



Delíme sieť, ale inak

Čo je to VLAN?



EURÓPSKA ÚNIA

Európsky sociálny fond
Európsky fond regionálneho rozvoja



OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE



MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Zopakujme si:

- Čo je to sieť?
- Ako sa nazýva proces delenia siete na menšie časti?
- Aké typy vysielania (z hľadiska počtu prijímateľov) poznáme?
- Aké zariadenie je potrebné na oddelenie sietí?
- Aké sú výhody a nevýhody spôsobu delenia siete, ktorý už poznáte?



Obsah

Definícia VLAN

Rozsahy VLAN

Typy VLAN

Značkovanie rámcov vo VLAN

Módy rozhraní pri VLAN

Výhody a nevýhody VLAN

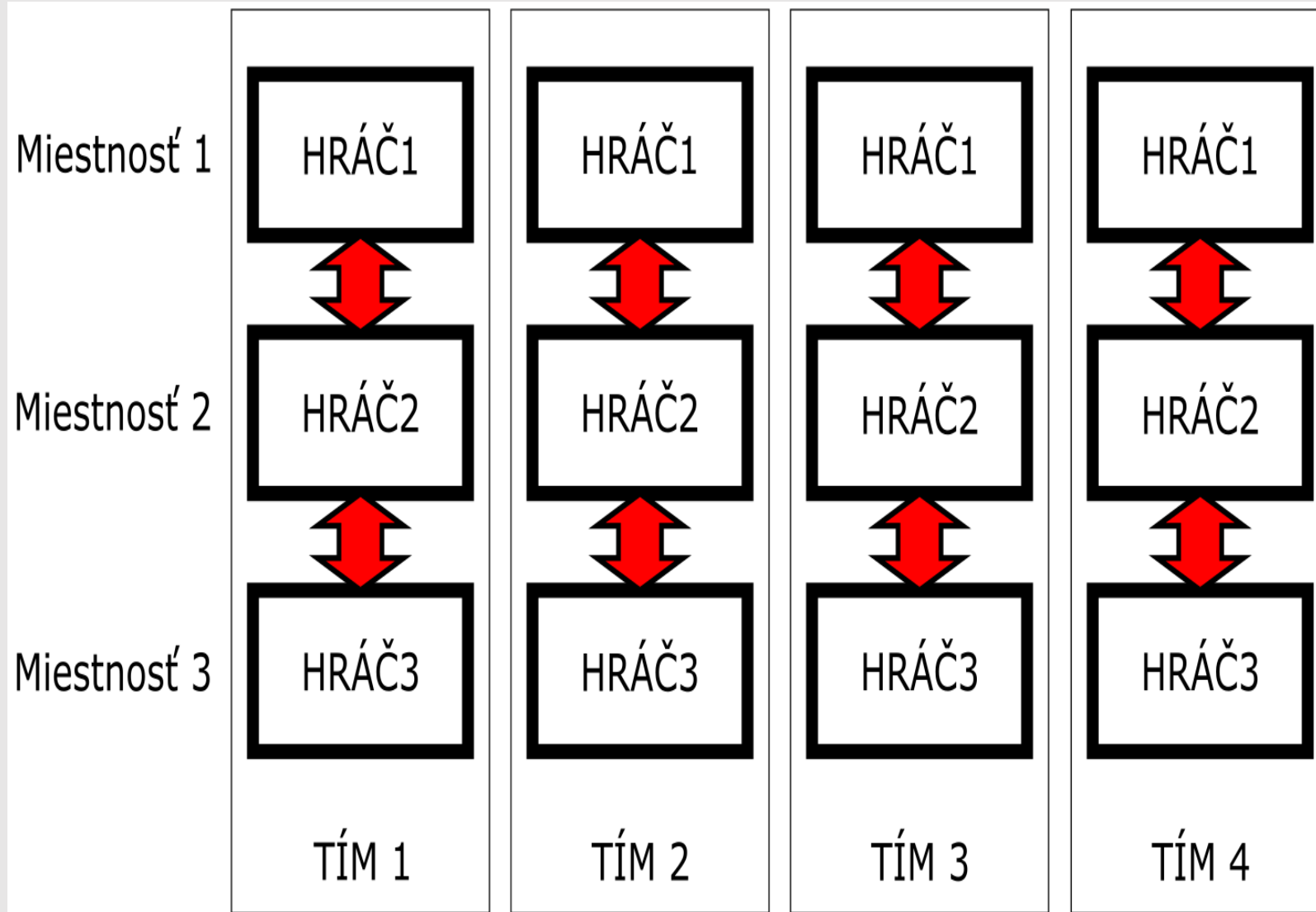


Navrhujeme sieť: Aktivita (18.1)

- Predstavte si PC herňu, ktorá je rozložená v 3 miestnostiach budovy
- Do herne prišlo trénovať viacero tímov, aby sa pripravilo na dôležitý turnaj
- Jeden hráč v tíme vytvorí server (ako pri Counter Strike) a ostatní sa k nemu pripoja
- Hráči v herni si však neposadali k sebe, ale každý sa posadil tam, kde mu to vyhovuje
- Stalo sa teda, že hráči jedného tímu sú usadení vo viacerých miestnostiach
- Skúste využiť Vaše doterajšie vedomosti a načrtnúť návrh hernej siete podľa nasledujúcich požiadaviek

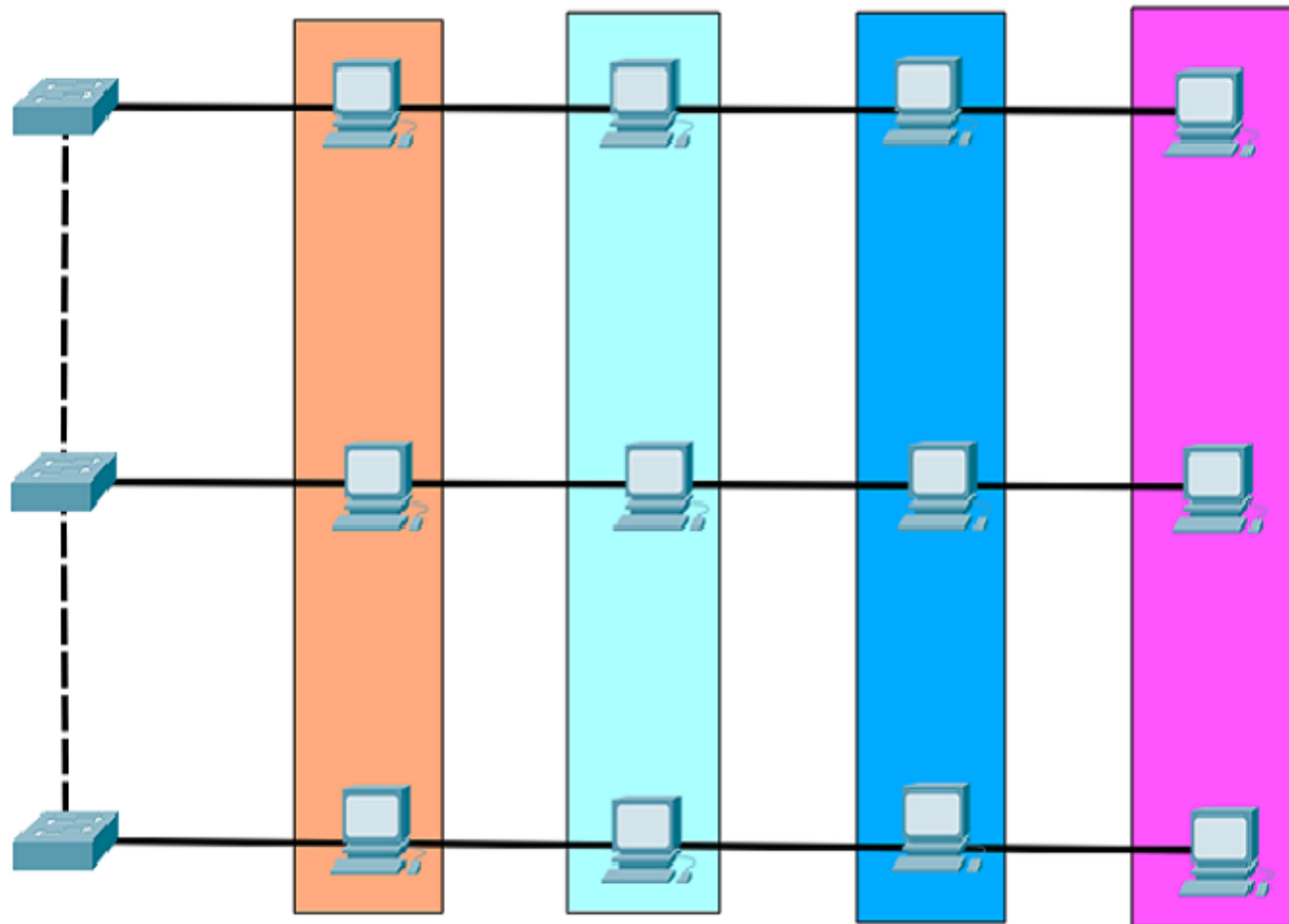
Navrhujeme sieť: Aktivita (18.1)

- Užívatelia v 1 sieti nesmú zasahovať do inej siete – **odhalenie tímovej stratégie**
- Zariadenia v rovnakých herných tímoch sa musia správať tak, ako keby boli súčasťou 1 LAN – **lokálny herný server**
- Použite čo najmenej zariadení – **náklady, spoľahlivosť**



Realizácia aktivity 18.1 pomocou VLAN

- Dodržané všetky požiadavky hráčov
- Len 3 zariadenia (prepínače)



Definícia VLAN

- VLAN je definovaná ako logická broadcastová oblasť.
- Logická = tváriaca sa ako...
- Umožňuje oddelenie jednotlivých sietí bez použitia smerovača
- Prináša možnosť oddeľovania sietí podľa:
 - Funkcie (pre VoIP, kamerový systém a pod.)
 - Príslušnosti k oddeleniu firmy
 - Potreby použitia špeciálnych aplikácií a služieb
- Realizujeme na zariadeniach 2. vrstvy - prepínačoch

Identifikácia VLAN

Každá VLAN je identifikovaná jedinečným číslom/identifikátorom (ID) = na prepínači nemôžu existovať 2 VLAN-y s rovnakým ID

VLAN-y je možné si pomenovávať – uľahčí to orientáciu v topológii a aj prípadné hľadanie chýb v topológiách

Rozsahy VLAN

Vzhľadom na nasadenie a špeciálnu funkciu sú VLAN rozdelené nasledovne:

1. Normálny rozsah
2. Špeciálne VLAN
3. Rozšírený rozsah

Normálny rozsah

- Je rozsah VLAN s identifikátormi od 1 do 1005
- Informácie o týchto VLAN sú uložené v špeciálnom súbore vlan.dat vo Flash pamäti prepínača
- Používajú sa pri realizácii malých a stredných sietí



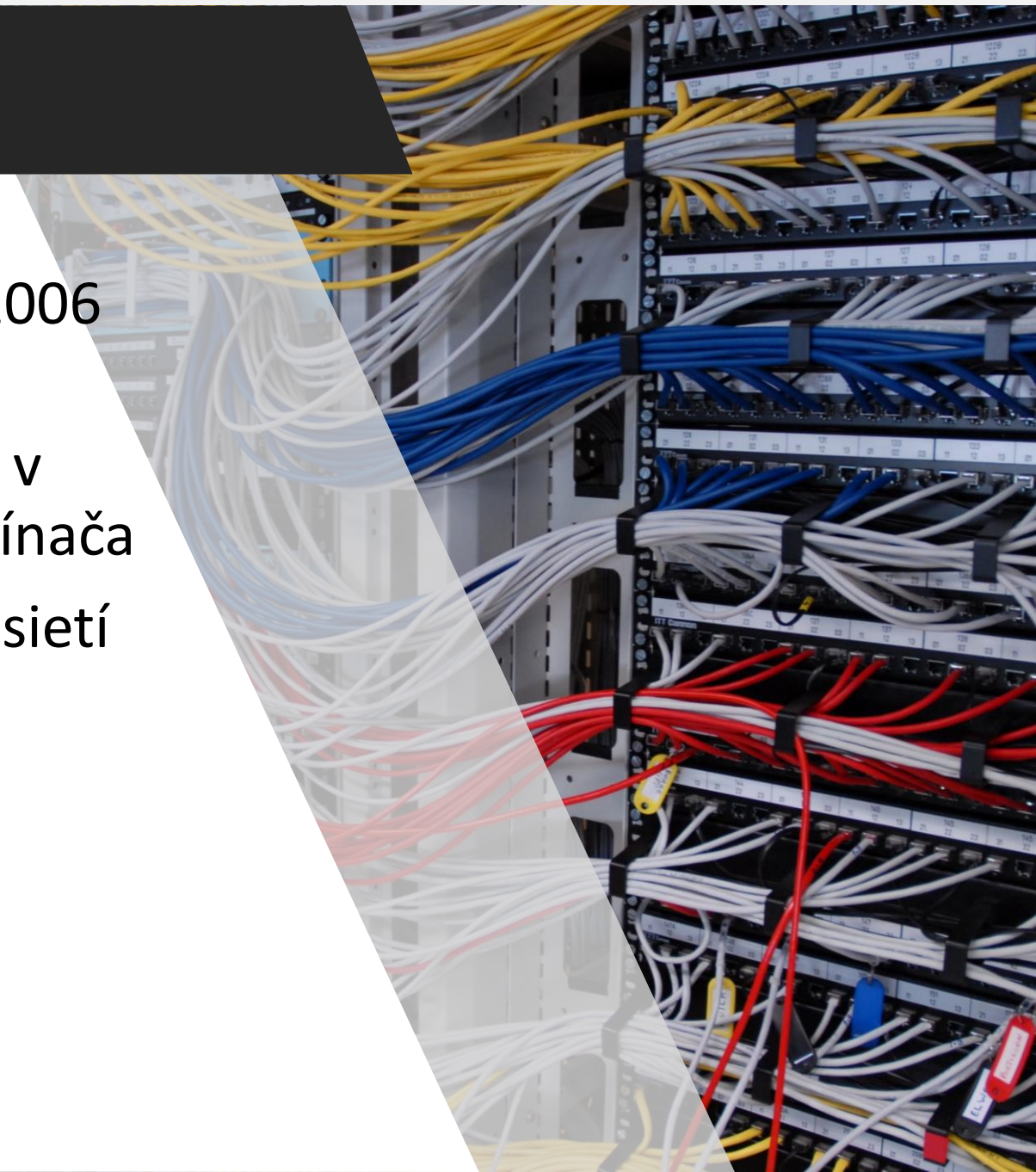
Špeciálne VLAN

- Sú to VLAN s predvolenou funkcionalitou
- Sú vytvárané automaticky a nemôžu byť vymazané
- K špeciálnym VLAN patria VLAN1 a VLAN1002 – VLAN1005
- VLAN1002 – VLAN1005 sú určené pre realizáciu Token Ring a FDDI sietí



Rozšírený rozsah VLAN

- Je rozsah VLAN s identifikátormi od 1006 do 4094
- Informácie o týchto VLAN sú uložené v bežiacej (aktuálnej) konfigurácii prepínača
- Používajú sa pri realizácii rozsiahlych sietí



Typy VLAN

Podľa typu komunikácie resp. podľa špecifického určenia rozdeľujeme VLAN-yna:

1. Dátová (Data) VLAN
2. Predvolená (Default) VLAN
3. Natívna (Native) VLAN
4. Parkovacia VLAN
5. Hlasová (Voice) VLAN
6. Správcovská (Management) VLAN



Dátová VLAN

- Slúži výhradne na prenos užívateľských dát
- Priradíme do nej užívateľov (užívateľské zariadenia)



Predvolená (Default) VLAN

- Po zapnutí prepínača sú jej súčasťou všetky rozhrania
- Zabezpečuje hlavnú funkciu prepínača bez nutnosti akejkoľvek konfigurácie
- Táto VLAN má identifikátor 1 (VLAN1)



Natívna (Native) VLAN

- Slúži na prenos dát medzi prepínačmi, na ktorých je vytvorená viac ako 1 VLAN
- Slúži na prenos neznačkových (netagovaných) dát – cez porty, ktoré nie sú súčasťou konkrétnej VLAN
- Predvolenou natívnou VLAN býva nastavená VLAN1 – **bezpečnostné riziko**



Parkovacia VLAN

- Slúži na „zaparkovanie“ nepoužívaných rozhraní prepínača
- Nesmie sa použiť na žiadny iný účel – **bezpečnostné riziko**



Hlasová (Voice) VLAN

VLAN na prenos hlasu (Voice over IP – Hlas cez IP) musí spĺňať niekoľko parametrov:

- Dostatočná priepustnosť
- Vysoká priorita hlasových paketov
- Rýchle smerovanie medzi zaťaženými uzlami siete
- Oneskorenie maximálne 150 ms

Tieto parametre sú dosiahnuté úplným oddelením hlasových prenosov od iných užívateľských dát (dátových VLAN)



Správcovská (Management) VLAN

- Slúži na vzdialenú správu zariadení
- Nesmie byť používaná na iné účely (prenos užívateľských dát a pod.)
- Nerealizujeme pomocou predvolenej VLAN (VLAN1)



Módy rozhraní pri VLAN

V závislosti na funkcii alebo na type zariadení, ktoré k rozhraniám prepínača pripájame, nastavujeme rozhrania vo VLAN do jedného z nasledovných módo:

1. Staticky konfigurované – fungujú len v pevne nastavenom móde
 - a) PRÍSTUPOVÝ (ACCESS)
 - b) TRUNK
2. Dynamicky konfigurované – prispôsobia sa módu rozhrania na opačnom konci linky
 - a) DYNAMIC AUTO
 - b) DYNAMIC DESIRABLE

Rozhranie v móde ACCESS

- Slúži na pripojenie koncových zariadení (PC, tlačiareň, IP kamera a pod.).
- Spravidla býva súčasťou niektorej z dátových alebo správcovských VLAN.
- Cez rozhranie sa prenášajú informácie len z VLAN, ku ktorej je priradené.
- Rozhranie môže patriť len 1 VLAN
 - výnimkou je iba rozhranie pre IP telefón, ktoré môže patriť hlasovej (voice) a zároveň dátovej (data) VLAN



Rozhranie v móde TRUNK

- Slúži na prepojenie prepínač – prepínač, alebo prepínač – smerovač (spomenieme neskôr)
- Prenáša informácie z viacerých VLAN medzi prepínačmi
- Rozhranie nemôže patriť žiadnej VLAN



Rozhranie v móde DYNAMIC AUTO

- Prispôsobí sa zariadeniu na opačnom konci linky
- Uprednostňuje mód ACCESS
- Vyjednávanie prebieha pomocou protokolu DTP (Dynamic Trunking Protocol)

Veľké bezpečnostné riziko – po nakonfigurovaní a sfunkčnení linky nastaviť linku do vyjednaného módu (access/trunk)



Rozhranie v móde DYNAMIC DESIRABLE

- Prispôsobí sa zariadeniu na opačnom konci linky
- Uprednostňuje mód TRUNK
- Vyjednávanie prebieha pomocou protokolu DTP (Dynamic Trunking Protocol)

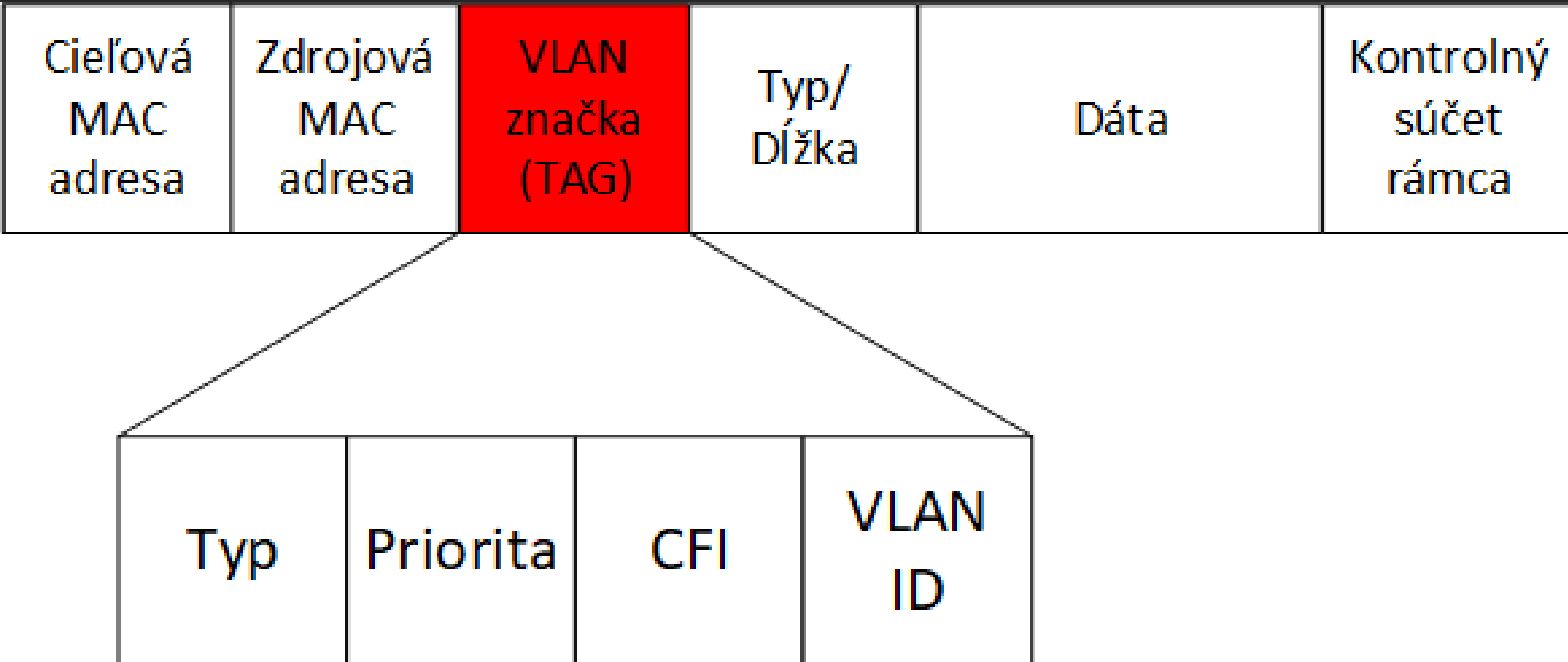
Veľké bezpečnostné riziko – po nakonfigurovaní a sfunkčnení linky nastaviť linku do vyjednaného módu (access/trunk)



Značkovanie rámcov vo VLAN

- Aby sa rámec (dáta) dostali na správne miesto určenia (do správnej VLAN), musia sa označovať.
- Značka nesie informáciu, z ktorej VLAN rámec vychádza resp. do ktorej VLAN smeruje.
- Na značkovanie sa využíva štandard IEEE 802.1Q

Čo sa nachádza vo VLAN značke rámca?



VLAN značka - popis

Typ – identifikátor protokolu

Priorita – uprednostnenie rámca pred inými

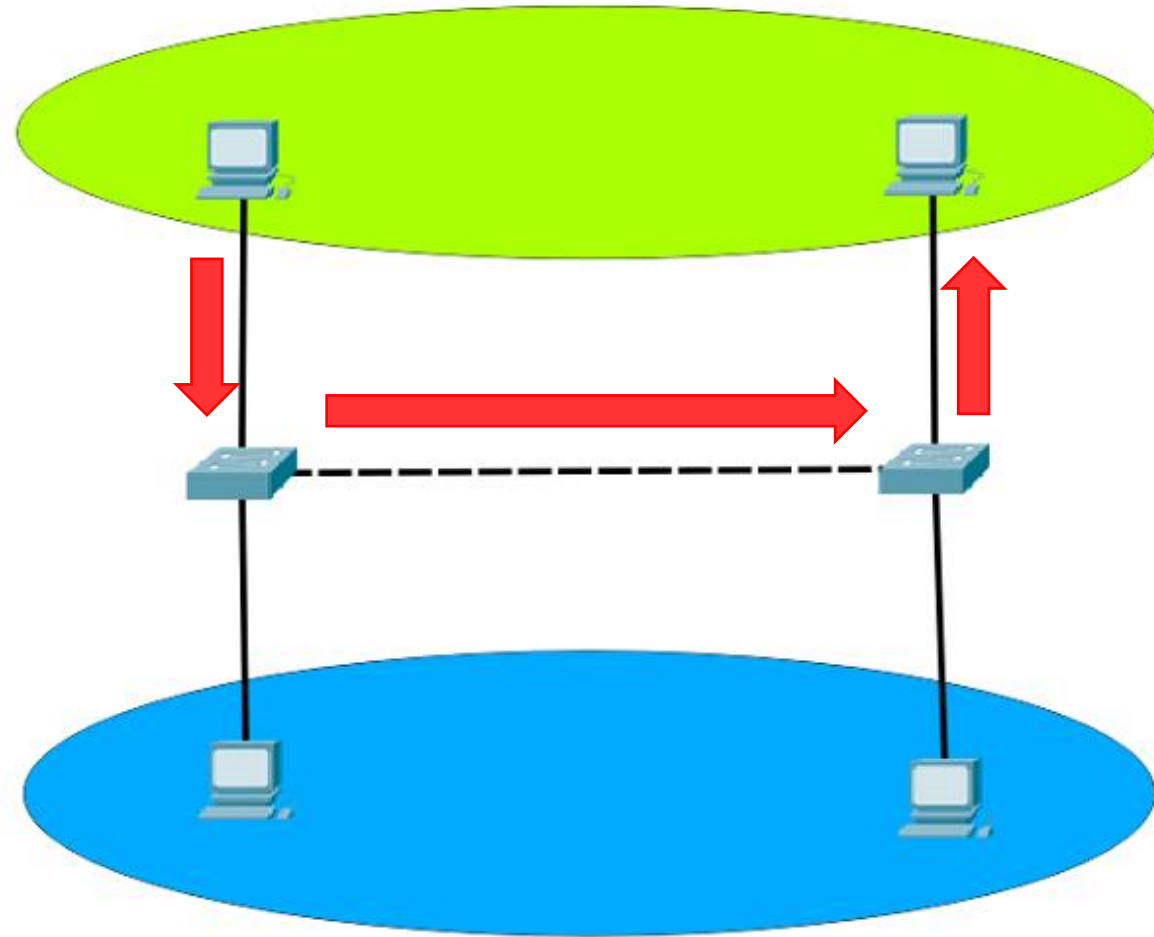
CFI – umožňuje prenos token-ring rámcov prostredníctvom Ethernet protokolu

VLAN ID – identifikátor VLAN



Kedy sa rámec značkuje?

- Ak je rámec posielaný cez trankovú linku do zariadenia v rovnakej VLAN, musí byť označovaný.



CAM tabuľka

Obsahuje záznamy o VLAN, MAC adresách jednotlivých zariadení a portoch, ku ktorým sú tieto zariadenia pripojené.

Mac Address Table

Vlan	Mac Address	Type	Ports
1	000a.417a.6e18	DYNAMIC	Fa0/24
10	0003.e426.0bc8	DYNAMIC	Fa0/24
10	000a.41ba.a89b	DYNAMIC	Fa0/2
20	000b.be34.d316	DYNAMIC	Fa0/11
20	000c.8589.772c	DYNAMIC	Fa0/24

Zobrazenie CAM tabuľky

```
>enable  
#show mac-address-table
```

Skúmame CAM tabuľku: *Aktivita (18.2)*

Pri aktivite využijeme:

- pracovný list
- vzorovú topológiu

