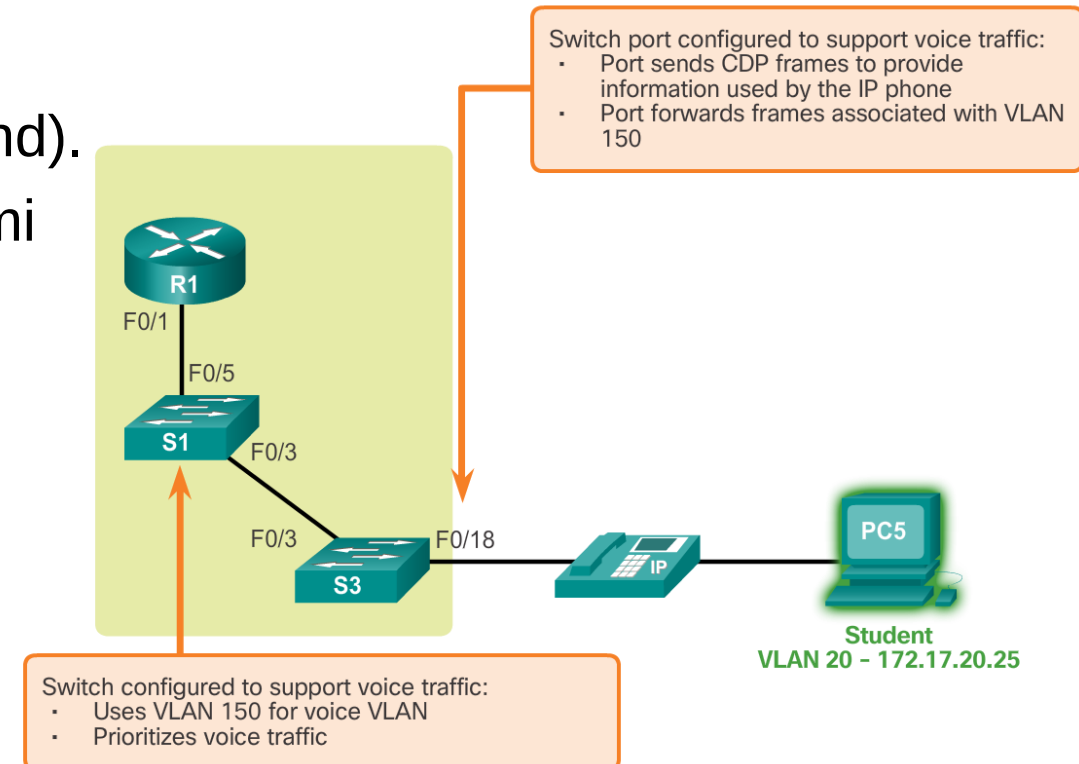
```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Zmena trunku na access port

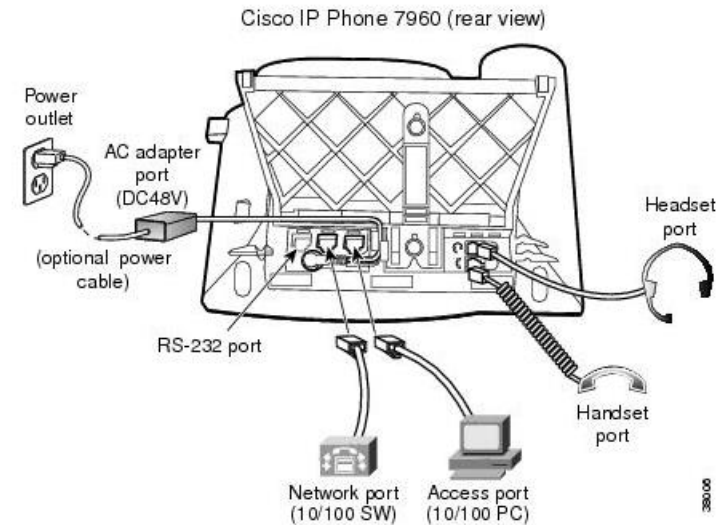
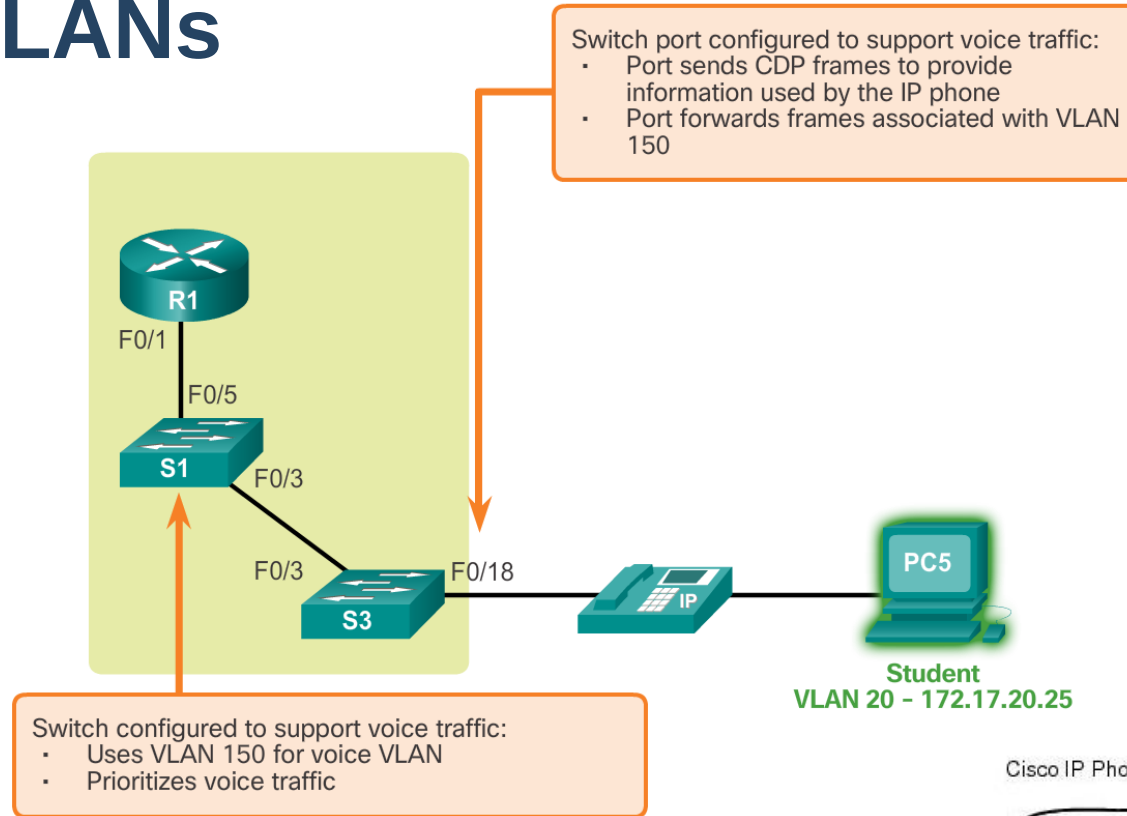
```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```


Voice VLANs

- VoIP prevádzka je citlivá na oneskorenie a vyžaduje:
 - Garantovanú šírku pásma (bandwidth)
 - Pre zabezpečenie potrebnej kvality hlasu
 - Prioritu pred ostatnými typmi prevádzky.
 - Hlavne v stave zahltenia
 - Oneskorenie menšie ako 150 ms (end-to-end).
 - Všetko viem zabezpečiť QoS mechanizmami
- Voice VLAN:
 - Umožňuje prenášať hlasovú prevádzku z IP telefónu
 - Cisco 7960 IP phone



Voice VLANs

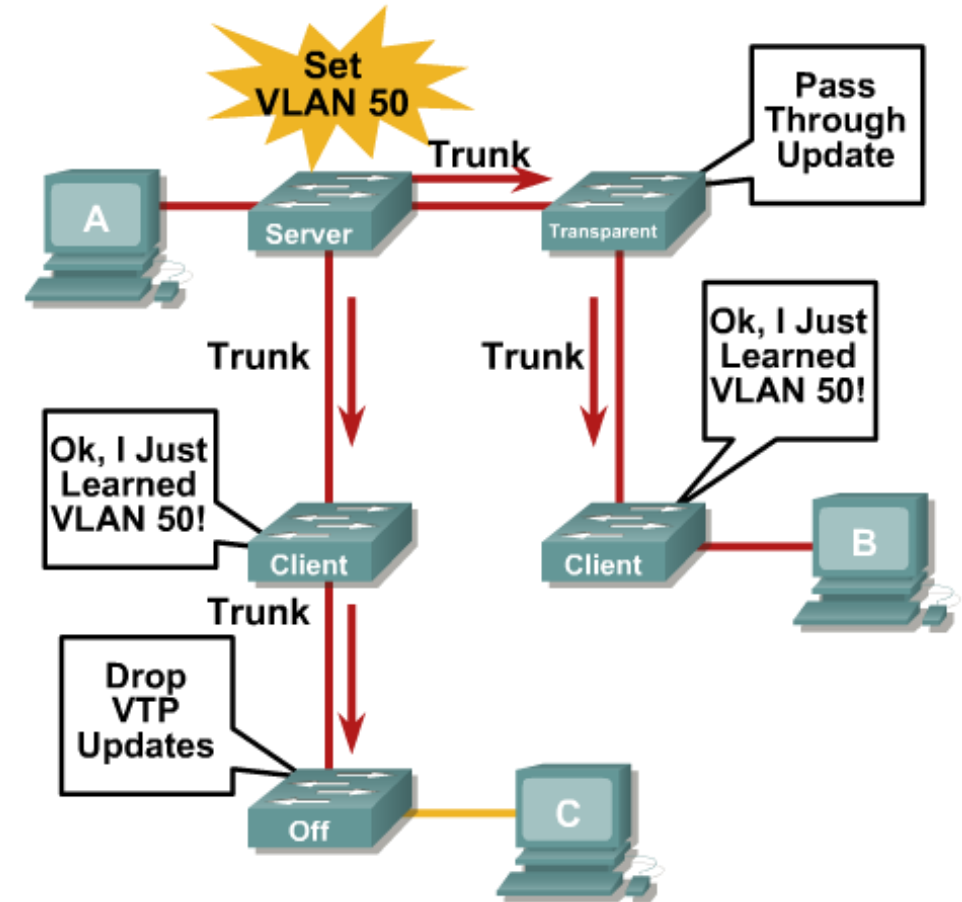




Virtual Trunking Protocol (VTP)

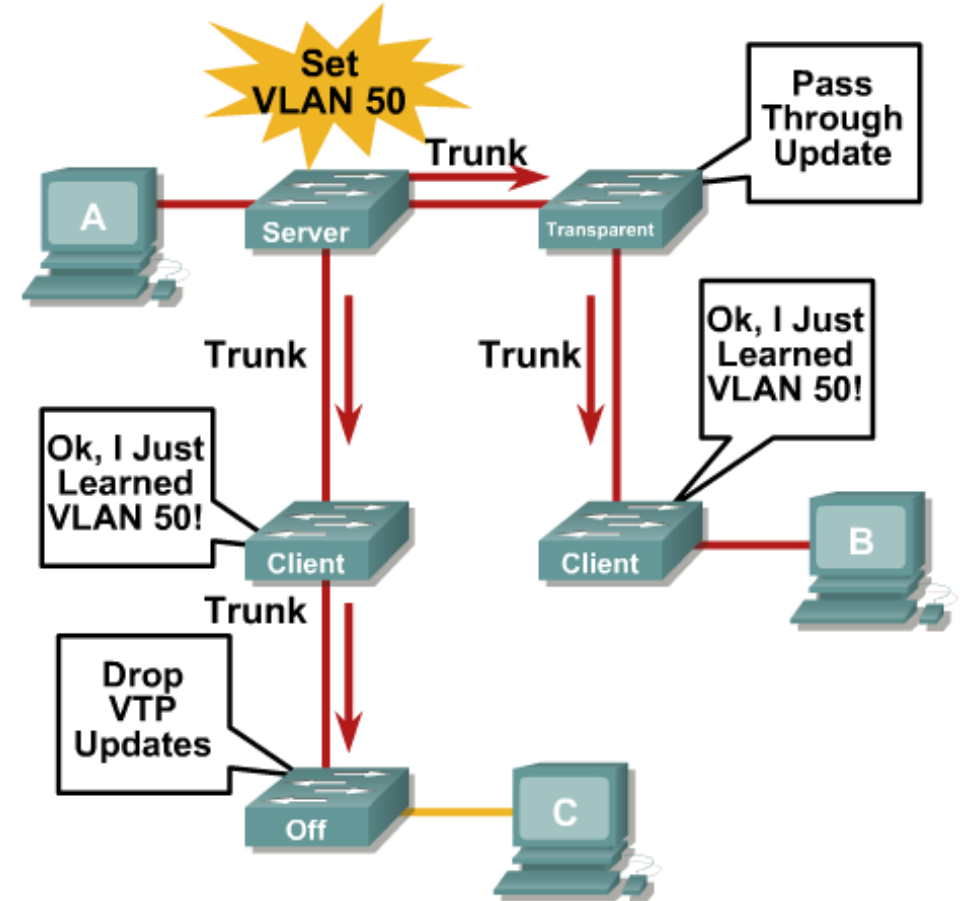
Výhody VTP

- 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 konfigurácii VLAN sietí



Virtual Trunking Protocol (VTP)

- VTP správy sa prenášajú výlučne **cez trunk** porty
 - Používa dot1q or ISL rámce
 - Prenášané cez native VLAN (def. VLAN 1)
- Tri verzie
 - VTPv1 a VTPv2 boli donedávna dominantné
 - VTPv3 bolo pôvodne podporované len na high-end switchoch, od verzie IOSu 12.2(52)SE je k dispozícii na všetkých Catalyst switchoch
 - VTPv1 a VTPv2 prenášajú iba info o VLAN 1-1005
 - VTPv3 prenášajú info o všetkých VLAN
- Catalyst podporuje verzie VTP 1, 2, 3
 - V2 je najbežnejšia, ale default je v režime v1
 - Navzájom nekompatibilné





Rozdiely medzi VTP verziami

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

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

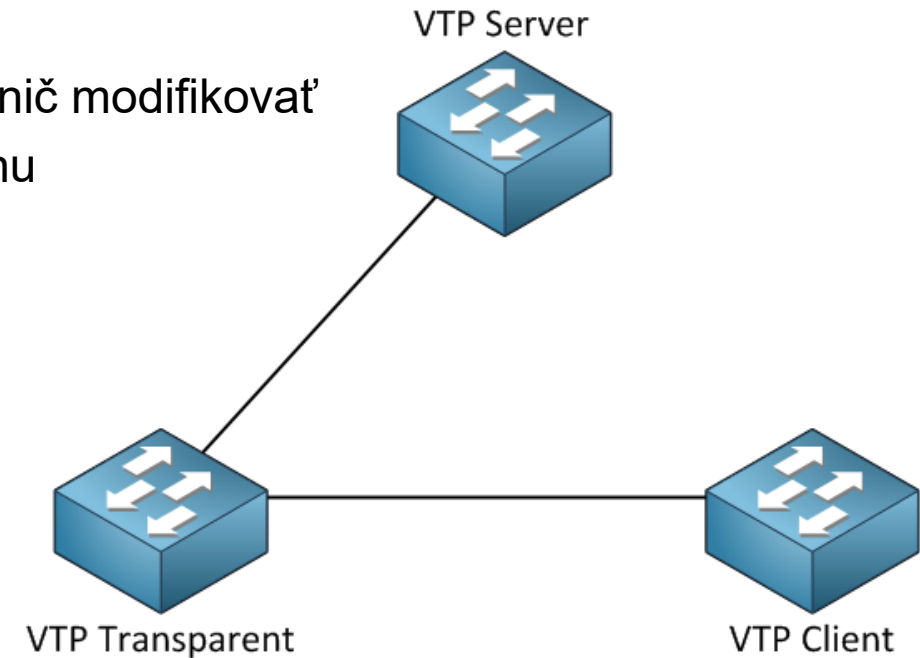
- Adaptuje sa na zmeny VLAN databázy, no sám nemá právo nič modifikovať
- Spracováva a preposiela prijaté VTP správy pre danú doménu
- Informácia o VLAN sa ukladá iba do súboru vlan.dat

■ Transparent

- Nie je skutočným členom domény
- Preposiela VTP správy, ale ignoruje ich obsah
- Má vlastnú nezávislú VLAN databázu
- Má vždy VTP číslo revízie 0

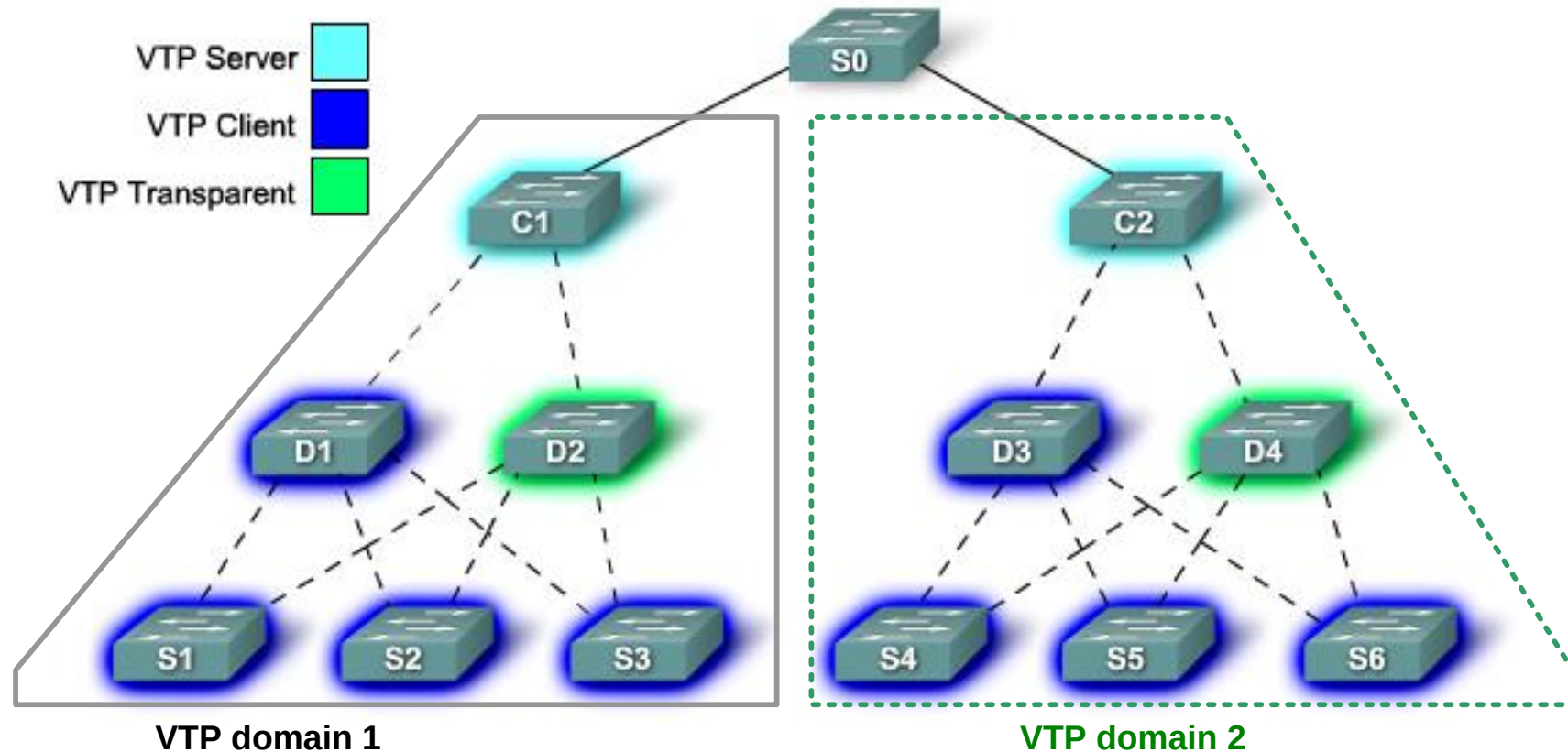
■ Off

- Ignoruje a nepreposiela VTP správy (len VTPv3 alebo CatOS)



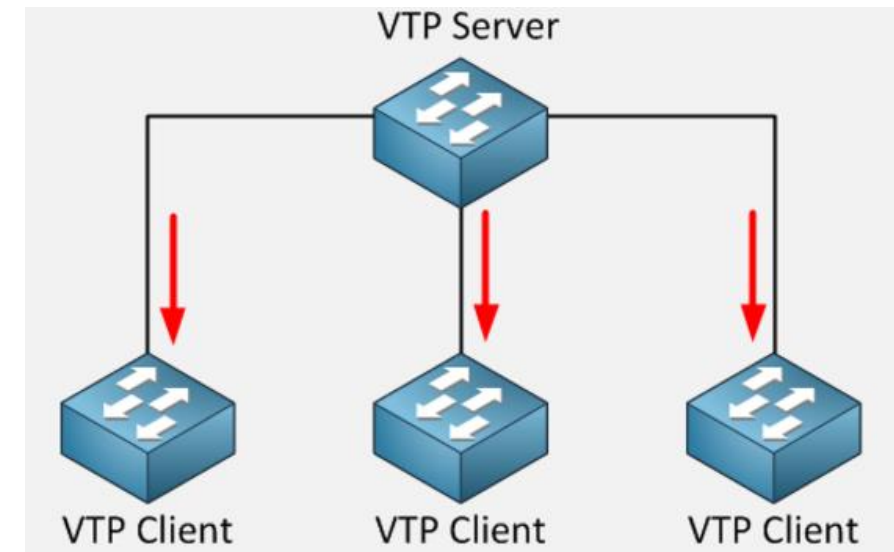
VTP doména

- 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

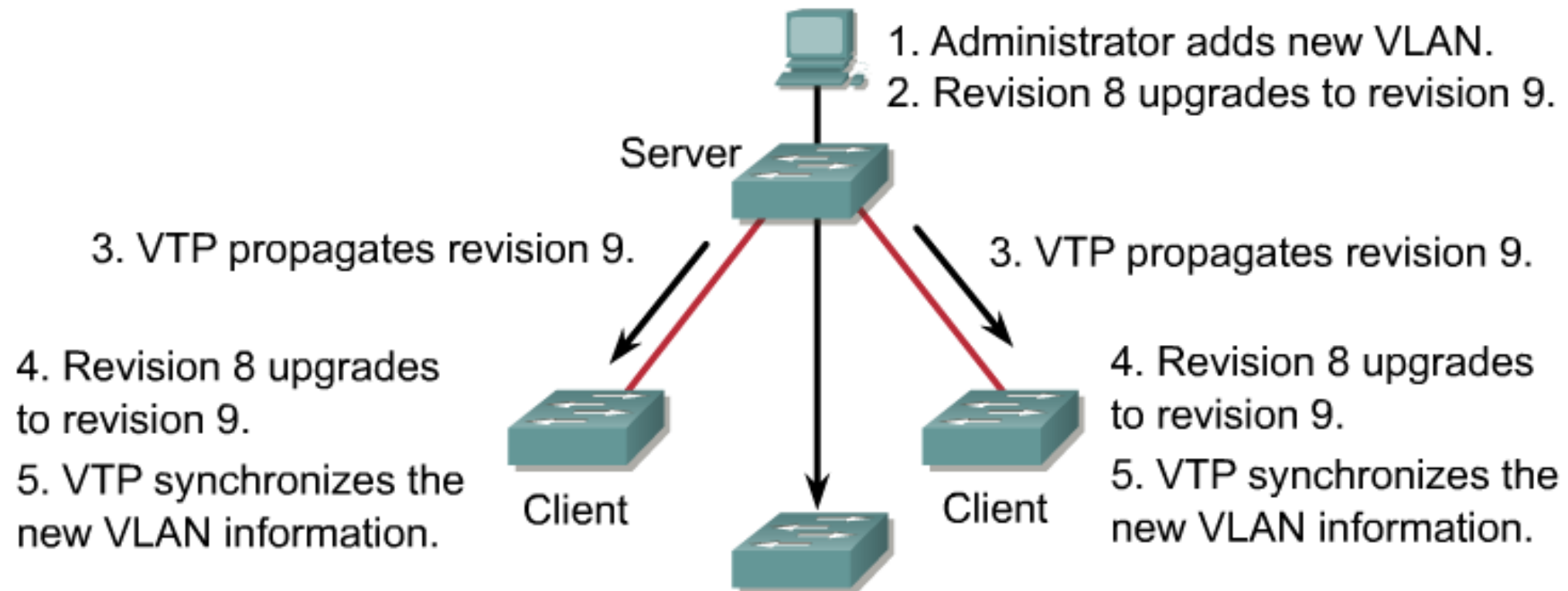
- VTP používa dva druhy VTP správ (advertisements):
 - **Požiadavky** od VTP klientov, ktorí chcú info pri bootovaní
 - **Odpovede** (inzercia) od VTP serverov
- Pri tom VTP používa tri typy VTP správ:
 - **Summary advertisements**
 - VTP server posiela sumárne VLAN info každých päť minút
 - Alebo keď 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**
 - Nasleduje 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 otláčok 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

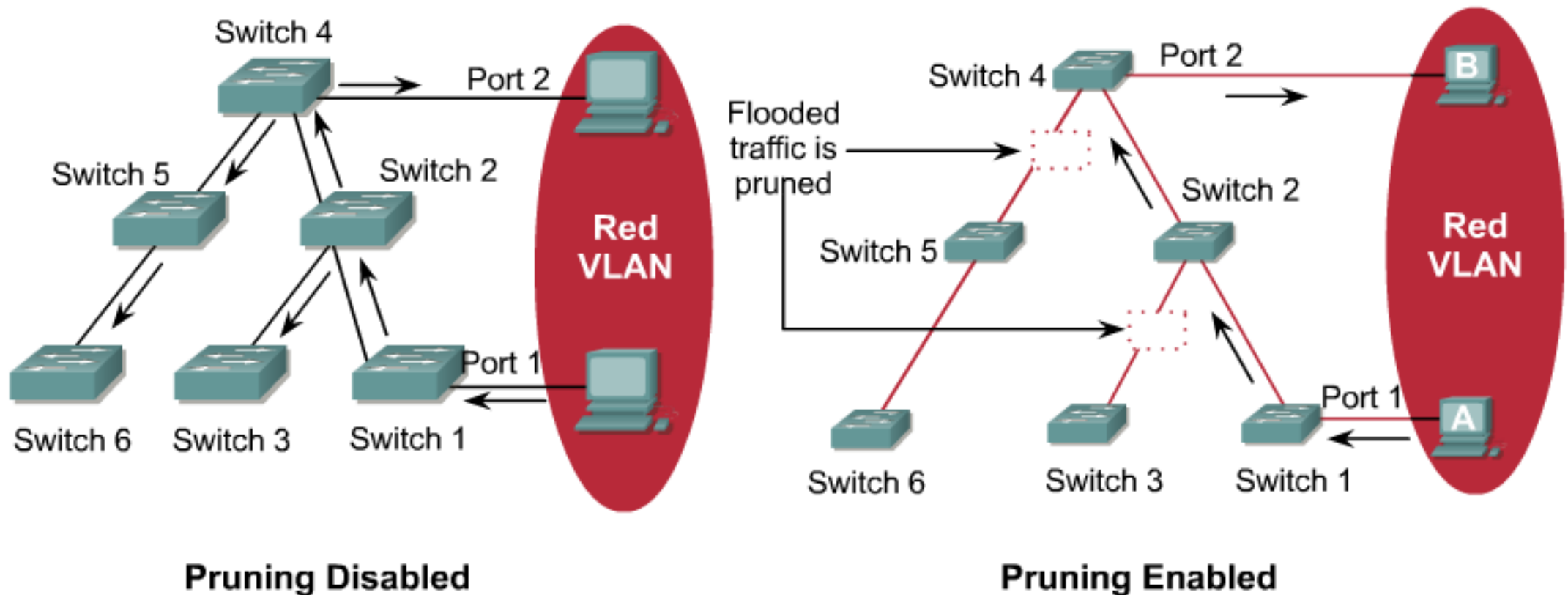
Činnost' VTP



Transparent mode passes the VTP advertisements but does not synchronize.

VTP pruning

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





Konfigurácia VTP

Základná konfigurácia VTP

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

VTP konfiguračné príkazy

```
Switch(config)#vtp domain MENO_DOMENY  
Switch(config)#vtp mode {client | server | transparent}  
Switch(config)#vtp password TVOJE_HESLO  
Switch(config)#vtp version {1 | 2}
```

!Len na VTP serveroch

```
Switch(config)#vtp pruning
```

Overenie činnosti VTP

```
Switch#sh vtp status
```

```
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 64
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             : Null
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x7D 0x5A 0xA6 0x0E 0x9A
0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```


Overenie činnosti VTP

```
Switch#sh vtp counters
```

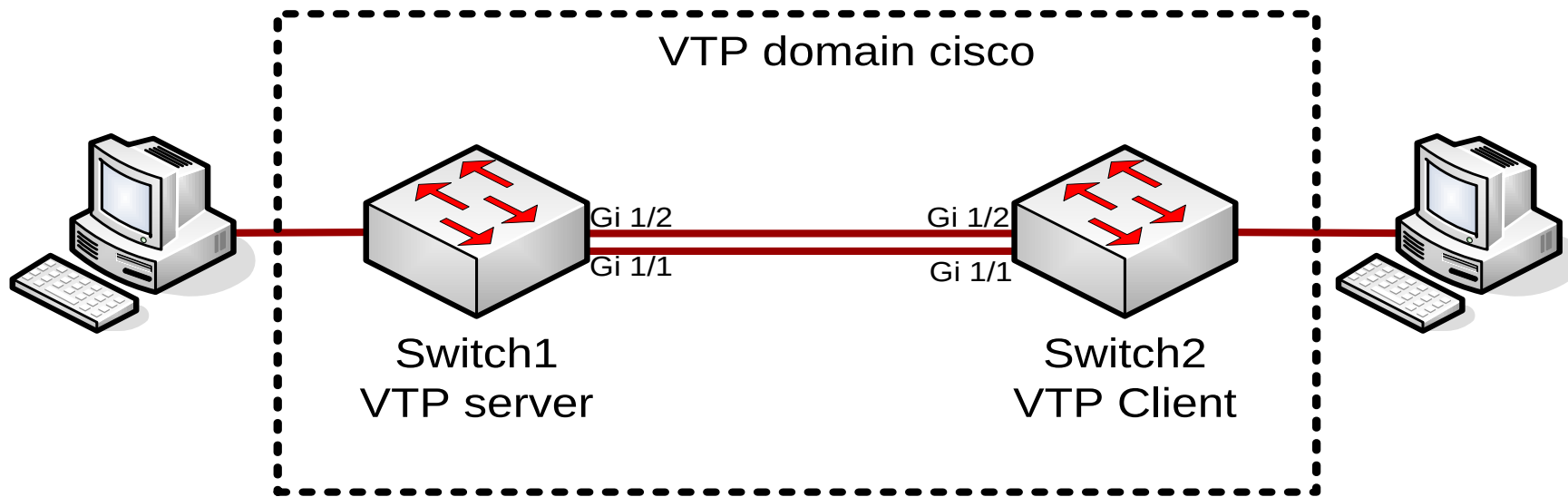
```
VTP statistics:
```

```
Summary advertisements received      : 1
Subset advertisements received      : 1
Request advertisements received      : 2
Summary advertisements transmitted  : 5
Subset advertisements transmitted    : 5
Request advertisements transmitted   : 0
Number of config revision errors     : 0
Number of config digest errors       : 0
Number of V1 summary errors          : 0
```

```
VTP pruning statistics:
```

Trunk	Join Transmitted	Join Received	Summary advts received from non-pruning-capable device
-----	-----	-----	-----

Príklad konfigurácie



Príklad konfigurácie

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

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

Príklad konfigurácie

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

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

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

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

Časté chyby pri konfigurácii VTP

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

Pár tipov

- Zmena revízneho čísla VTP
 - Reštart prepínača, alebo:
 - Zmena domény

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

- Zakázanie VTP na prepínači

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

Vymazanie prepínača pripojeného do väčšej živej siete s VTP

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

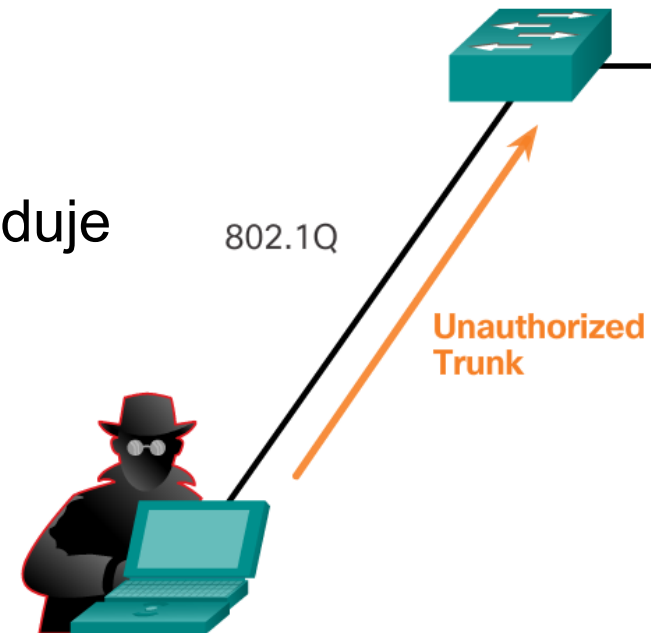
```
Switch#conf t
Switch(config)#
Switch(config)#interface range FastEthernet 0/1 -24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range GigabitEthernet 0/1 -2
Switch(config-if-range)#shutdown
15:45:59: %LINK-5-CHANGED: Interface GigabitEthernet0/2,
changed state to administratively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



Bezpečnostné aspekty VLAN

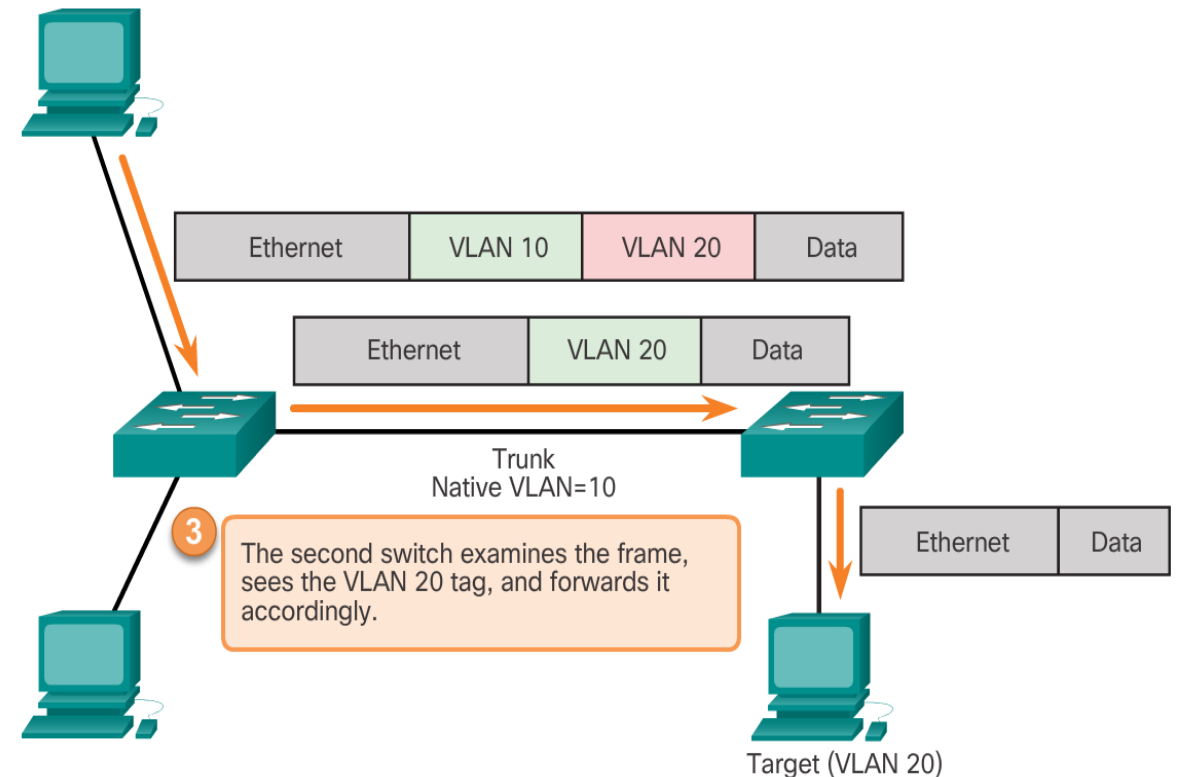
Switch Spoofing Attack

- DTP je zapnuté na Cisco Catalyst 2960 aj 3560 by default
 - Default konfigurácia portu: dynamic auto.
- Útočníkovi stačí vystupovať (spoof) ako prepínač a vytvoriť trunk
 - Tým získa prístup do akejkoľvek VLAN
- Prevencia:
 - vypnúť DTP
 - trunk iba na portoch, kde sa to skutočne vyžaduje



Double-Tagging Attack (VLAN hopping)

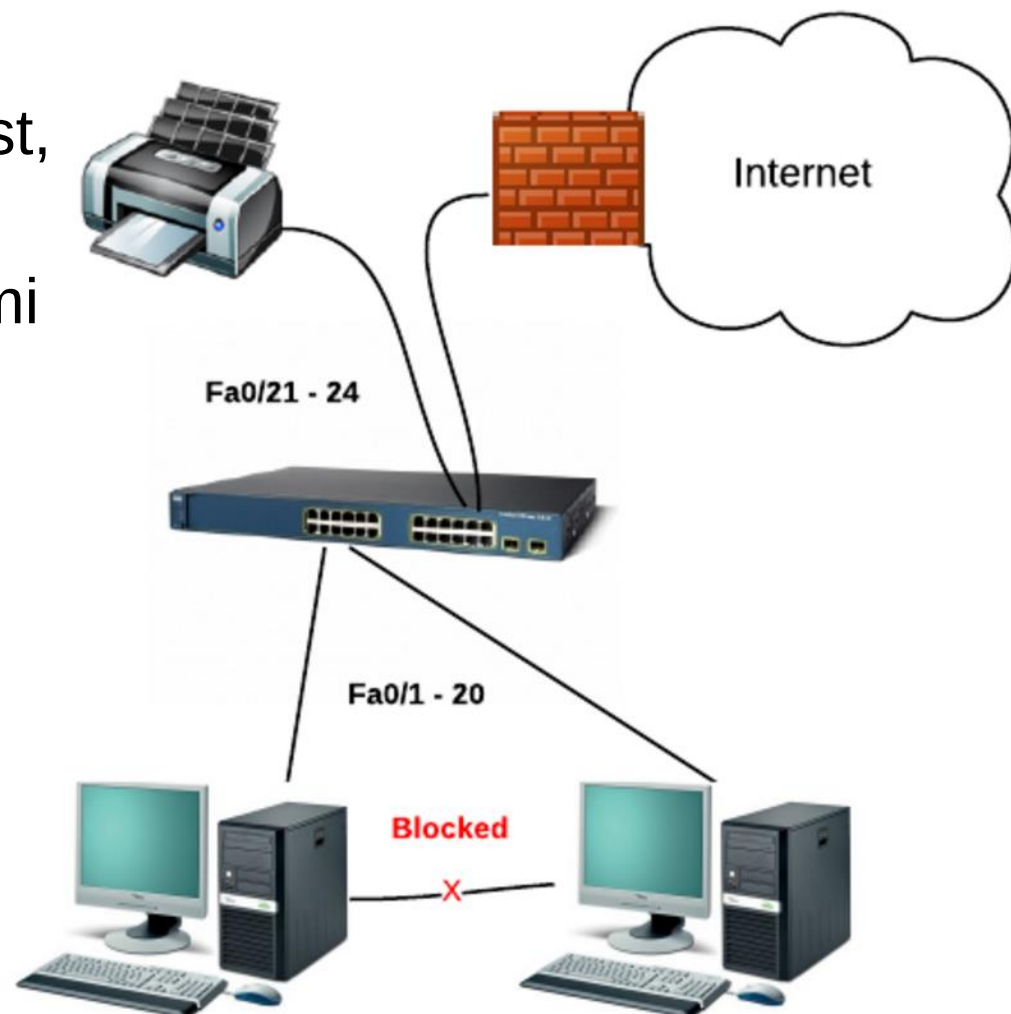
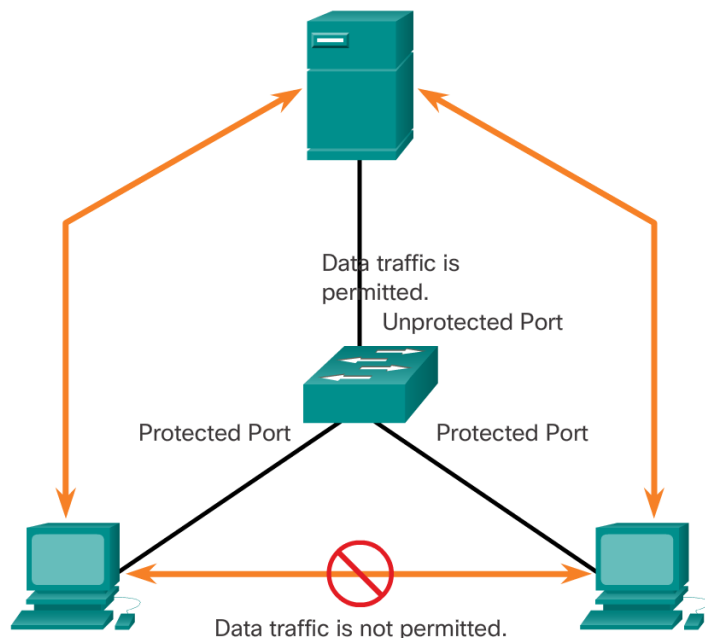
- Ak má rámec viacero vnorených značiek, väčšina prepínačov de-encapsuluje iba jednu tú prvú/vonkajšiu
 - To dáva priestor útočníkom, aby využili druhú značku na prienik do inej VLAN, a obišli tak smerovač a bezpečnostné mechanizmy na ňom
- Podmienky úspešnosti útoku:
 - Ak je port trunk, nastaviť vonkajšiu značku na značku pre natívnu VLAN daného trunk portu
 - Ak je port vo Voice VLAN, no problem
 - Z takého portu prepínač očakáva značky (na dátovom access porte nie)
- Prevencia:
 - Natívnu VLAN dať inú ako akúkoľvek data VLAN (pre všetky trunk porty)



Funkcia „private VLAN Edge“ = PVLAN

Definujú sa tzv. protected porty

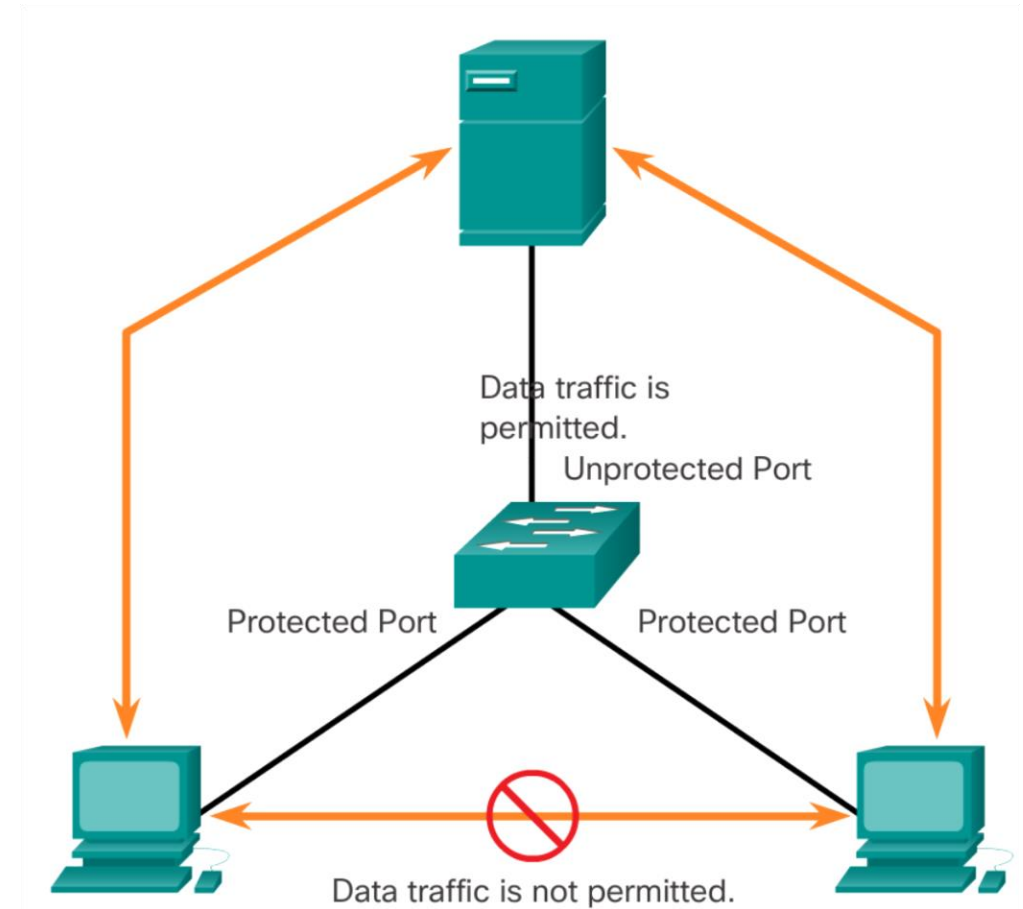
- Medzi nimi bude zakázaná akákoľvek unicast, broadcast, aj multicast prevádzka
- Komunikovať môžu iba s unprotected portami
- Platí lokálne na danom prepínači

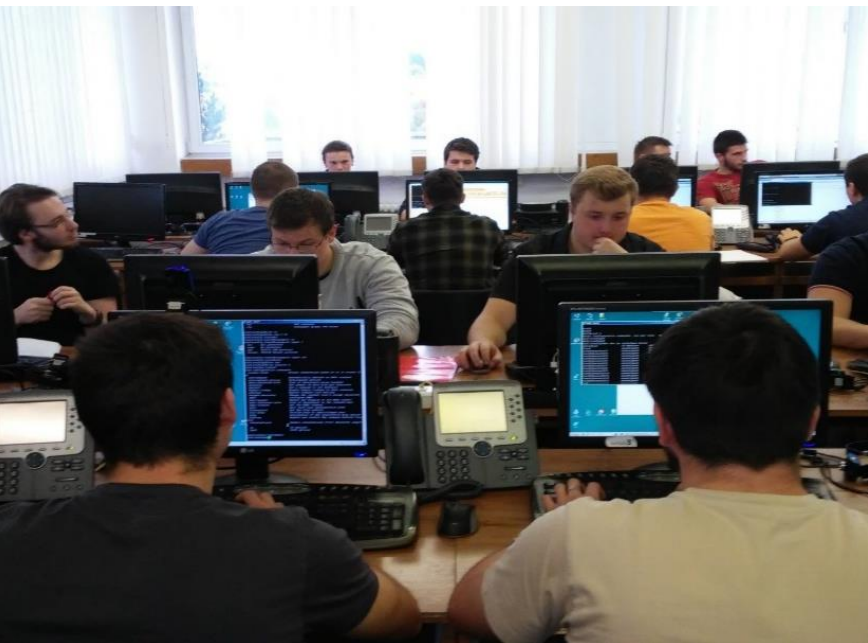


Funkcia „private VLAN Edge“ = PVLAN

```
S1(config)# interface g0/1
S1(config-if)# switchport protected
S1(config-if)# end
S1# show interfaces g0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<output omitted>

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```





Smerovanie medzi VLAN

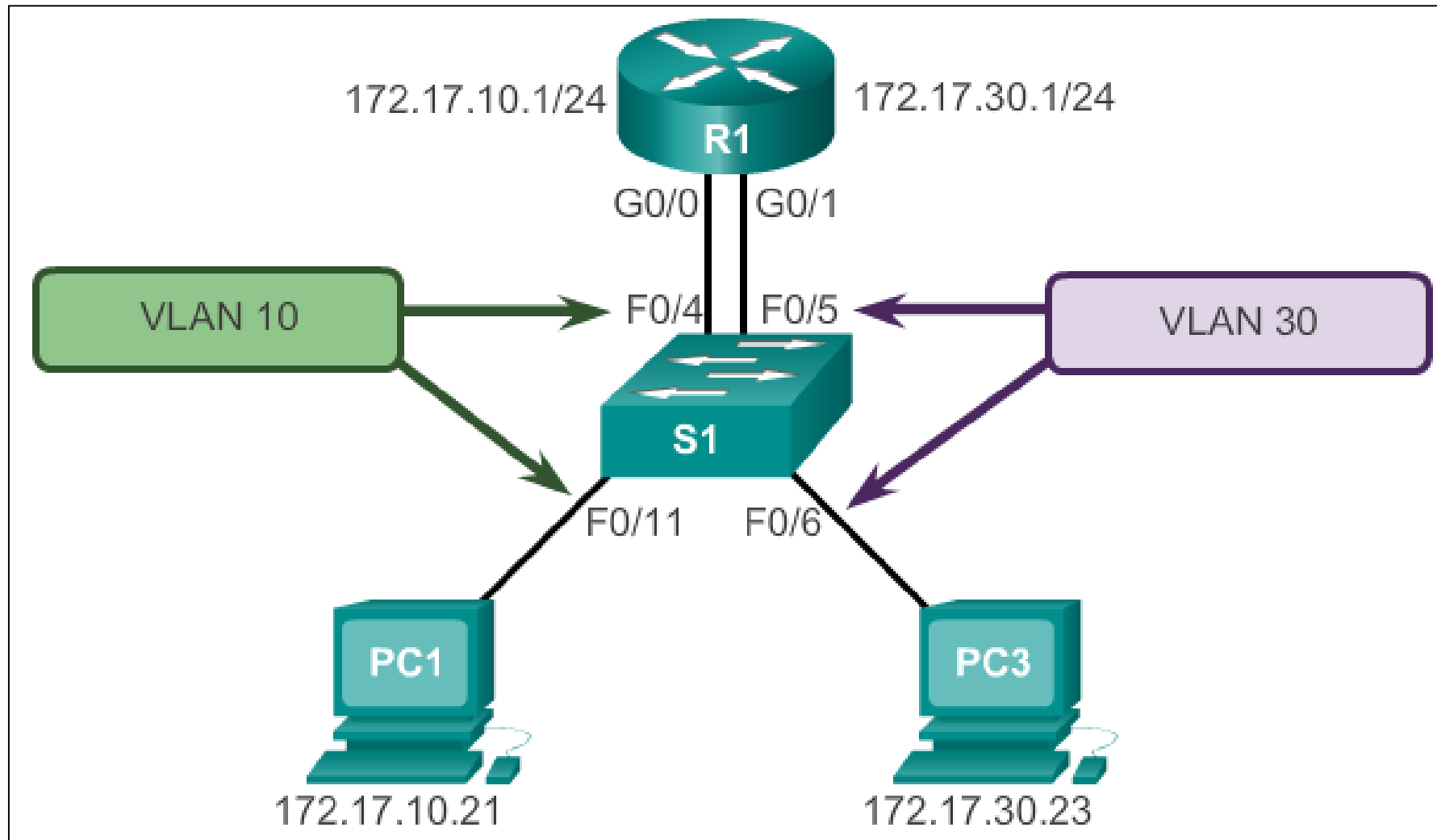
Router-on-Stick

RSE chapter 3: časť Inter-VLAN routing

Smerovanie medzi VLAN

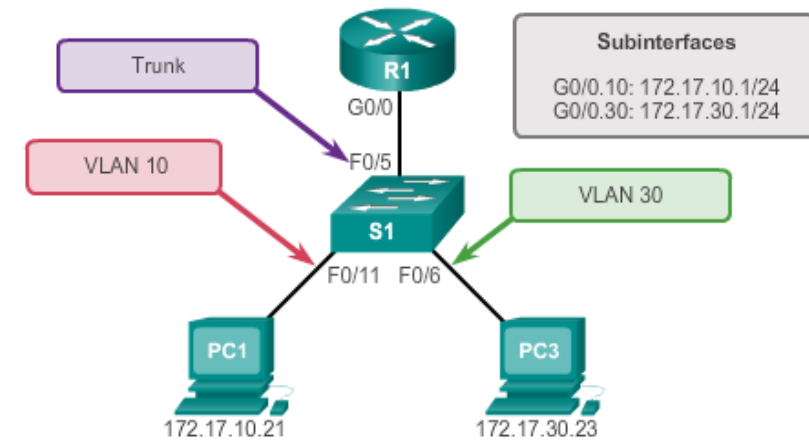
- VLAN vytvárame na to, aby sme sústredili ich členské stanice do spoločných, vzájomne nezávislých sietí
 - Neznamená to ale, že VLAN nemôžu medzi sebou komunikovať
 - Keďže 1 VLAN $\approx$ 1 IP sieť, komunikácia medzi VLAN je komunikáciou medzi IP sieťami – na to je nevyhnutný smerovač
- Ako vlastne prebieha komunikácia medzi IP sieťami?
 - Odosielajúca stanica zistí, že adresát paketu je v inej IP sieti. Paket preto zabalí do rámca adresovaného svojej bráne
 - Brána (smerovač) prevezme rámec, vybalí z neho paket, podľa smerovacej tabuľky určí výstupné rozhranie a next hop IP adresu, paket opäť zabalí do rámca, ktorý adresuje sieťovej karte ďalšieho hopu na ceste a odošle výstupným rozhraním

Možné riešenie smerovania medzi VLAN

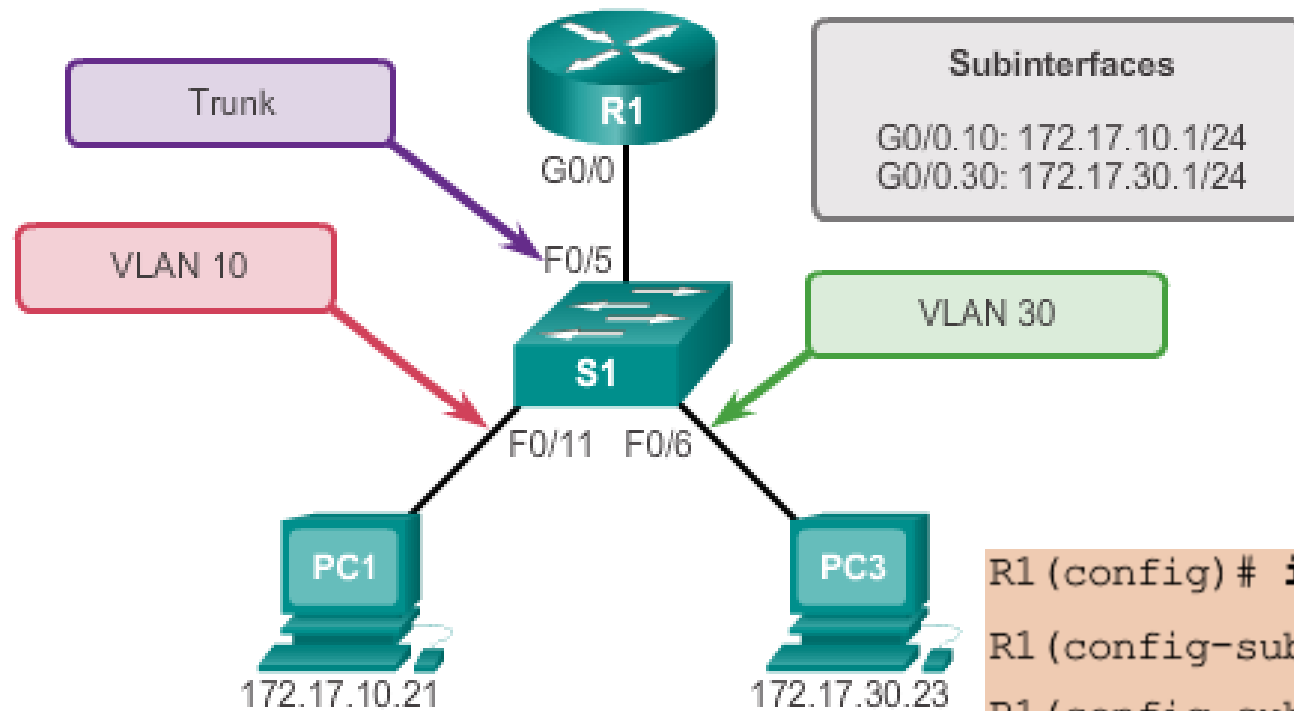


Smerovanie medzi VLAN

- Smerovanie medzi VLAN by sa dalo robiť pomocou **dedikovaných fyzických portov**, ale nevýhody sú zrejmé
 - Koľko VLAN, toľko portov na smerovači a vyhradených prístupových portov na prepínači voči smerovaču
- S výhodou však môžeme využiť **trunk port** zavedený voči smerovaču
 - Cez trunk budú voči smerovaču posielané značkované rámce
 - Smerovač bude pre každú VLAN mať vytvorené tzv. logické podrozhranie (subinterface) so samostatnou IP sieťou
 - Podrozhrania sú vždy asociované s príslušným fyzickým rozhraním
 - Ak fyzickým rozhraním vojde rámec s istou značkou, smerovač ho spracuje, ako keby vošiel podrozhraním pre danú VLAN
 - Ak má rámec byť odoslaný nejakým podrozhraním, smerovač doň vloží príslušnú značku a odošle ho fyzickým rozhraním
- Tento spôsob sa volá **router-on-stick**

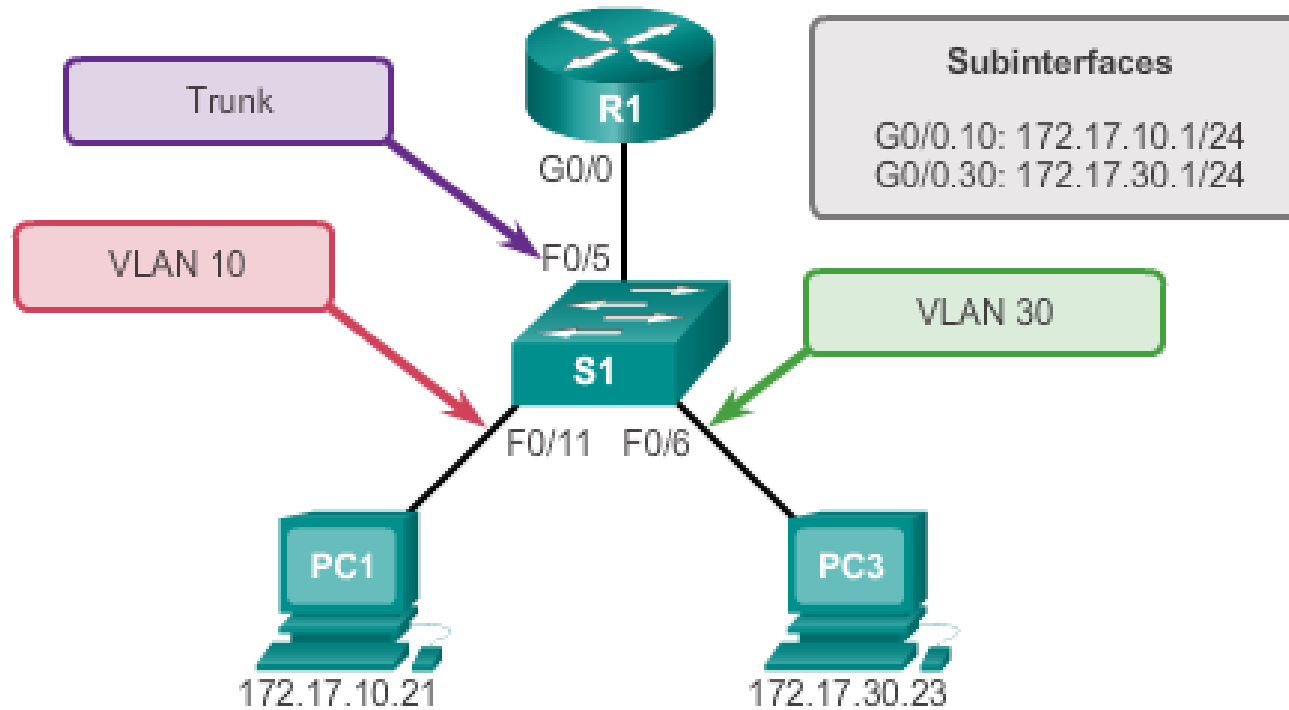


Smerovanie medzi VLAN pomocou router-on-stick



```
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
```

Smerovanie medzi VLAN pomocou router-on-stick



Smerovacia tabuľka na R1:

```
Gateway of last resort is not set
```

```
172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C    172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L    172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C    172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L    172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

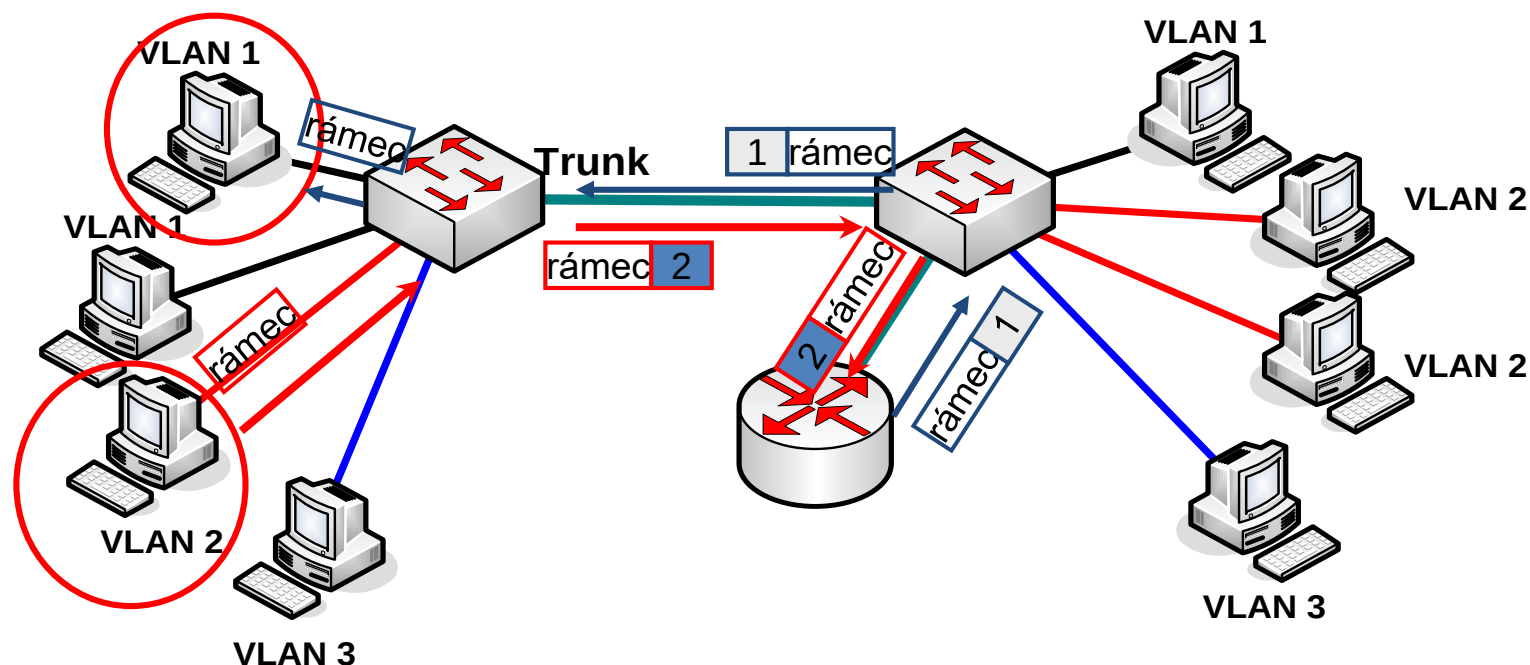
Ďalší příklad na router-on-stick

```
interface FastEthernet0/0
  no shutdown
!
interface FastEthernet0/0.1
  encapsulation dot1Q 1
  ip address 192.168.11.1 255.255.255.0
!
interface FastEthernet0/0.2
  encapsulation dot1Q 2
  ip address 192.168.12.1 255.255.255.0
!
interface FastEthernet0/0.3
  encapsulation dot1Q 3
  ip address 192.168.13.1 255.255.255.0
```

```
Router# show ip route connected
```

```
C    192.168.11.0/24 is directly connected, FastEthernet0/0.1
C    192.168.12.0/24 is directly connected, FastEthernet0/0.2
C    192.168.13.0/24 is directly connected, FastEthernet0/0.3
```

Ďalší príklad na router-on-stick



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

Paket z 192.168.12.100 na 192.168.11.50

```
C    192.168.11.0/24 is directly connected, FastEthernet0/0.1
C    192.168.12.0/24 is directly connected, FastEthernet0/0.2
C    192.168.13.0/24 is directly connected, FastEthernet0/0.3
```

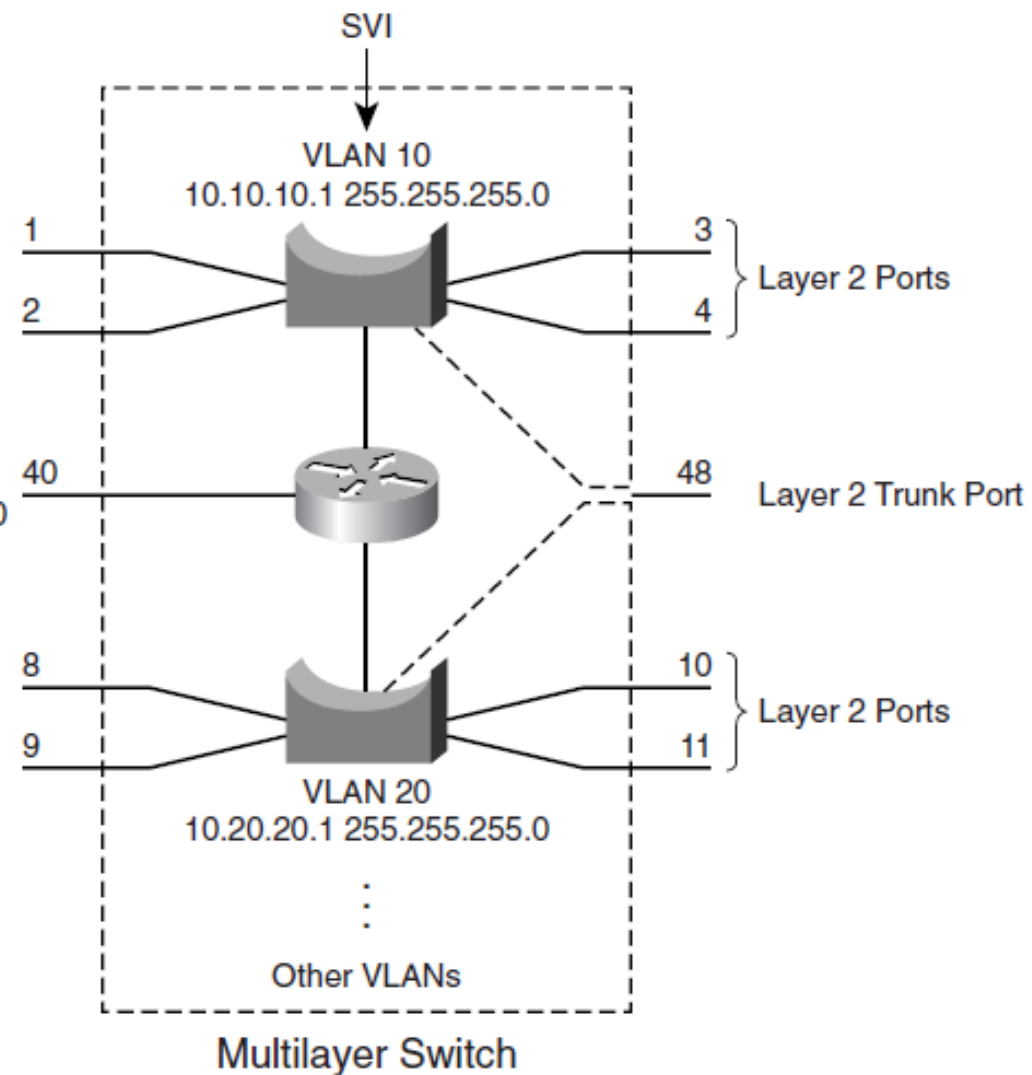
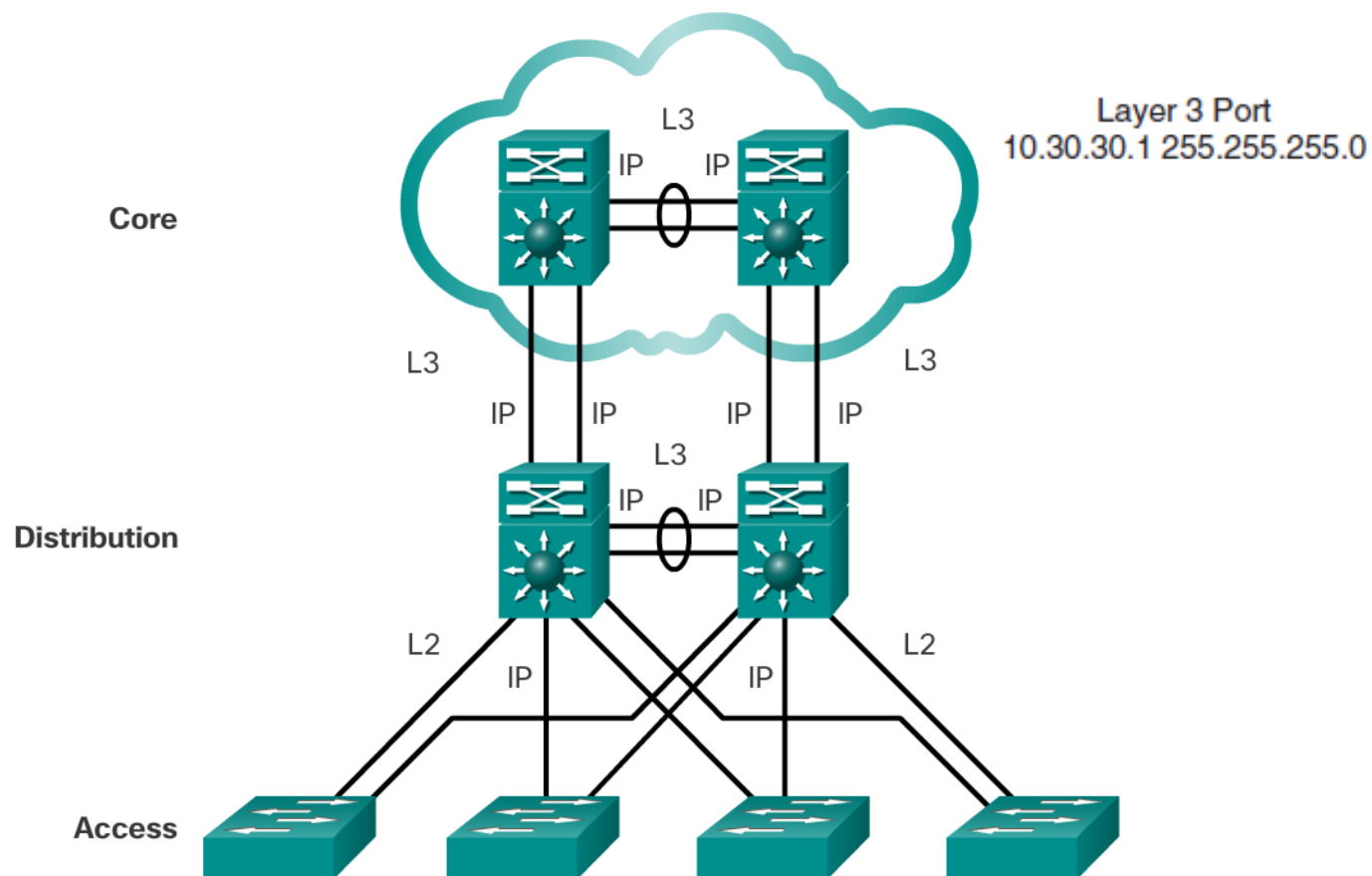


Smerovanie medzi VLAN pomocou multilayer switchingu

Smerované rozhrania na MLS

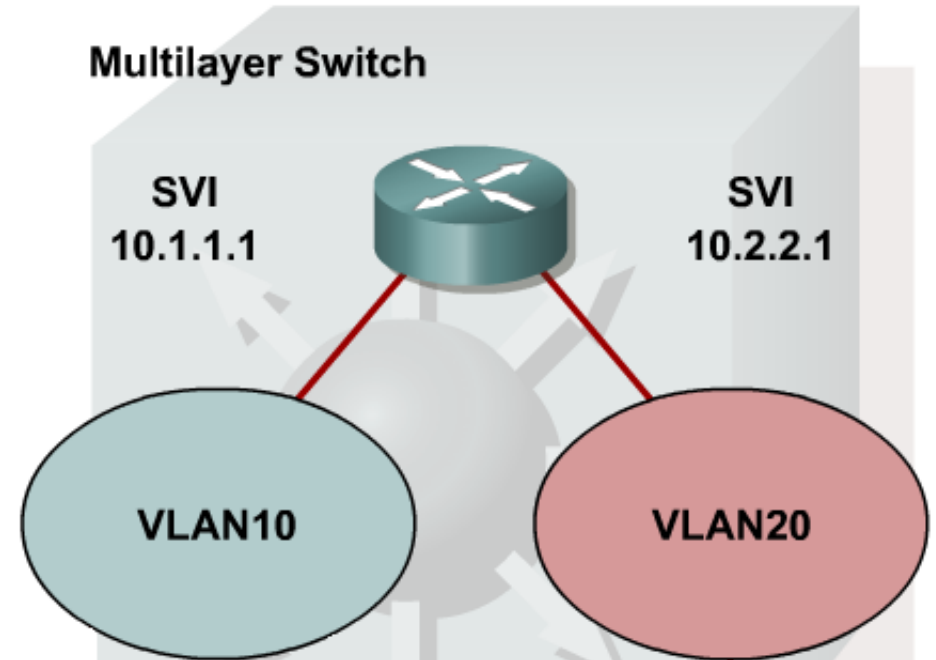
- Smerovanie pomocou smerovačov typu router-on-stick je funkčné a použiteľné, ale zároveň málo výkonné
- Rádovo **vyššiu priepustnosť** i **operatívnosť** ponúkajú tzv. multilayer switches (MLS)
 - Prepínače, ktoré vo svojich špecializovaných HW obvodoch vedia robiť funkcie prepínania aj smerovania zároveň
- 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

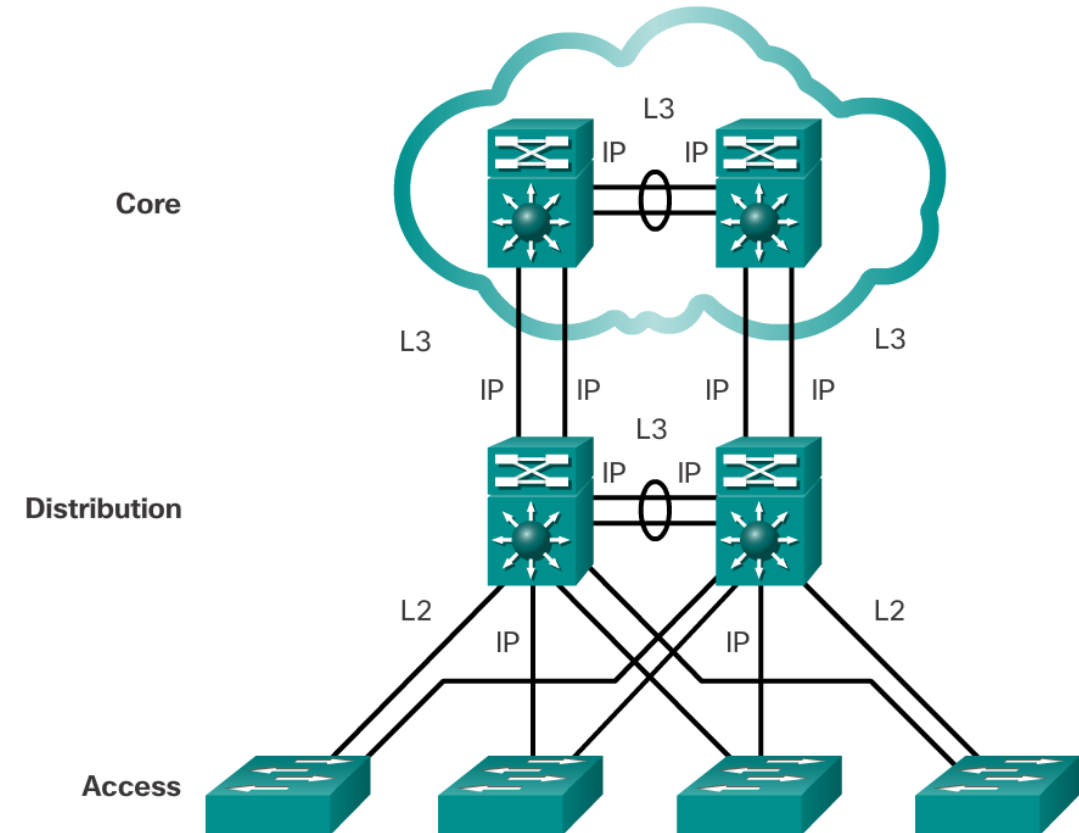
- Príkaz **ip routing** aktivuje podporu pre L3 switching
 - Môžu byť potrebné i dodatočné príkazy
- Po zadaní tohto príkazu je možné na MLS pracovať ako na routeri
 - Smerovacia tabuľka
 - Smerovacie protokoly



```
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
```


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





Ďakujem za pozornosť!



Ohodnot' našu CNA na google:

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