**Základy Ethernet-u – komunikácia**

**Unicast**

Najbežnejšia forma komunikácie, jeden odosielateľ- jeden príjemca, odosielateľ vyplní rámec s unicast adresou odosielateľa a unicast adresou prijímateľa, sieť doručí práve danému prijímateľovi

**Broadcast**

Častá forma komunikácie, jeden rámec zaslaný všetkým LAN staniciam, LAN zariadenia kopírujú rámec

**Broadcast cont.**

Odosielateľ , vyplní rámec svojou unicast adresou a všetkých prijímateľov tzv. Broadcast adresa, Sieť doručí všetkým uzlom

**Multicast**

Skupinová komunikácia ,Jeden rámec zaslaný podskupine prijímateľov (nie všetkým), sieť kopíruje rámec len na porty prijímateľov ,odosielateľ vyplní rámec svojou unicast adresou a adresou pod skupiny prijímateľov na všetky svoje porty

**Konfigurácia prepínača**

1. **Začiatok konfigurácie prepínača**

- zmazanie cudzej konfigurácie

Pred začiatkom práce ak tam ostala cudzia konfigurácia môžeme vymazať nastavenia prepínača nasledujúcim spôsobom. Potrebné vymazať všetky VLAN informácie vymazaním VLAN databázy

vlan.dat z Flash pamäte. - delete vlan.dat

**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)**

**Switch#delete vlan.dat**

**Delete filename [vlan.dat]?**

**Delete flash:vlan.dat? [confirm]**

**Switch#**

Vymaž štartovací konfiguračný súbor startup-config

**erase startup-config**

Reštartuj prepínač

**reload**

**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)**

**Switch#delete vlan.dat**

**Delete filename [vlan.dat]?**

**Delete flash:vlan.dat? [confirm]**

**Switch#**

2.**Konfigurácia SSH prístupu**

**Switch(config)#username Meno password Heslo**

**! Domena musi byt zadefinovana**

**Switch(config)#ip domain-name pepe.sk**

**Switch(config)# crypto key generate rsa**

**The name for the keys will be: Switch.pepe.sk**

**Choose the size of the key modulus in the range of 360 to 2048 for your**

**General Purpose Keys. Choosing a key modulus greater than 512 may take**

**a few minutes.**

**How many bits in the modulus [512]: (768) pre version .2**

**% Generating 512 bit RSA keys, keys will be non-exportable...[OK]**

**Switch(config)#ip ssh version 2**

**\*III 1 0:1:9.780: %SSH-5-ENABLED: SSH 1 has been enabled**

**Switch(config)#line vty 0 15**

**Switch(config-line)#transport input ssh**

**Switch(config-line)#login local**

**3.** **Zabezpečenie IP prístupu na prepínač – management VLAN**

**Tristan(config)#interface vlan 99**

**Tristan(config-if)#ip address 192.168.1.2 255.255.255.0**

**Tristan(config-if)#no shutdown**

**00:53:16: %LINK-3-UPDOWN: Interface Vlan99, changed state to up**

**00:53:17: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up**

**Tristan(config-if)#exit**

**Tristan(config)#ip default-gateway 192.168.1.1**

**Tristan(config)#interface fa 0/18**

**Tristan(config-if)#switchport mode access**

**Tristan(config-if)#switchport access vlan 99 - Priradenie fyzického portu do vlan99**

**! Obnovenie telnet pristupu**

**Switch(config)#line vty 0 15**

**Switch(config-line)#transport input telnet**

**! Or**

**Switch(config-line)#transport input all**

**4.Port Security**

**-** Stáva sa, že príde nepovolaná osoba a len tak si pripojí svoj notebook alebo počítač do voľnej zásuvky

- Nechránené porty sú potenciálnym miestom pre vstup nepovolaných osôb alebo zariadení do siete Cisco prepínače ponúkajú funkciu, ktorá sa volá **port security**

**Pomocou nej je možné**

- Obmedziť počet zariadení, ktoré môžu byť pripojené k jednému rozhraniu prepínača

- Definovať zoznam MAC adries staníc, ktoré smú byť pripojené k danému rozhraniu prepínača

- Definovať, čo sa stane, ak dôjde k porušeniu niektorého z týchto bezpečnostných pravidiel

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

**Sw(config)# interface fa0/2**

**Sw(config-if)# switchport mode access alebo trunk**

**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**

**Virtuálne LAN (VLAN)**

Dôležitá vlastnosť Ethernet LAN prepínačov

**Virtual LAN (VLAN**):

- VLAN sú samostatné, nezávislé logické LAN siete, definujúce broadcast doménu, virtualizované v OS prepínača

- 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.

**Všeobecné 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 , Šetrenie finančných prostriedkov na infraštruktúru

**Implementácia statických VLAN**

**Postup pri vytváraní VLAN**

1. Vytvorenie VLAN

2. Overenie VLAN konfigurácie

3. Priradenie portu/portov prepínača do VLAN

4. Overenie konfigurácie portov prepínača

5. Overenie funkčnosti VLAN

 Overenie adresy KZ - ping

6. Implementácia zabezpečenia VLAN a prepínača - napr. nová manažment VLAN

**Vytvorenie VLAN**

**Switch#conf t**

**Enter configuration commands, one per line. End with CNTL/Z.**

**Switch(config)#vlan 2**

**Switch(config-vlan)#name Uctaren**

**Switch(config-vlan)#vlan 3**

**Switch(config-vlan)#name Marketing**

**Switch(config-vlan)#end**

**Switch#**

**Priradenie portu prepínača do VLAN**

**Switch#configure terminal**

**Enter configuration commands, one per line. End with CNTL/Z.**

**Switch(config)#int fa 0/1**

**Switch(config-if)#switchport mode access**

**Switch(config-if)#switchport access vlan 2**

**Switch(config-if)#exit**

**Switch(config)#int fa 0/2**

**Switch(config-if)#switchport mode access**

**Switch(config-if)#switchport access vlan 3**

**Switch(config-if)#end**

**Overenie VLAN konfigurácie**

**- Switch#show vlan**

**- Switch#show vlan brief**

**- Switch#show vlan id ID\_VLANY**

**- Switch#show vlan name MENO\_VLANY**

**- Switch#show vlan summary**

**Priradenie rozsahu portov prepínača do VLAN – overenie konfigurácie**

**Switch#conf t**

**Enter configuration commands, one per line. End with CNTL/Z.**

**Switch(config)#interface range fa 0/1 - 5**

**Switch(config-if)#switchport mode access**

**Switch(config-if)#switchport access vlan 2**

**Switch(config-if)#end**

**Switch#sh vlan**

**VLAN Name Status Ports**

**---- -------------------------------- --------- -------------------------**

**1 default active Fa0/6, Fa0/7, Fa0/8, Fa0/9,**

**Fa0/10, Fa0/11, Fa0/12,**

**Fa0/13, Fa0/14, Fa0/15,**

**Fa0/16, Fa0/17, Fa0/18,**

**Fa0/19, Fa0/20, Fa0/21,**

**Fa0/22, Fa0/23, Fa0/24**

**Gi0/1, Gi0/2**

**2 Uctaren active Fa0/1, Fa0/2, Fa0/3, Fa0/4**

**Fa0/5**

**Overenie VLAN konfigurácie a priradenia portov -** #show vlan, #show vlan brief, #show vlan id ID\_VLANY

**Zmazanie VLAN konfigurácie**

**! Erase vlan.dat - spominane**

**Switch#delete flash:vlan.dat**

**! Removes VLAN 5 from the VLAN database**

**Switch(config)#no vlan 5**

**! Removes port from VLAN 5 and reassigns it**

**! to the default VLAN (vlan1 ??)**

**Switch(config)#interface fastethernet 0/5**

**Switch(config-if)#no switchport access vlan 5**

**Trunk**

- Fyzická alebo logická (etherchannel) linka

- „Prenosový kanál medzi dvoma bodmi“

- Tvorí „backbone“ pre rôzne Virtuálne LAN (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

- Býva súčasťou tzv. Native VLAN

- Rámce native VLAN prechádzajú trunk-om neznačkované

- Oba konce trunk-u musia byť v tej istej Native VLAN ,

**Konfigurácia Trunk-u**

**Trunk môžeme konfigurovať**

**- Manuálne (Staticky)**

**- Dynamicky -** Dynamic Trunking Protocol (DTP).

**Statická konfigurácia trunk portu**

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#int gi 1/1

Switch(config-if)#switchport mode trunk

! Zadefinovanie novej NATIVE VLAN

Switch(config-if)#switchport trunk native vlan 99 - Switch#sh int trunk

**Dynamic Trunking Protocol (DTP) -** automatické dohodovanie vytvorenia

trunku

- Cisco proprietárny protokol

- Umožňuje automatické dohodovanie vytvárania trunkov zasielaním DTP rámcov medzi

prepínačmi

- Defaultne je spúšťaný na Cisco zariadeniach

- Ktoré ho podporujú

- Nie všetky Cisco zariadenia podporujú DTP

- Nijako neovplyvňuje možnosť statického zostavenia trunku či činnosť trunku

**Operačné módy DTP:**

**Dynamic Auto**

- Default mód na Cat2960

- Lokálny port prepínača oznamuje druhej strane, že je schopný byť trunkom, ale nevyžaduje prechod do trunk módu

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

**Dynamic Desirable**

- Default mód na Cat2950

- Lokálny port prepínača oznamuje druhej strane, že je schopný byť trunkom, a vyžaduje od druhej strany aby sa stala trunkom

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

**Nonegotiate**

- Vypnutie DTP na porte prepínača

- Žiadne DTP rámce nebudú posielané

- Switch(config-if)#switchport nonegotiate

**Trunk („On“)**

- Vytvorí trunk bez ohľadu na DTP žiadosti suseda alebo stav portu suseda

**Access („Off“)**

- Trunk nie je povolený na tomto porte

**Virtual Trunking Protocol (VTP)**

**Výhody:**

**-** Zjednodušený a konzistentný manažment VLAN naprieč prepínanou sieťou

- Uľahčené monitorovanie stavu VLAN

- Dynamické reportovanie aktuálnych zmien v konfigurácií VLAN sietí

**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

**VTP správy sa prenášajú výlučne cez trunk porty**

- Používa dot1q or ISL rámce

- Prenášané cez manažment VLAN (def. VLAN 1)

**Základná konfigurácia VTP**

1. Zisti/urči verziu VTP, ktorá sa bude používať/používa

2. Urči doménu

- Hranice

- Meno: Znakovo citilivé

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**

**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 konfiguracie -** #sh vtp status

**Upozornenie -** Vždy keď pridávaš nový prepínač do VTP domény, ubezpeč sa, že jeho revízne číslo je nižšie ako aktuálne používané !! !! !!

**Router on a Stick**

Router(config)#interface fastethernet 0/0

Router(config-if)#no shutdown

Router(config-if)#interface fastethernet 0/0.1

Router(config-subif)#encapsulation dot1q 1 native

Router(config-subif)#ip address 192.168.1.254 255.255.255.0

Router(config-if)#interface fastethernet 0/0.2

Router(config-subif)#encapsulation dot1q 2

Router(config-subif)#ip address 192.168.2.254 255.255.255.0

Router(config-if)#interface fastethernet 0/0.3

Router(config-subif)#encapsulation dot1q 3

Router(config-subif)#ip address 192.168.3.254 255.255.255.0

**Spanning Tree Protocol (STP)**

**- Štandardizovaný ako IEEE 802.1d**

**- Pracuje na L2 vrstve**

**- Zabraňuje vzniku slučiek v prepínaných sieťach**

- Detekuje redundantné linky a tie blokuje

- Do každého cieľa len jedna cesta

- Ochrana voči brodcast búrkam a problémom s konektivitou

**- Umožňuje prepínačom navzájom spolu komunikovať**

- Posielaním BPDU rámcov (každé 2 sekundy)

**- Používa Spanning Tree Algoritmus (STA)**

- Tento volí v sietí referenčný bod, ROOT prepínač (RB)

- Ostatné prepínače si určujú najlepšiu cestu k RB

- Na základe ceny (rýchlosti) linky tvoriacej cestu

- Ak sú dve cesty, lepšia je AKTÍVNA, horšia BLOKOVANÁ

STP tvorí tzv. „strom“

**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

**Konfigurácia STP**

**! Zistenie MAC adresy prepínača**

**Switch#show version**

**Base MAC address is 0002.4b21.3640 (bia**

**S2#show spanning-tree**

**VLAN0001**

**Spanning tree enabled protocol ieee**

**Root ID Priority 32769**

**Address 000A.0011.1111**

**Cost 19**

**Port 2 (FastEthernet0/2)**

**Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec**

**Bridge ID Priority 32769**

**Address 000A.0022.2222….**

**! Spustenie STP**

**Switch(config)#spanning-tree vlan vlan-id**

**! Vlan-id = Číslo VLAN, pre ktorú spúšťam STP**

**! Vypnutie STP**

**Switch(config)#no spanning-tree vlan vlan-id**

**! Nastavenie priority prepinaca per VLAN**

**Switch(config)#spanning-tree vlan vlan-id priority PRIORITY**

**! PRIORITY = priradena priorita v ramci STP per vlan s ID**

**% Allowed values are:**

**0 4096 8192 12288 16384 20480 24576 28672**

**32768 36864 40960 45056 49152 53248 57344 61440**

**! Spustenie Rapid PVST+**

**Switch(config)#spanning-tree mode rapid-pvst**

**! Nastavenie priority prepinaca per VLAN**

**Switch(config)#spanning-tree vlan vlan-id priority PRIORITY**

**! PRIORITY = priradena priorita v ramci STP per vlan s ID**

**% Allowed values are:**

**0 4096 8192 12288 16384 20480 24576 28672**

**32768 36864 40960 45056 49152 53248 57344 61440**

**! MAKRO: Nastavenie root bridge**

**Switch(config)#spanning-tree vlan vlan-id root primary**

**Overenie činnosti RSTP -** #show spanning-tree, #show spanning-tree vlan VLAN\_ID, #show spanning-tree detail

**PPP autentifikácia**

**- Password Authentication Protocol (PAP)**

**- Challenge Handshake Authentication Protocol (CHAP)**

**PAP autentifikácia**

**Pravy(config)#username Lavy password heslo**

**Pravy(config)#int serial 1/0**

**Pravy(config-if)#encapsulation ppp**

**Pravy(config-if)#ppp authentication pap**

**Lavy(config)#int s 1/0**

**Lavy(config-if)#encapsulation ppp**

**Lavy(config-if)#ppp pap sent-username Lavy password heslo**

**PAP autentifikácia – obojsmerná**

**Pravy(config)#username Lavy password heslo\_2**

**Pravy(config)#int serial 1/0**

**Pravy(config-if)#encapsulation ppp**

**Pravy(config-if)#ppp authentication pap**

**Pravy(config-if)#ppp pap sent-username Pravy password heslo\_1**

**Lavy(config)#username Pravy password heslo\_1**

**Lavy(config)#int serial 1/0**

**Lavy(config-if)#encapsulation ppp**

**Lavy(config-if)#ppp authentication pap**

**Lavy(config-if)#ppp pap sent-username Lavy password heslo\_2**

**Pozn. Heslo musí byť zhodné na oboch stranách**

**CHAP autentifikácia - jednosmerná**

**Pravy(config)#username Lavy password heslo**

**Pravy(config)#int serial 1/0**

**Pravy(config-if)#encapsulation ppp**

**Pravy(config-if)#ppp authentication chap**

**Lavy(config)#username Pravy password heslo**

**Lavy(config)#int serial 1/0**

**Lavy(config-if)#encapsulation ppp**

**Frame Relay**

**-** F.R. je najpoužívanejšia WAN technológia vo svete

- Definuje rozhranie medzi používateľom a verejnou sieťou (FR mračnom), tzv. UNI

- Definuje zapuzdrenie rámcov medzi DTE a DCE

**FR vlastnosti**

- FR je paketová technológia

- Pracuje na ISO OSI L2

- Je spojovo orientovaná

- Založená na Packet switching prepínaní

- Ponúka rýchlosti od 64 kbps do približne 45 Mbps

**FR topológie**

- Star (Hub and Spoke)

- Partial Mesh

- Full Mesh

**FR Oversubscription**

- Provider predá často väčšiu kapacitu ako fyzická rýchlosť linky. (málokedy pri data komunikácii idú všetci zákazníci naplno v rovnakom čase).

**Mapovanie adries vo FR**

**- Dynamicky - inARP (inverse ARP) -** Smerovač zistí IP adresu suseda z DLCI adresy VC

- Smerovač posiela cez všetky svoje VC inARP správy

- **LMI (Local Management Interface)**

- **Statické mapovanie -** Manuálne zadáme aké IP adresy mapovať do akého DLCI VC

**LMI (Local Management Interface)**

**-** Signálny štandard medzi DTE a Frame Relay prepínačom

**- Funkcie poskytované LMI - Keepalive mechanizmus (**Zisťuje stav spojenia medzi DCE a DTE, 10s**)**

**- Používa aj inArp na mapovanie DLCI a IP**

**Konfigurácia FR**

**- nevyhnutné úkony**

**! Nastavenie enkapsulácie**

**Switch(config)#int serial 0/0/0**

**Switch(config-if)#encapsulation frame-relay**

**Konfigurácia dynamického alebo statického mapovania**

**-** Defaultne je spustené LMI, ktoré využíva inArp

**- Vypnutie LMI – no keepalive**

**- Vypnutie inARP - no frame-relay inverse-arp**

**Základné príkazy**

**! Specifikacia rozhrania**

**Router(config)# interface serial0**

**! Zadefinovane enkapsulacie**

**Router(config-if)# encapsulation frame-relay [cisco | ietf]**

**!zadefinovanie BW pre smerovaci protokol**

**Router(config-if)# bandwidth value-in-kbps**

**!popis rozhrania**

**Router(config-if)# description text**

**!volitelne, od 12.1 autosence**

**!Zadefinovanie LMI a druhu LMI**

**Router(config-if)# frame-relay lmi-type [ansi | cisco | q933a]**

**! Staticke mapovanie IP na DLCI**

**Router(config-if)# frame-relay map <protocol> <address> <DLCI> [broadcast]**

**! Nastavenie lokalneho DLCI**

**Router(config-if)# frame-relay interface-dlci DLCI\_num**

**Konfiguráca smerovača ako FR prepínač**

**!konfiguracia FR prepinania**

**FR(config)#frame-relay switching**

**! Konfigurácia rozhraní**

**FR(config)#int s1/4**

**FR(config-if)#encapsulation frame-relay**

**FR(config-if)#frame-relay intf-type dce**

**FR(config-if)#clock rate 64000**

**FR(config-if)#no shut**

**FR(config-if)#int s 1/5**

**FR(config-if)#encapsulation frame-relay**

**FR(config-if)#frame-relay intf-type dce**

**FR(config-if)#clock rate 64000**

**FR(config-if)#no shut**

**!Konfigurácia FR prepinacej mapy**

**FR(config)#int s 1/4**

**FR(config-if)#frame-relay route 102 int s 1/5 201**

**FR(config-if)#int s 1/5**

**FR(config-if)#frame-relay route 201 interface s1/4 102**

Overenie - sh frame-relay route