

# **Virtual LAN, VLAN trunking, Virtual Trunking Protocol Module 8; 9**

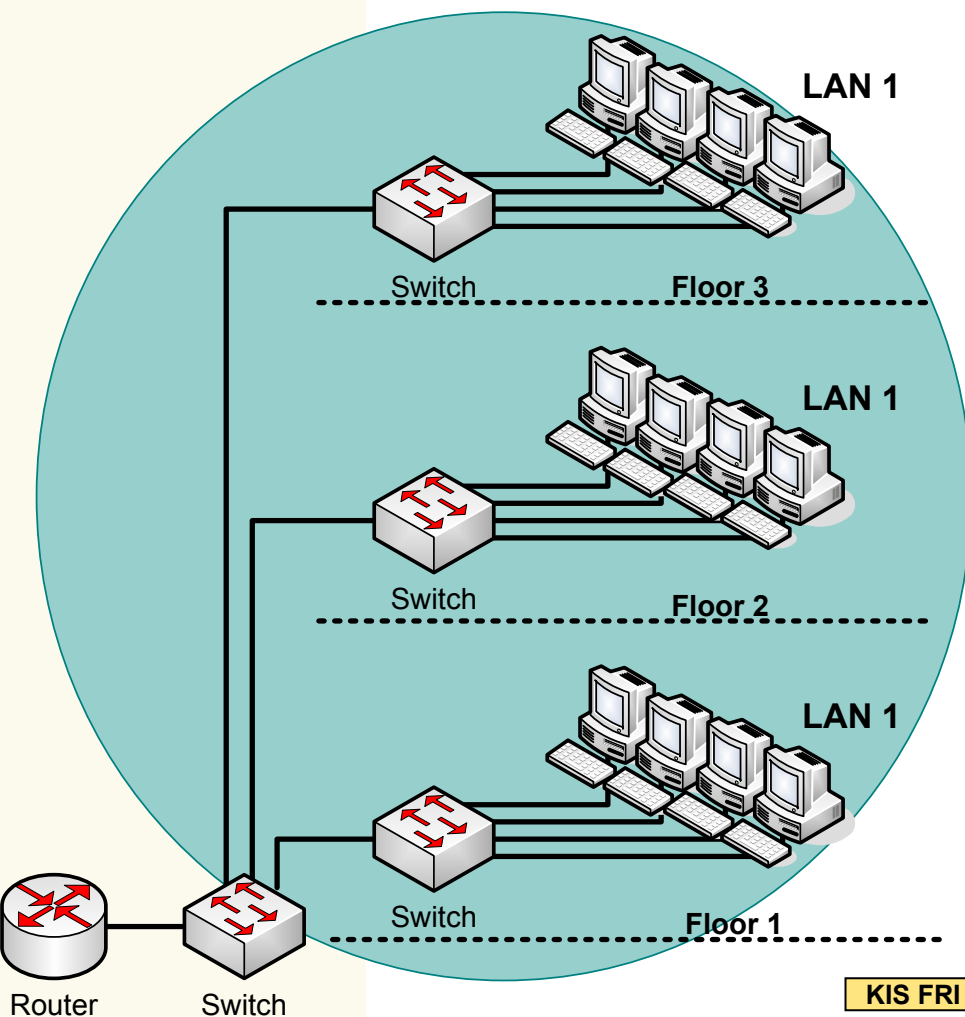
Prednáška 7

# VLAN

- Dôležitá vlastnosť Ethernet LAN prepínačov
- Virtual LAN (VLAN):
  - VLAN umožňujú logicky segmentovať fyzické, prepínané LAN siete
    - Doteraz logické delenie záviselo od fyzickej dostupnosti portov prepínanej LAN siete
  - Získame
    - Možnosti riadenia toku
    - Oddelenie fyzickej (geografickej) topológie od logickej
    - Môžeme vytvárať LAN siete napr.
      - Podľa funkcií v organizácií
      - Projektových tímov
      - Aplikácií a pod.

# Tradičné LAN

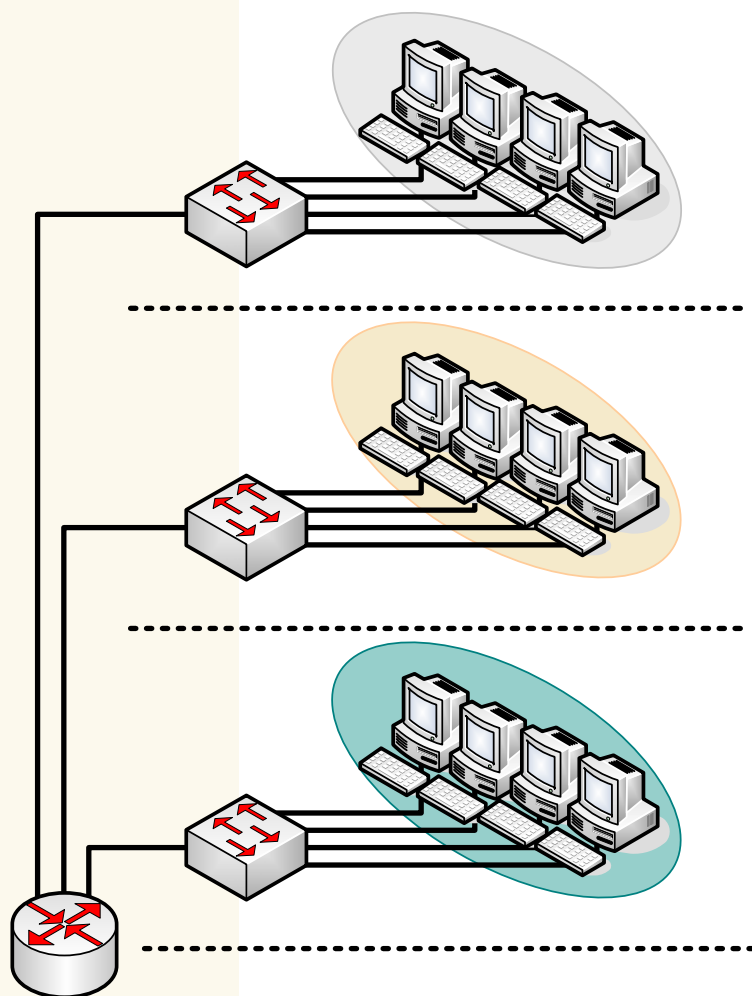
Traditional LAN segmentation



## ■ Tradičné LAN

- Nie je možné uskutočniť delenie koncových staníc podľa iných funkcií ako dostupnosť portov LAN sietí
- Zariadenia je možné umiestniť len na daný fyzický segment

# Tradičné LAN



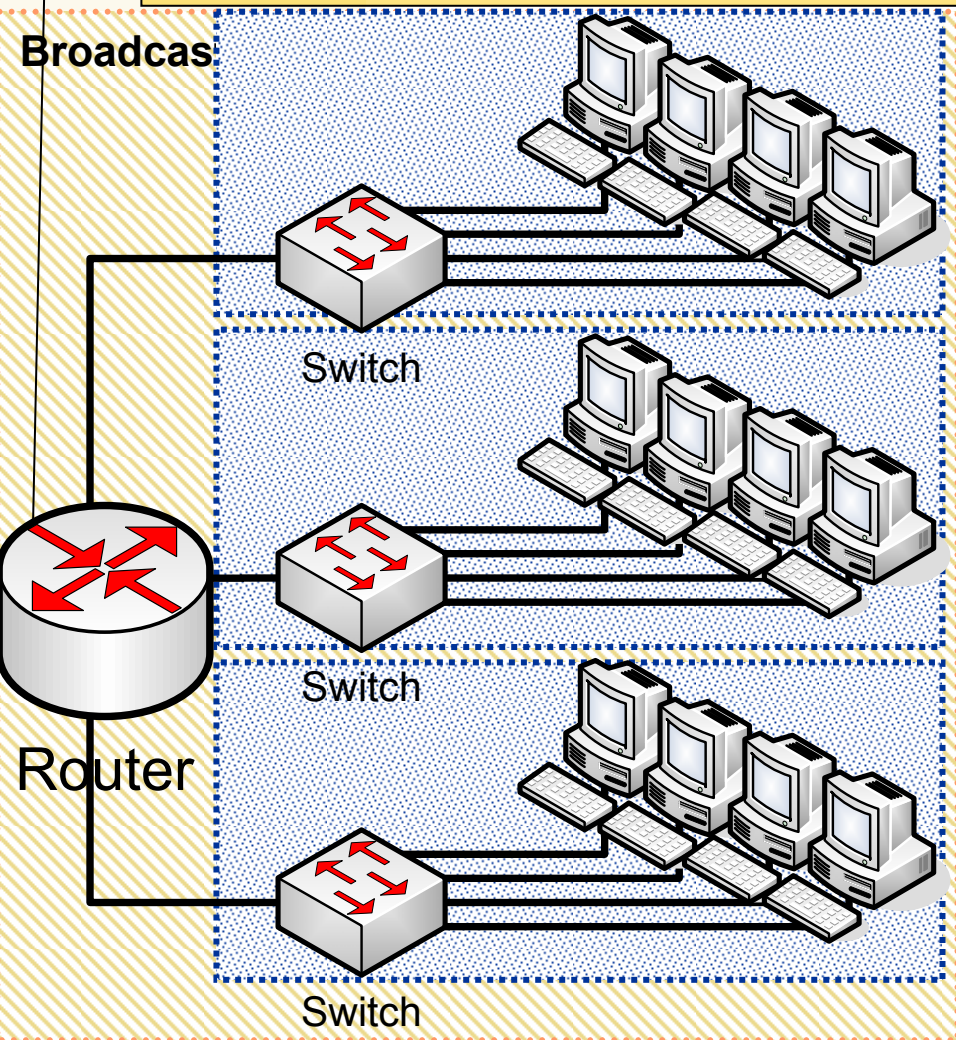
- Segmentácia siete, riadenie toku
- L3 zariadením (smerovač)

**Traditional LAN segmentation**

**LAN 3**

Ak chceme  
„rozbiť“  
Bcast  
doménu,  
musíme použiť  
Router

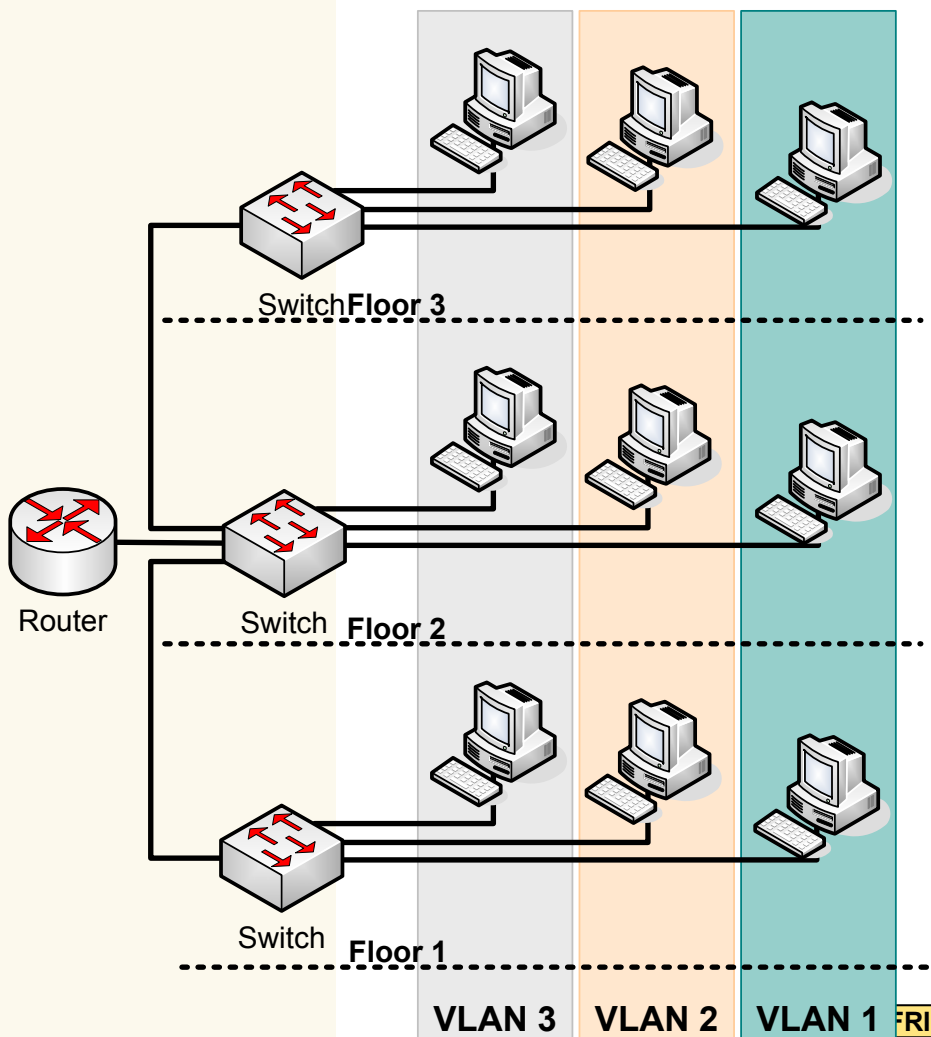
# Broadcast domény



- V tradičných LAN Broadcast doména:
  - Všetky prepínače
  - Všetky porty
- Rozdeliť Bcast doménu
  - Smerovač

# Virtuálna LAN

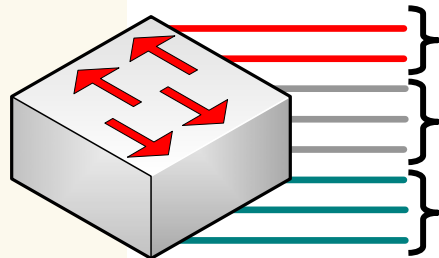
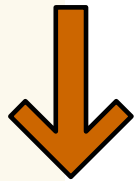
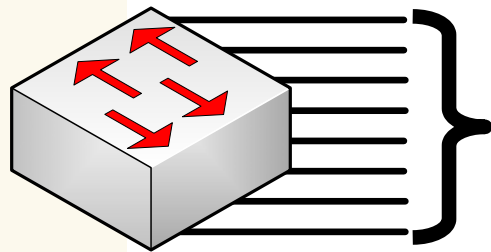
VLAN segmentation



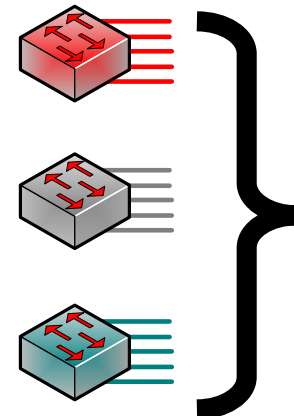
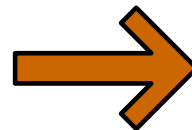
## ■ Virtuálna LAN

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

# Princíp VLAN

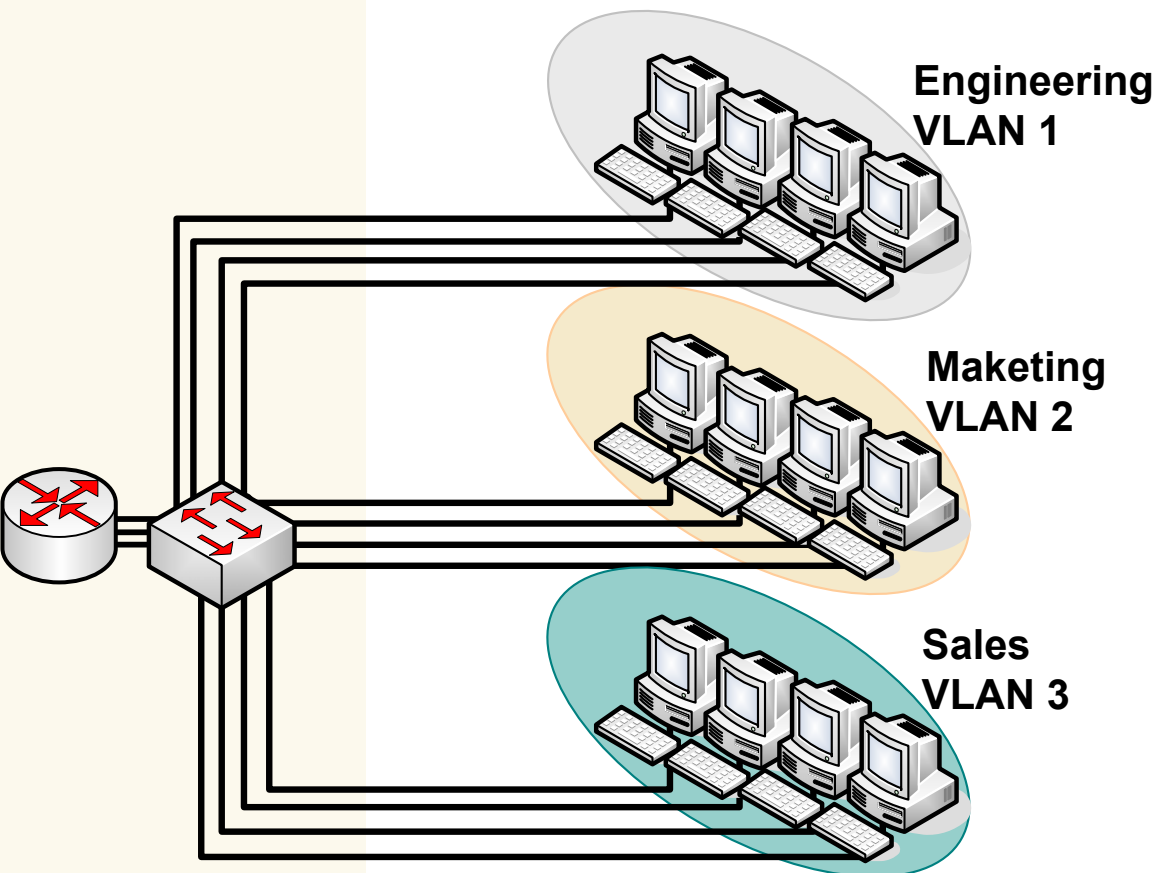


**VLAN  
supported  
LAN switch**



All ports  
same L  
(function  
as tradit  
LAN sw

# Broadcast domény a VLAN



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



# Broadcast domény a VLAN

## ■ Tradičné LAN

- Všetky porty prepínača
- Všetky prepínače prepínanej LAN siete
  - = **jedna broadcast doména**

## ■ VLAN

- Jeden prepínač podporuje **viac** VLAN
- Jedna VLAN
  - Sa môže rozprestierať nad jedným or viac prepínačmi
- Každá VLAN
  - Tvorí **samostatnú** broadcast doménu
    - Bcast rámce šírené len na portoch tej istej VLAN
    - Nie sú pre posielané na porty iných VLAN (aj toho istého prepínača)
  - Unicast rámce sú šírené len na portoch tej istej VLAN
- Každá VLAN samostatný IP adresný priestor
- Na **prepojenie viacerých VLAN je potrebné použiť smerovač!!!**

# Typy VLAN

## ■ Typy VLAN

### ■ Statické

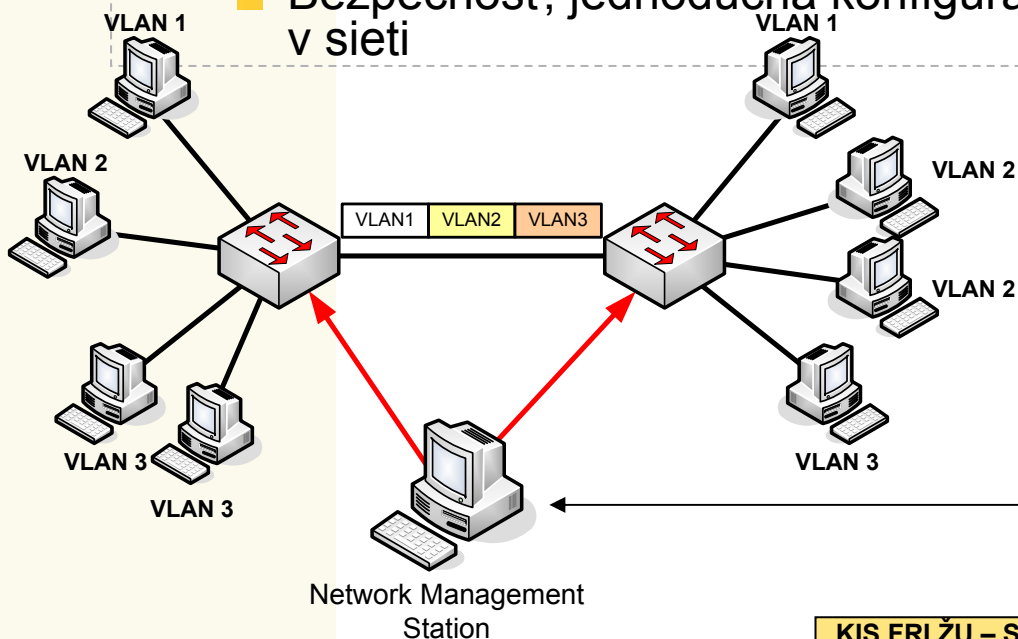
- Manuálne konfiguruje administrátor

### ■ Dynamické

- Dynamické určenie členstva na základe určitých kritérií

# Statické VLAN

- Členstvo vo VLAN nastavuje administrátor manuálne
  - Priraduje fyzický port prepínača do VLAN
  - Kým administrátor nezmení priradenie portu je členom danej VLAN
- Známe aj ako
  - port-based, port-centric
- Výhody
  - Bezpečnosť, jednoduchá konfigurácia a monitorovanie pohybu staníc v sieti

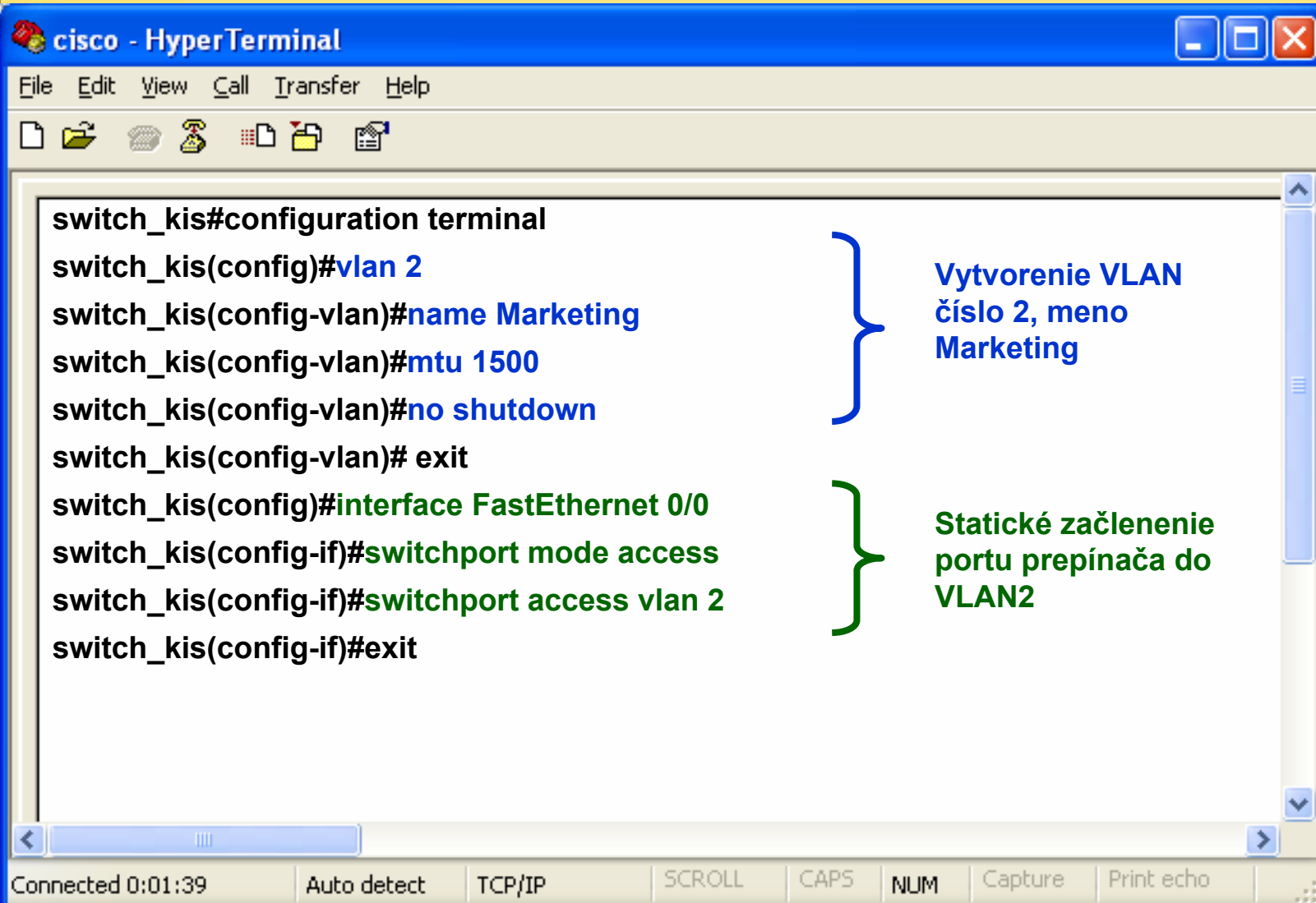


The screenshot shows the 'Modify Port Mode' configuration window for a switch port. The configuration is as follows:

Field	Value
Device:	sw_2950T_kis
Port:	Fa0/14
Administrative Mode:	Dynamic Desirable
Administrative Encapsulation:	802.1Q
Operating Mode:	Static Access
Operating Encapsulation:	Native
Static-Access VLAN [1-1005]:	1
Trunk-Allowed VLANs [all, 1-1005]:	ALL
Pruning VLANs[none, [2-1001]]:	2-1001
Native VLAN:	1

Buttons: OK, Cancel, Help

# Statické VLAN – Vytvorenie VLAN a začlenenie portu



The screenshot shows a Cisco HyperTerminal window with a blue title bar and a menu bar (File, Edit, View, Call, Transfer, Help). Below the menu bar is a toolbar with icons for file operations. The main text area displays the following commands:

```
switch_kis#configuration terminal
switch_kis(config)#vlan 2
switch_kis(config-vlan)#name Marketing
switch_kis(config-vlan)#mtu 1500
switch_kis(config-vlan)#no shutdown
switch_kis(config-vlan)# exit
switch_kis(config)#interface FastEthernet 0/0
switch_kis(config-if)#switchport mode access
switch_kis(config-if)#switchport access vlan 2
switch_kis(config-if)#exit
```

Two blue curly braces on the right side of the terminal window group the commands into two sections:

- The first brace groups the commands for creating the VLAN: `switch_kis(config)#vlan 2`, `switch_kis(config-vlan)#name Marketing`, `switch_kis(config-vlan)#mtu 1500`, and `switch_kis(config-vlan)#no shutdown`. To the right of this brace is the text: "Vytvorenie VLAN číslo 2, meno Marketing".
- The second brace groups the commands for assigning the port to the VLAN: `switch_kis(config)#interface FastEthernet 0/0`, `switch_kis(config-if)#switchport mode access`, `switch_kis(config-if)#switchport access vlan 2`, and `switch_kis(config-if)#exit`. To the right of this brace is the text: "Statické začlenenie portu prepínača do VLAN2".

The status bar at the bottom of the window shows "Connected 0:01:39" and several tabs: "Auto detect", "TCP/IP", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

# show vlan (Cisco IOS)

C:\ Telnet 158.193.152.20

switch# show vlan

ULAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
2	Testovacia	active	
3	Marketing	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

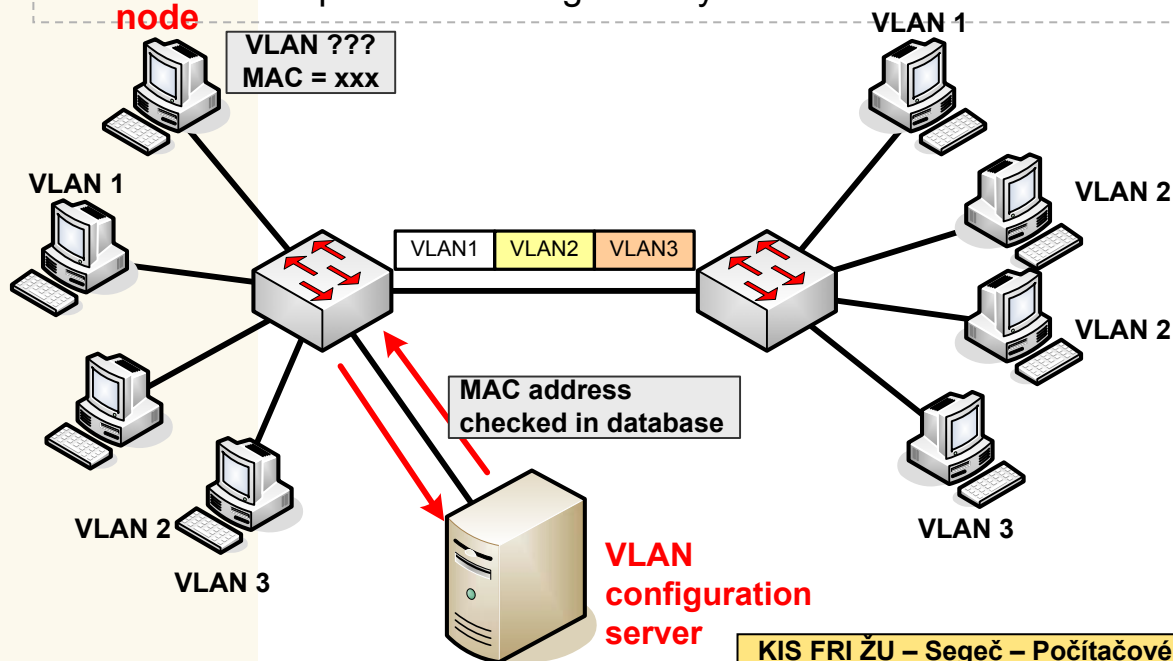
ULAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	1002	1003
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	1	1003
1003	tr	101003	1500	1005	-	-	-	srp	1	1002
1004	fdnet	101004	1500	-	-	1	ibm	-	0	0
1005	trnet	101005	1500	-	-	1	ibm	-	0	0

Remote SPAN VLANs

Primary	Secondary	Type	Ports
---------	-----------	------	-------

# Dynamické VLAN

- Pridelovanie členstva dynamicky
- V okamihu keď sa host pripojí na port
  - Na základe:
    - MAC adresy pripojeného hosta
    - IP adresy
    - Typ protokolu
  - Vyžaduje sa **konfiguračný server** v sieti
    - Správne nakonfigurovaný



# Výhody VLAN

- Jednoduché premiestňovanie pracovných staníc na LAN
- Jednoduché pridávanie staníc do LAN
- Jednoduchá zmena konfigurácie LAN
- Zvýšená bezpečnosť
  - Izolácia prevádzky na VLAN
  - Ľahká kontrola sieťovej prevádzky
  - Použitie smerovačov
- Zvýšená priepustnosť
  - Segmentácia siete
    - Menej staníc, ktoré sa delia o prenosovú kapacitu
  - Redukcia broadcastu v sieti

# **Komunikácia v a medzi VLAN**



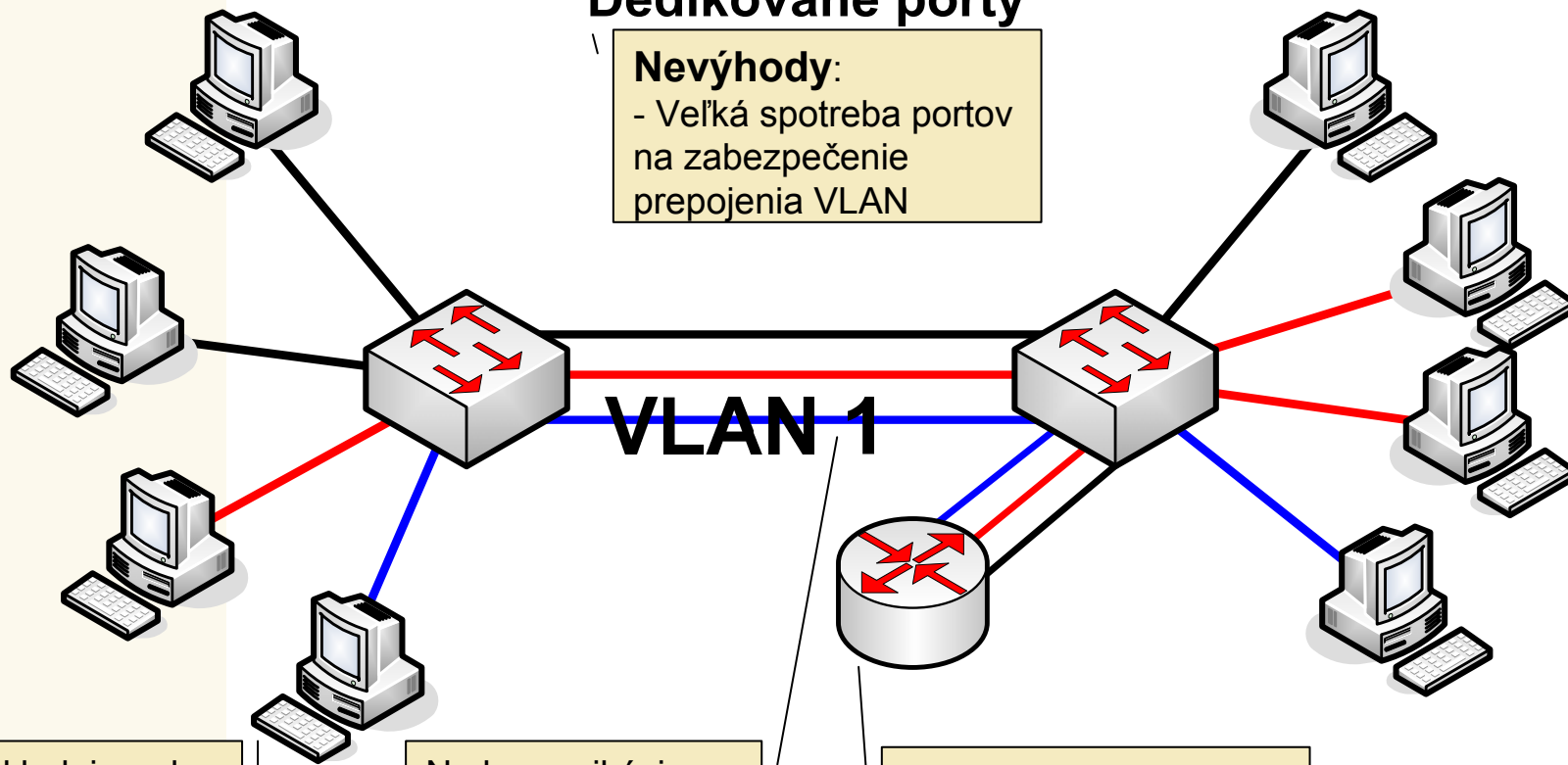


# Intra VLAN komunikácia - Dedikované porty

## Dedikované porty

### Nevýhody:

- Veľká spotreba portov na zabezpečenie prepojenia VLAN

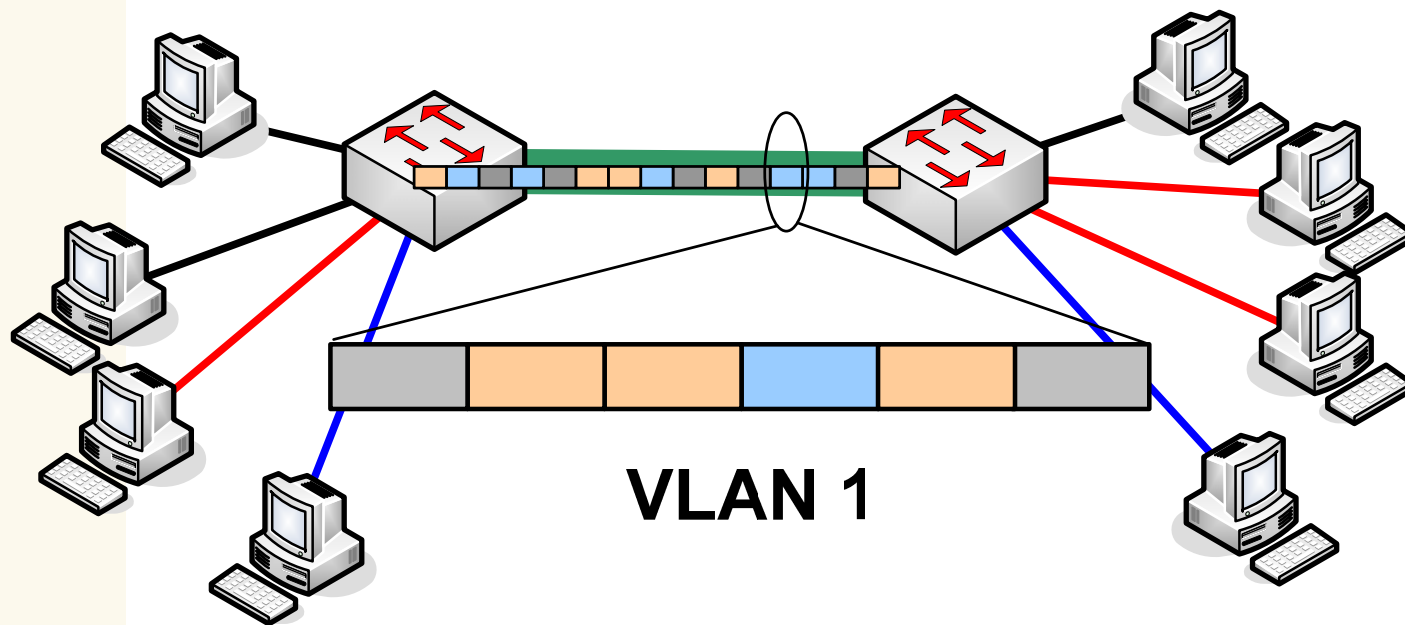


Predpokladajme dva prepínače s nakonfigurovanými 3 VLAN-ami. Ako zabezpečiť ich prepojenie?

Na komunikáciu medzi prepínačmi a VLAN určíme separátne fyzické porty pre každú VLAN.

Na inter VLAN komunikáciu potrebujeme smerovač. Na smerovači pre každú VLAN vyhradené rozhranie (port).

# Intra VLAN komunikácia - Trunking



## Trunk

- Fyzická linka medzi prepínačmi
- Rámce sa **multiplexujú** cez Trunk

**VLAN 1**

- Ako rozlíšiť v multiplexovanom toku do ktorej VLAN patrí ktoré rámce?

- Rozlíšenie značkováním rámcov podľa VLAN
- Tzv. **TAGGING**

**Trunk**

# Trunking

## ■ Trunking

- Poskytuje efektívnu cestu pre komunikáciu medzi prepínačmi
- Cesta ako poskytovať VLAN cez „internetwork“

## ■ Trunk

- Fyzická alebo logická linka
  - „Prenosový kanál medzi dvoma bodmi“
- Tvorí „backbone“ pre rôzne VLAN v prepínanej LAN sieti
- Prepája prepínače navzájom
  - Pre potreby **Intra VLAN** komunikácie
- Prepája prepínač (-e) so smerovačom (-čmi)
  - Pre **Inter VLAN** komunikácie
- Rámce rôznych VLAN sú na trunk-u multiplexované
  - Do rámcov je pridávaný špeciálny TAG (značka)
    - Tzv. TAGGING
    - TAG určuje z/do ktorej VLAN rámce patria
- Býva súčasťou tzv. **Native VLAN**
  - Rámce native VLAN môžu prechádzať trunk-om neznačkové
  - Oba konce trunk-u musia byť v tej istej Native VLAN

# Trunk protokoly

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

**IEEE802.1q a IEEE802.1p**

**Virtual Bridged Local Area  
Networks**

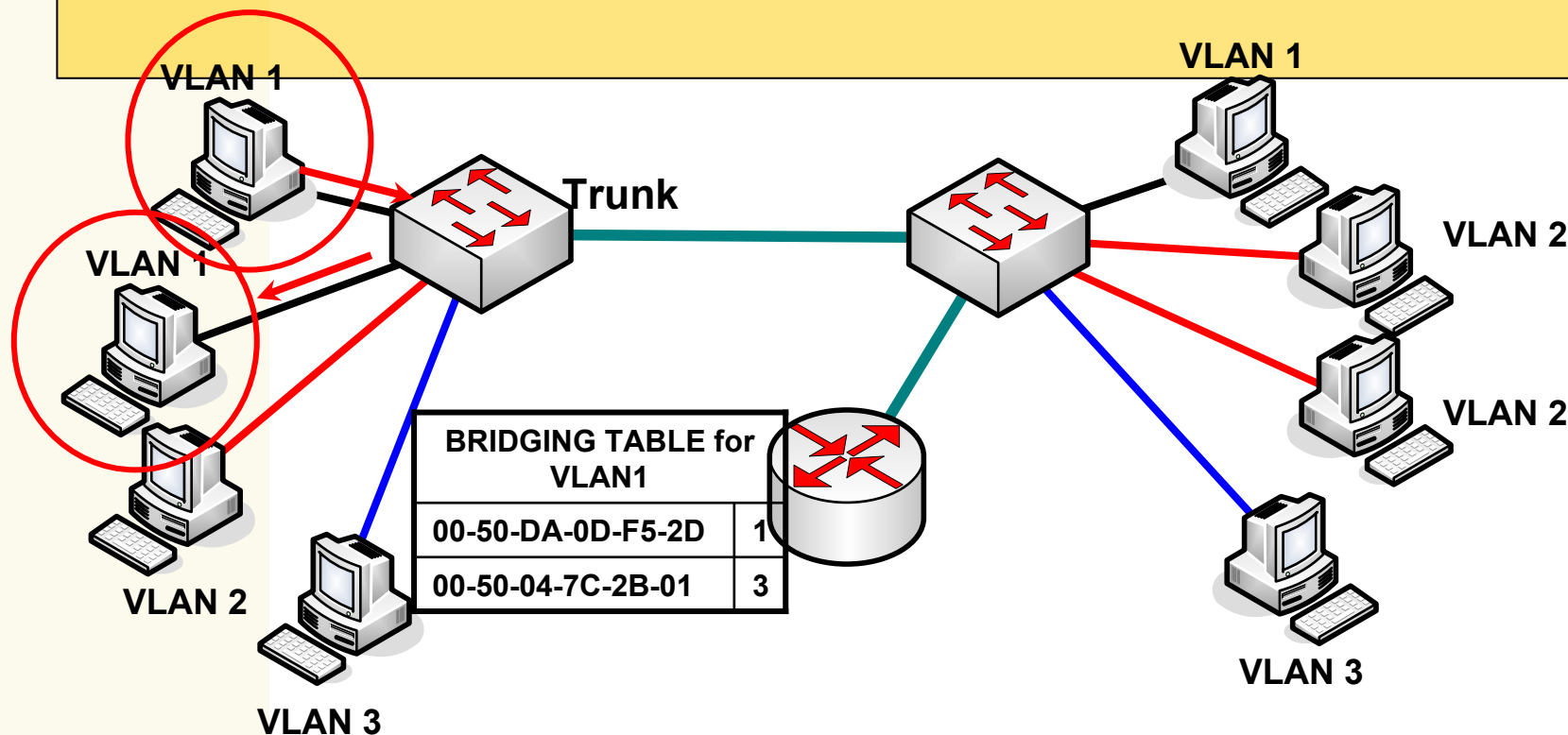
# IEEE 802.1q

- Štandardizovaná značkovacia schéma IEEE (trunk protokol)
  - Zabezpečená interoperabilita zariadení rôznych výrobcov
- Na základe ktorej:
  - Je možné prenášať cez jednu linku (**trunk**) rámce viacerých VLAN
  - Prepínač rozlišuje do ktorej VLAN rámce patria
    - Pridáva, číta **VLAN Identifier** do/z rámcov

# IEEE 802.1q

- IEEE 802.1q mechanizmus
  - Pridáva do rámca 4 bytovú značku (**Tag**)
    - Značka identifikuje rámec a VLAN do ktorej rámec patrí
- Značka sa pridáva
  - Medzi pole Source address a pole Type/Length
  - Pre všetky rámce tečúce cez trunk
  - Pridávanie značky = zmena formátu Ethernet rámca
    - Musí sa prepočítať FCS
- Vysielajúci trunk-prepínač pre rámce vstupujúce na trunk
  - Vloží 4B tag do rámca
  - Prepočíta FCS
  - Pošle rámec cez trunk
- Prijímajúci trunk prepínač (druhá strana)
  - Odstráni tag
  - Skontroluje FCS
  - Prepne rámec do danej VLAN

# 802.1q – Intra VLAN komunikácia



## Príklad:

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

-Prepínač prijme rámec na vstupnom porte (**VLAN Access port**).

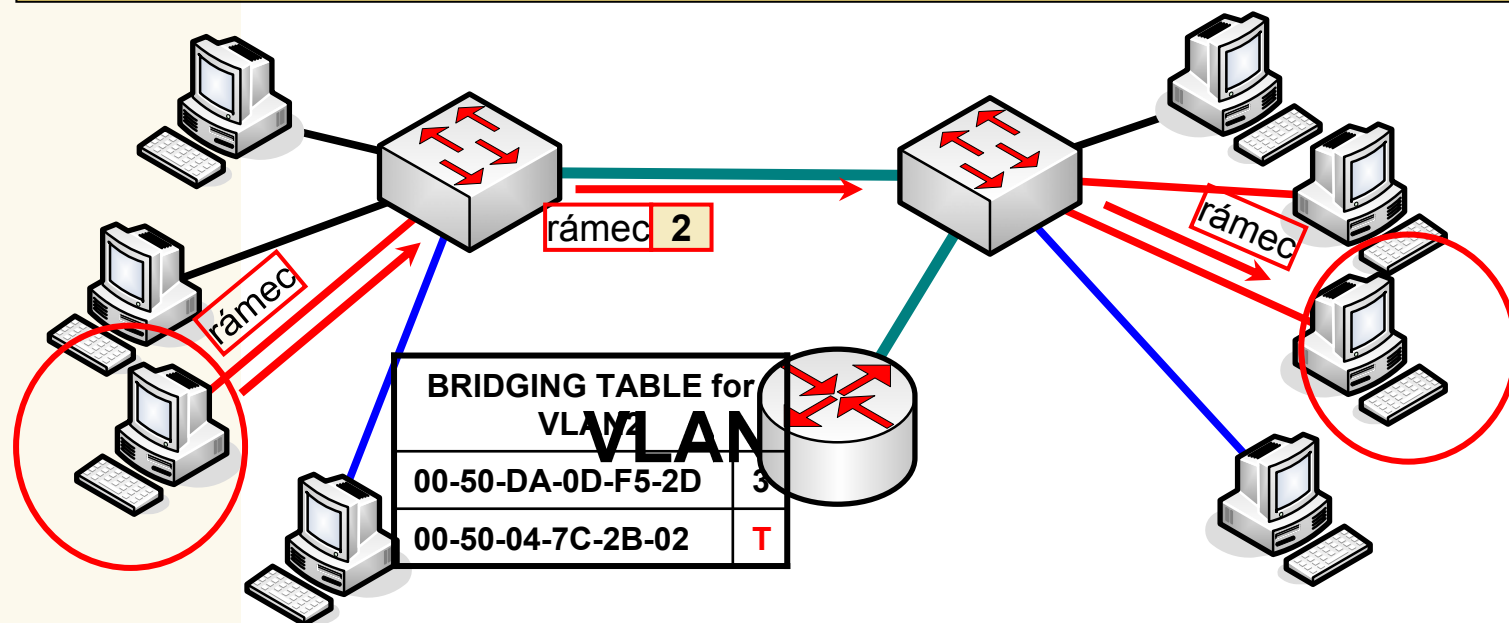
-prezrie Bridging table for VLAN 1  
-prepne rámec na výstupný port

**Rámec nie je pozmenený (značkováný) nakoľko nevstupuje na trunk port!**

- Rámec je prepnutý ako na bežnom prepínači.



# 802.1q – Intra VLAN komunikácia



## Priklad:

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

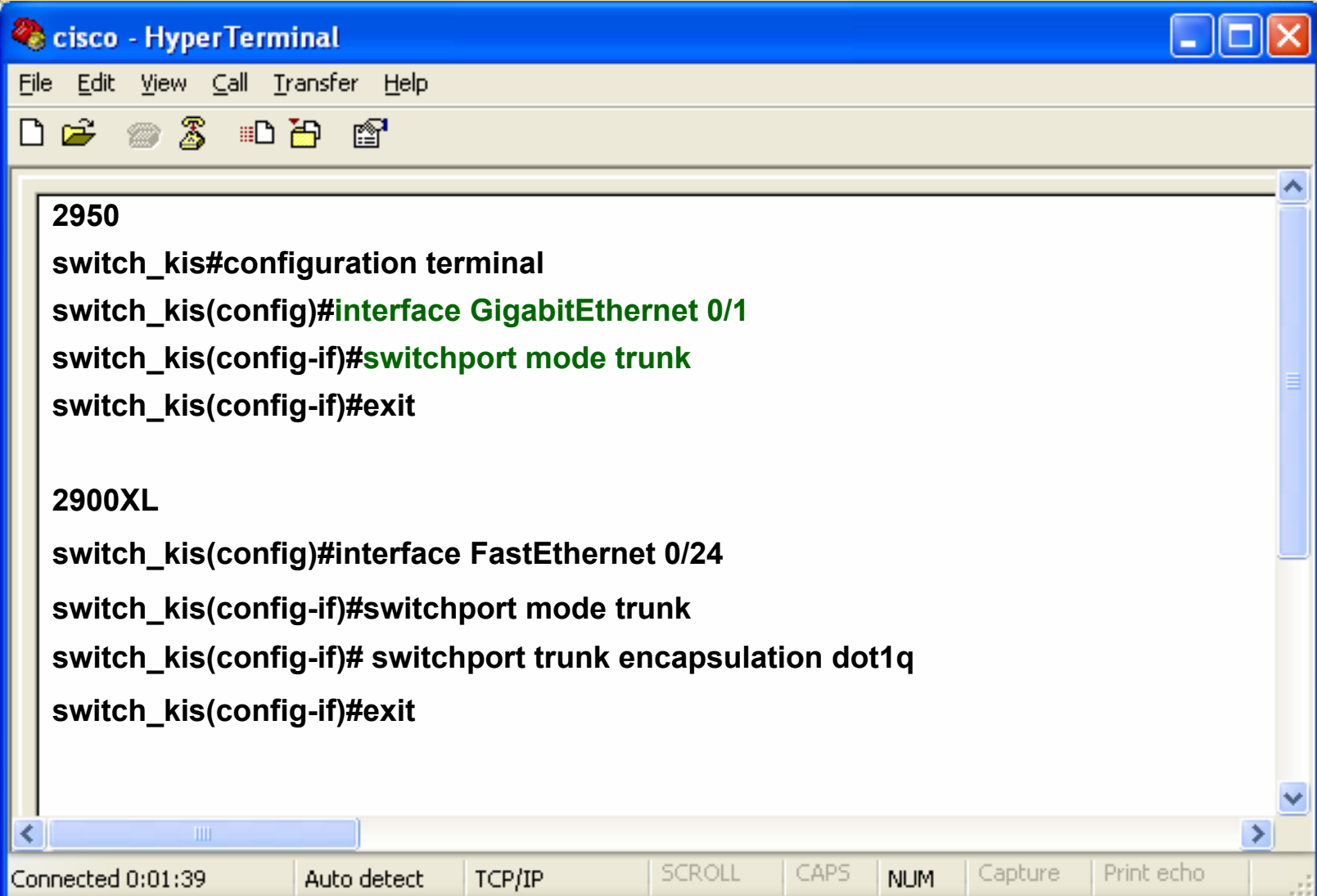
- Prepínač prijme rámec na vstupnom porte (**VLAN Access port**).
- prezrie Bridging table for VLAN 2
- rámec musí byť prepnutý cez trunk
- vloží Tag, identifikujúci, že rámec je pre VLAN 2 (2)
- Prepne rámec na trunk port

- Prijímajúci prepínač prijme rámec
- prezrie Bridging table
- ak cieľová stanica je na jeho porte
- odstráni Tag
- prepne rámec

## Trunk

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

# VLAN – Vytvorenie trunk



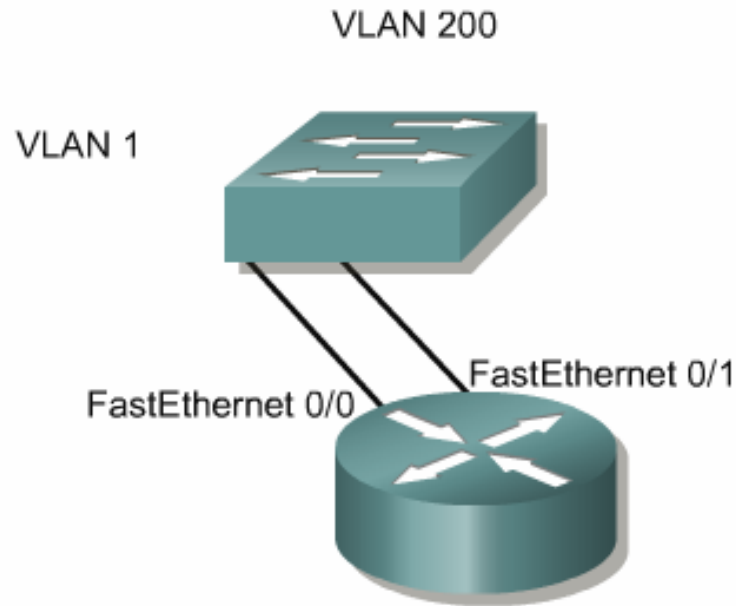
The screenshot shows a Cisco HyperTerminal window with a blue title bar and a menu bar (File, Edit, View, Call, Transfer, Help). Below the menu bar is a toolbar with icons for file operations. The main text area contains configuration commands for two switches. The first switch, 2950, has its GigabitEthernet 0/1 interface configured as a trunk. The second switch, 2900XL, has its FastEthernet 0/24 interface configured as a trunk using dot1q encapsulation. The status bar at the bottom shows connection details and various control buttons.

```
2950
switch_kis#configuration terminal
switch_kis(config)#interface GigabitEthernet 0/1
switch_kis(config-if)#switchport mode trunk
switch_kis(config-if)#exit

2900XL
switch_kis(config)#interface FastEthernet 0/24
switch_kis(config-if)#switchport mode trunk
switch_kis(config-if)# switchport trunk encapsulation dot1q
switch_kis(config-if)#exit
```

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

# Inter-VLAN Routing



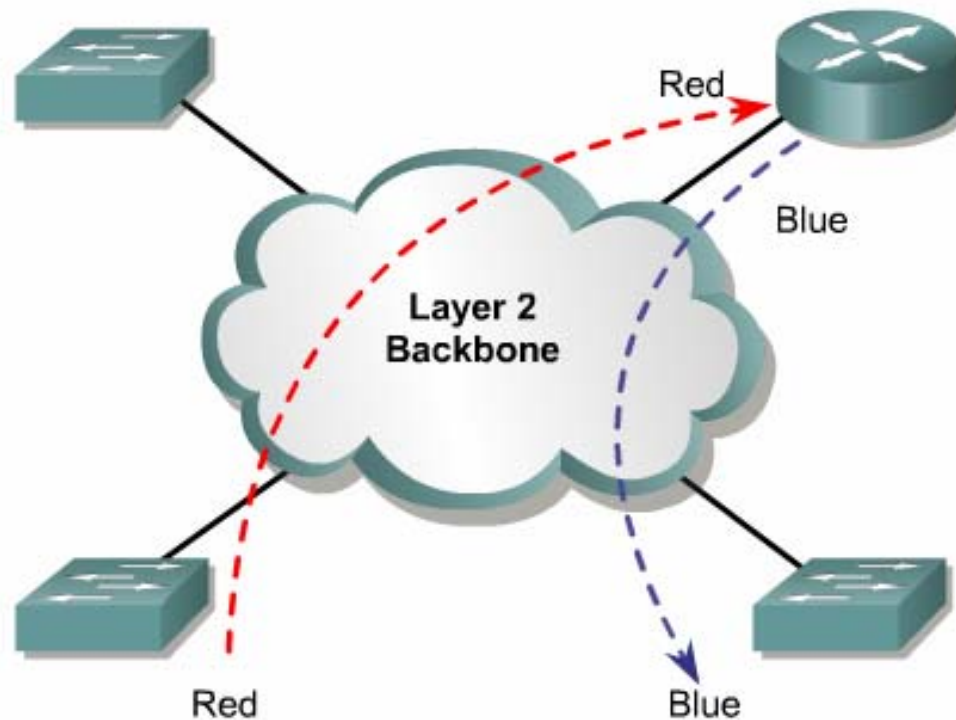
To route traffic between VLAN 1 and VLAN 200 in a non-VLAN-trunk environment, a router must be connected to a port in VLAN1 and a port in VLAN 200.

# Inter-VLAN Issues and Solutions

Two of the most common issues that arise in a multiple-VLAN environment are as follows:

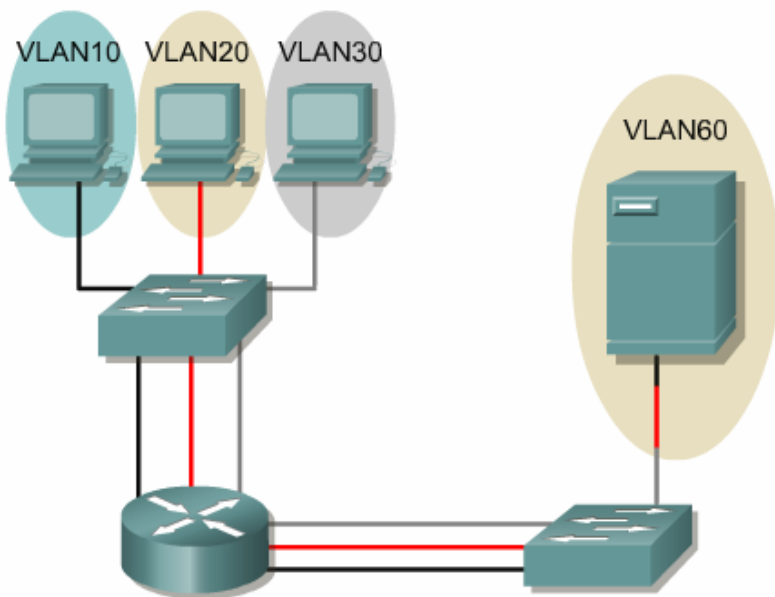
- The need for end-user devices to reach nonlocal hosts
- The need for hosts on different VLANs to communicate

# Router on a Stick

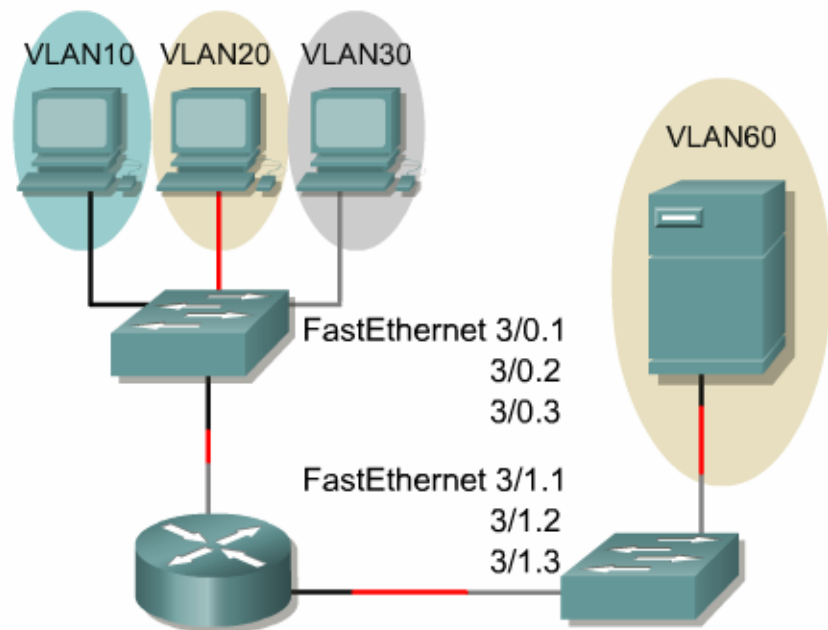


In order for traffic to move from one VLAN to another, it must go through the router.

# Physical and Logical Interfaces

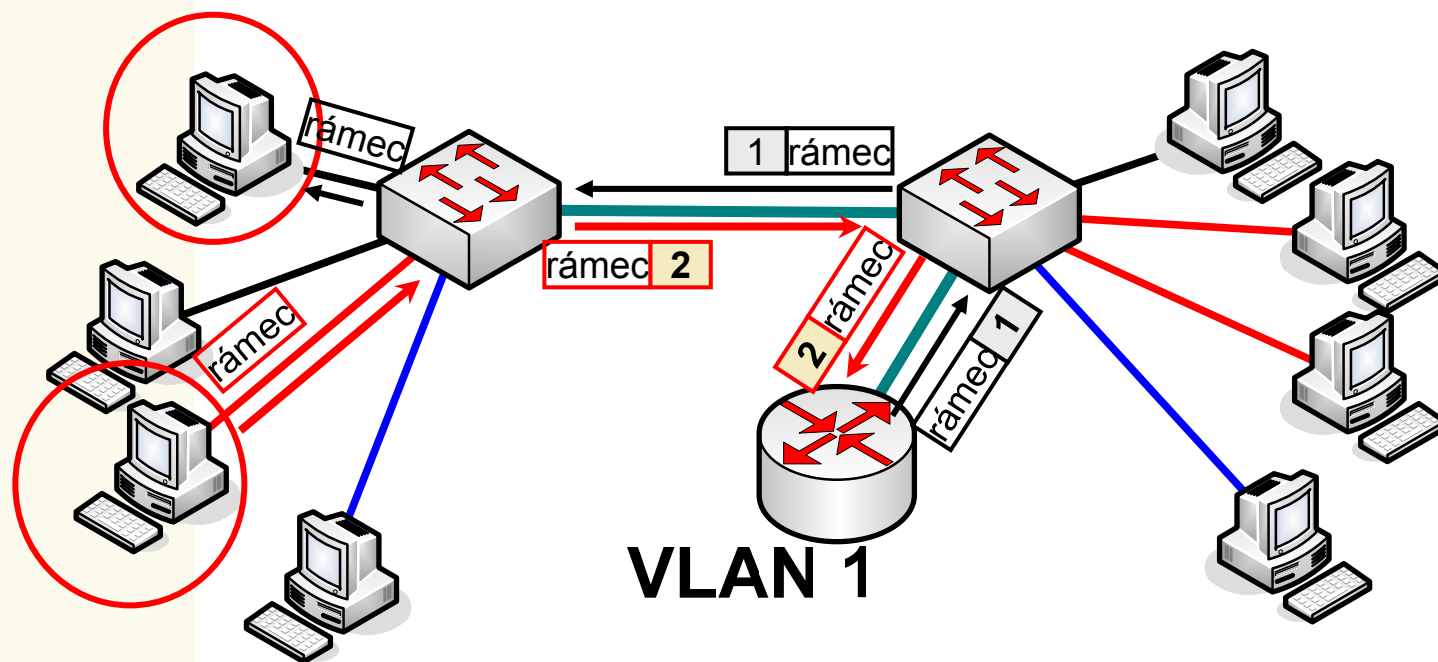


The router supports one VLAN per interface.



A single ISL link can support multiple VLANs.

# 802.1q – Inter VLAN komunikácia

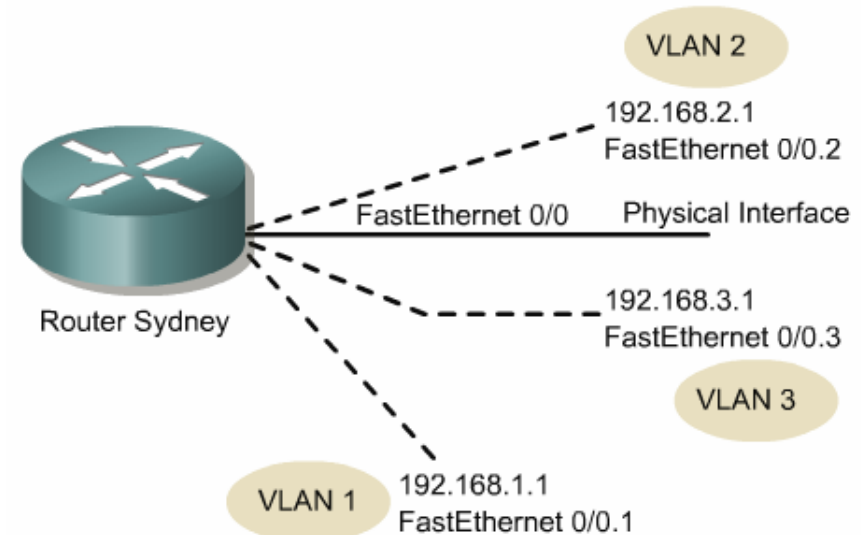


**Príklad:**  
Komunikácia medzi  
stanicami v rôznych  
VLAN (Inter VLAN)

**Trunk**

**VLAN 1**

# Dividing Physical Interfaces into Subinterfaces



```
Router_A(config)#interface fastethernet 0/0
Router_A(config-if)#no shutdown
Router_A(config-if)#interface fastethernet 0/0.1
Router_A(config-subif)#encapsulation dot1q 1
Router_A(config-subif)#ip address 192.168.1.1 255.255.255.0
Router_A(config-if)#interface fastethernet 0/0.2
Router_A(config-subif)#encapsulation dot1q 2
Router_A(config-subif)#ip address 192.168.2.1 255.255.255.0
Router_A(config-if)#interface fastethernet 0/0.3
Router_A(config-subif)#encapsulation dot1q 3
Router_A(config-subif)#ip address 192.168.2.1 255.255.255.0
```

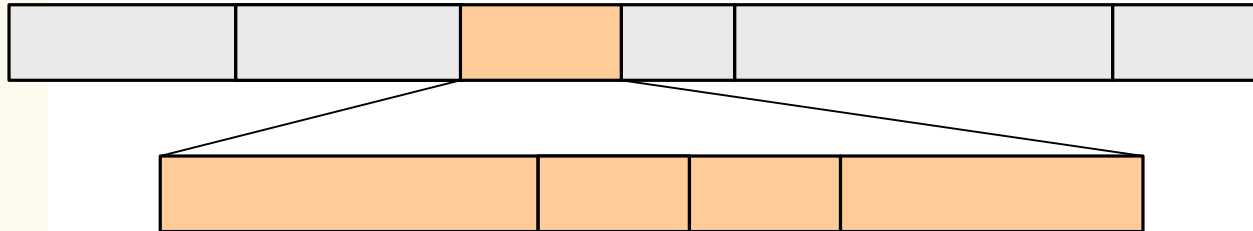
Each VLAN is its own IP network or subnet.



# QoS at L2



# 802.1q formát rámca



- **TPID (Tag Protocol Identifier):** 16 bitov

- Identifikuje rámec ako IEEE802.1q Ethernet rámec
- Nastavená hodnota 0x8100 pre tagovaný ethernet

- **Priority:** 3bity

- Indikuje prioritu rámca podľa prioritizačnej schémy 802.1p
- Použité na prioritizáciu rámcov

- **CFI (Canonical Format Indicator):** 1bit

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

- **VID (VLAN Identifier):** 12 bit

- Jednoznačne a jedinečne identifikuje VLAN do ktorej patrí rámec
- 4096 VLAN možných (0-4095)

Dest. Address      Source Addr.      VLAN  
6B                      (6B)                      (4B)

(16bit)

# IEEE 802.1p

## ■ IEEE 802.1p

- Rozšírenie IEEE 802.1q štandardu týkajúce sa **Quality of Service**

- 3 bity v 802.1q hlavičke

- Umožňuje deliť LAN prevádzku podľa stupňov priorít

  - 8 stupňov delenia priorít

## ■ Implementácia

- Mechanizmy riadenia front

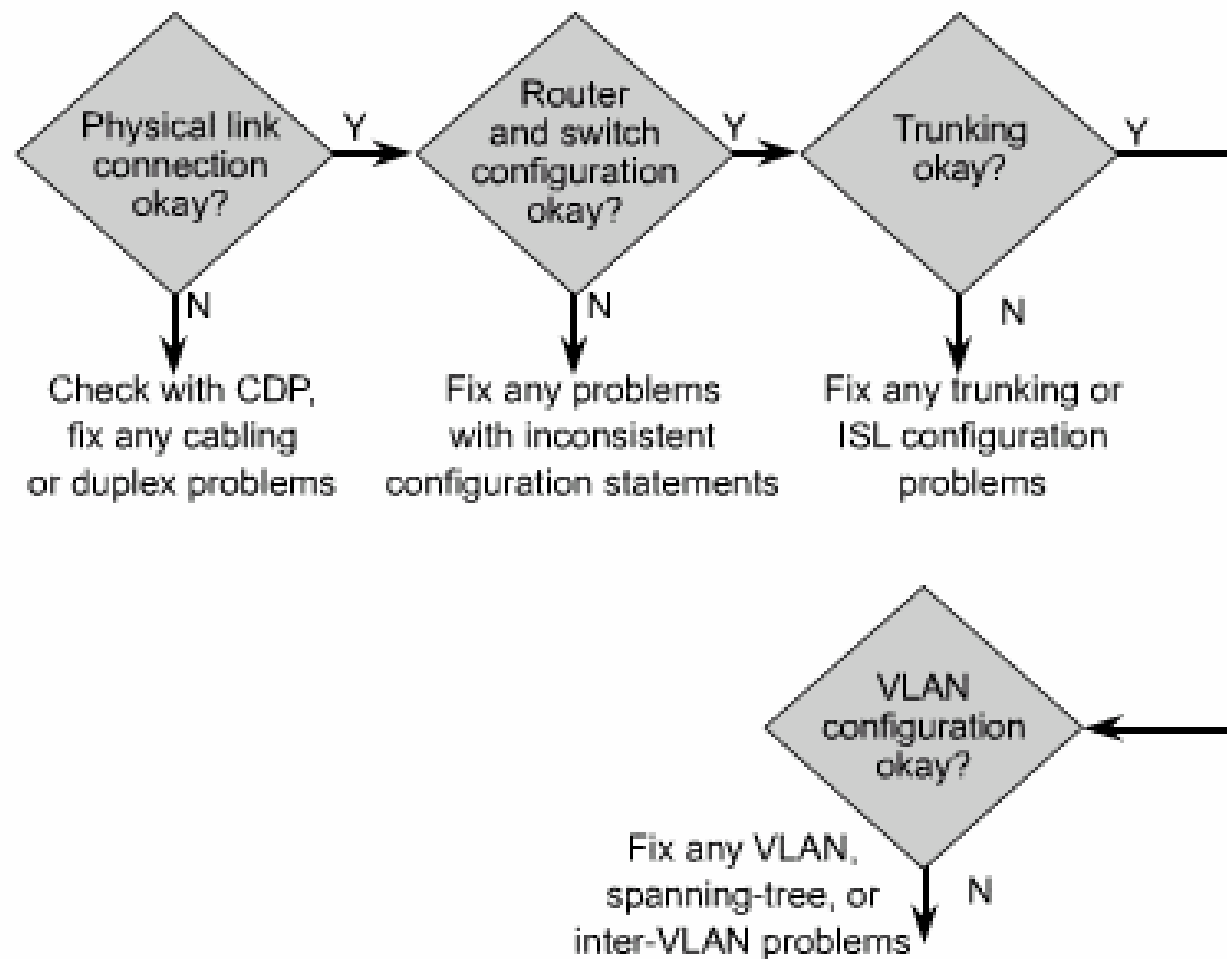
# IEEE 802.1p - Priority

- 8 úrovní priorít
  - 0 – **Default priority**, predpokladá sa Best Effort (BE)
    - Bežná LAN prevádzka
  - 1 – **Rezervované**, menej než BE
    - Hry
  - 2 – **Rezervované**
  - 3 – **Excellent effort**
    - Best Effort pre dôležitých používateľov
  - 4 – **Controlled load**, delay sensitive, bez ohraničenia
    - Dôležité aplikácie
  - 5 – **Delay sensitive**, ohraničenie 100ms
    - Video
  - 6 – **Delay sensitive**, 10ms ohraničenie
    - Hlas
  - 7 – **Network control**:
    - Dáta nevyhnutné na činnosť siete, napr. smerovanie

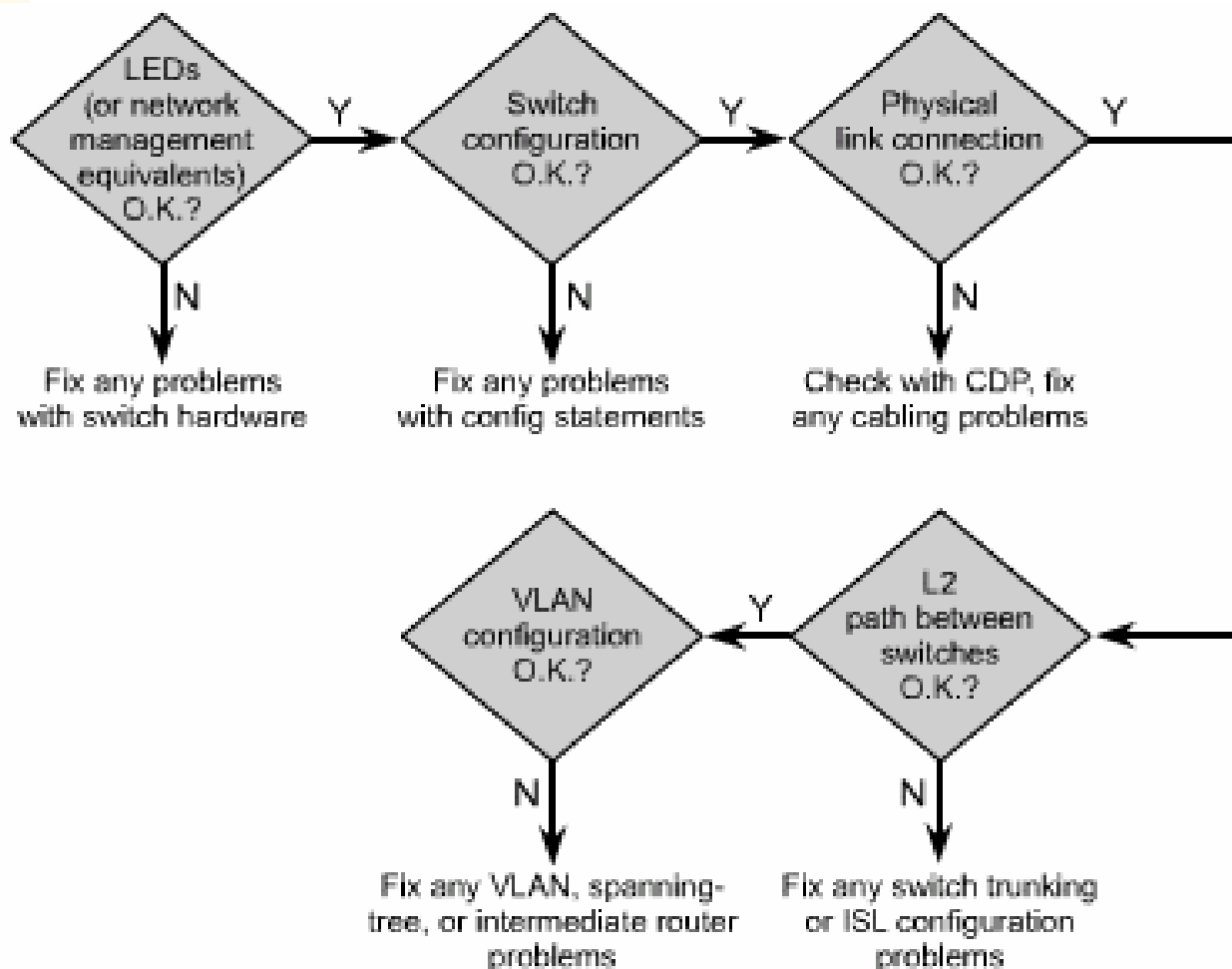
# Troubleshooting



# VLAN Problem Isolation



# Problem Isolation in Catalyst Networks



# Common Problems in Troubleshooting VLANs

Problem	Explanation and Possible Resolution
Trunk Ends in Different VLANs	Different ends of a trunk specify different VLANs. For example, vlan1, vlan2, and vlan3 are enabled on one end but not at the other end.
Protocol	Different ends of link specify different protocols. For example, this could occur on a Fast Ethernet link with Inter Switch Link (ISL) enabled on one end but not on the other end.
Single	Different ends of a single VLAN link specify different VLANs. (When the switches are not multi-VLAN capable when not running a trunking encapsulation protocol).
Name Conflict	<p>Two disconnected sets of switches that have VLANs of the same name.</p> <p>Implications: The VLANs are broken into two or more disjoint parts. Packets from one part are not traveling to the other part.</p> <p><b>Possible Resolution</b></p> <p>Rename one of the VLANs.</p>
VLAN Index Conflict	<p>Same VLAN name on different switches with different VLAN Indexes or domains.</p> <p>Traffic from switches with one number for this VLAN will not go to ports on switches with a different number for this VLAN.</p> <p><b>Possible Resolutions</b></p> <p>Rename one of the VLANs</p>
SAID Conflict	Indicates different SAID numbers on the same VLAN.



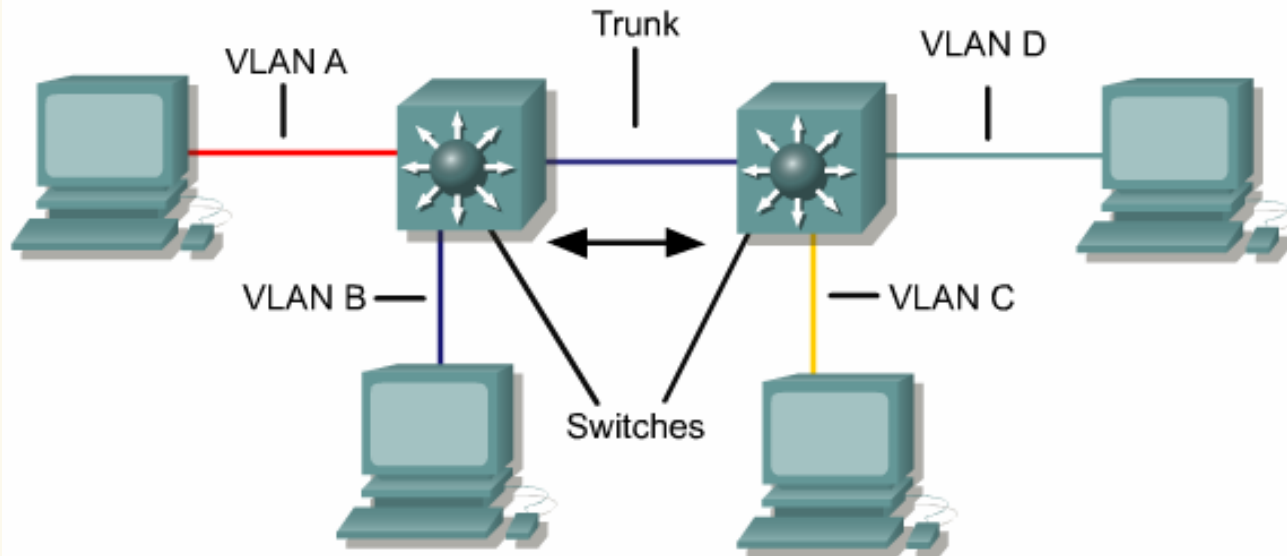
# **Virtual Trunking Protocol (VTP)**



# VTP Benefits

- VLAN configuration consistency across the network
- VLANs are trunked over mixed media. For example, an Ethernet VLAN is mapped to high-speed ATM LANE or FDDI VLAN
- Accurate tracking and monitoring of VLANs
- Dynamic reporting of added VLANs across the network
- "Plug-and-play" configuration when adding new VLANs

# VTP Concepts



**The role of VTP is to maintain VLAN configuration consistency across a common network administration domain.**

# VTP modes

- VTP switches operate in one of three modes:
  - **Server**
    - can create, modify, and delete VLAN and VLAN configuration parameters for the entire domain.
  - **Client**
    - cannot create, modify, or delete VLAN information
    - useful for switches that lack the memory to store large tables of VLAN information.
    - only role of VTP clients is to process VLAN changes and send VTP messages out all trunk ports
  - **Transparent**
    - forward VTP advertisements but ignore information contained in the message for the VTP domain
    - will not modify its database when updates are received, or send out an update that indicates a change in its VLAN status.

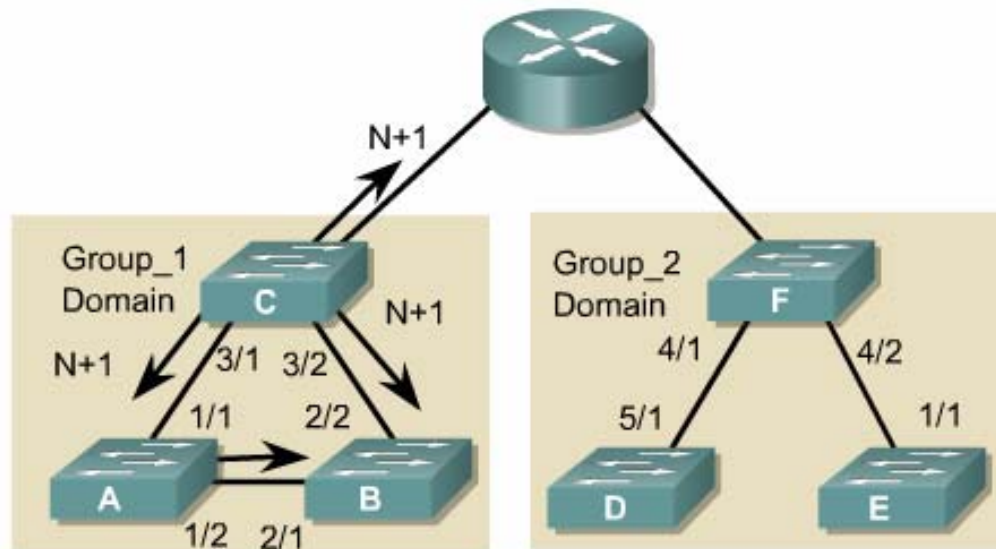
# VTP Mode Comparison

Feature	Server	Client	Transparent
Source VTP Messages	Yes	Yes	No
Listen to VTP Messages	Yes	Yes	No
Create VLANs	Yes	No	Yes*
Remember VLANs	Yes	No	Yes*

\*Locally Significant only

# VTP Operation

- advertisement starts as configuration revision number 0
- Changes = +1 revision #



Group\_1 Config Rev# N+1

1	default
2	first-vtp-vlan
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1003	trnet-default

# VTP Implementation

- There are two types of VTP advertisements:
  - Requests from clients that want information at bootup
  - Responses from servers
- There are three types of VTP messages:
  - Advertisement requests
    - clients request VLAN information and the server responds with summary and subset advertisements
  - Summary advertisements
    - Catalyst switches issue summary advertisements every five minutes
  - Subset advertisements
    - contain detailed information about VLANs such as VTP version type, domain name and related fields, and the configuration revision number.
- actions can trigger subset advertisements:
  - VLAN creation or deletion
  - VLAN suspension or activation
  - VLAN name change
  - VLAN maximum transmission unit (MTU) change

# VTP Basic Configuration Steps

- Determine the version number
- Choose the domain
- Choose the VTP mode
- Password protect the domain



# VTP Basic Configuration Steps

Switch#**vlan database**

Switch(vlan)#**vtp v2-mode**

Switch(vlan)#**vtp domain cisco**

Switch(vlan)#**vtp {client | server | transparent}**

# Verifying VTP

```
MDF_Switch#show vtp status
VTP Version                :2
Configuration Revision      :0
Maximum VLANs supported locally :64
Number of existing VLANs    :7
VTP Operation Mode         :Server
VTP domain Name             :cisco
VTP Pruning Mode            :Disabled
VTP V2 Mode                 :Disabled
VTP Traps Generation        :Disabled
MDS digest                  :0x30 0x50
Configuration last modified by 10.1.1.252 a local
updater ID 138.25.13.121 on interface found)
MDF_Switch#exit
```

# Verifying VTP

```
MDF_Switch#show vtp counters
```

```
VTP statistics:
```

Summary advertisements received	:4
Subset advertisements received	:1
Request advertisements received	:2
Summary advertisements transmitted	:7
Subset advertisements transmitted	:4
Request advertisements transmitted	:1
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
-----	-----	-----