**16. Segmentace sítí – VLAN**

## Principy segmentace

Segmentace se provádí hlavně z důvodu bezpečnosti, oddělením několika sítí od sebe. Využívá se při tom jednoduchého řešení pomocí VLAN tzn. na jednom kanálu dokážeme vytvořit klidně několik VLAN, kde každá může být na jiné síti. Odpadá tím nutnosti mít pro každou síť vlastní switch a router, zároveň nám to ulehčí správu sítě.

## VLAN (default, native, management)

**Default VLAN:** výchozí VLAN, 1, do této VLAN jsou přiřazeny všechny porty

**Native VLAN:** nastavuje se u trunk portu, native VLAN musíme vždy nastavit

**Mgmt VLAN:** používá se ke vzdálenému připojení a konfiguraci zařízení v síti (switch, router...)

## Konfigurace access, trunk

vlan 10

int vlan 10

int fa0/1

switchport mode access

switchport access vlan 10

switchport mode trunk

switchport allow vlan 10

## L2 a L3 switche

**L2 switch –** umí pracovat pouze s **MAC** adresami (**2. vrstva ISO/OSI**)

**L3 switch –** to stejné jako L2 switch, ale umí směrovat na základně **IP adres**, může částečně nahradit funkci routeru, lze nastavit, které porty se budou chovat jako porty routeru (routed porty), pracuje ve **3. vrstvě ISO/OSI**.

## Konfigurace DHCP

ip dhcp pool deset

network 192.168.1.0 255.255.255.0

default-router 192.168.1.254

ip dhcp exclude 192.168.1.254

## Protokoly VTP, RSTP, PVST+

**VTP (VLAN Trunking Protocol)**

L2 protokol, který slouží k **přenášení informací o VLANách** mezi více switchi, odpadá tím nutnosti manuální konfigurace VLAN na každém switchi pomocí trunku

VTP spravuje přidávání, mazání a přejmenování VLAN uvnitř VTP domény. VTP doména je tvořena síťovými zařízeními, která mají nastaveno stejné jméno domény a jsou propojeny pomocí trunku.

**Módy VTP domény:**

* **server** – defaultní mód, spravuje seznam všech VLAN, může vytvářet a mazat VLANy, přijímá a odesílá advertisements přes trunky ve VTP doméně
* **klient** – přijímá konfiguraci ze serveru, udržuje lokální kopii všech VLAN, kterou nelze měnit a nemá ji uloženou v NVRAM, přijímá a odesílá advertisements
* **transparentní** – neúčastní se VTP, pracuje samostatně, může vytvářet i mazat VLANy, ale změny jsou lokální, přijímá advertisements,



**RSTP (Rapid Spanning Tree Protocol)**

RSTP byl vymyšlen, aby **zkrátil čas konvergence STP** z původních 50s na 1 či 2s.

Základní princip je podobný klasickému STP, ale je upraven pro rychlejší konvergenci při změně topologii. Má integrován ekvivalent Cisco funkcí PortFast, UplinkFast a BackboneFast.

**Typy portů/linek:**

* **point-to-point** – připojení dalšího switche, linka musí být full duplex
* **edge** – koncový/hraniční port (PortFast), je do něj připojeno koncové zařízení PC
* **shared** – sdílená linka, například hub, linka je half duplex

**PVST+ (Per-VLAN Spanning Tree Plus)**

Pro každou VLAN běží vlastní samostatná instance STP. Výhodou je, že mohu rozdělit zátěž, že každá VLAN komunikuje jinou cestou. Používá **dot1q trunk**.

Čím více VLAN (více STP instancí), tím větší zatížení přepínače. Klasické STP, má pouze jednu STP instanci pro všechny VLANy, což znamená menší HW náročnost.   
Pro PVST+ může existovat max **128 STP instancí**.

**Konfigurace STP:**

spanning-tree mode pvst/rapid-pvst

spanning-tree vlan 10 root primary/secondary (nastavení root brdge)

## Princip a konfigurace EtherChannelu

Technologie pro **agregaci linek.** Používá se na switchi/routeru k rozložení zátěže nebo zvýšení propustnosti na linkách. Do EtherChannelu se může zapojit **2 až 8 linek** (kabelů). Používá se např. na páteřních spojích.

Je potřeba, aby byly porty stejného typu, rychlosti a byly zařazené do stejné VLANy nebo byly v trunk módu. Výhodou je zvýšení propustnosti, odolnost vůči výpadkům a nízké náklady (není nutnost nic upgradovat).

Používají se protokoly PaGP (Cisco proprietární, 16 rozhraní) a LACP (veřejně dostupný, 16 rozhraní, pouze 8 active).

int range fa0/10-11

channel-group 1 mode active/on/desirable

exit

int po1

switchport mode trunk enc dot1q

switchport mode trunk

switchport allowed vlan 10

## ACL (Access Control List)

Seznam pravidel, který jedná o řízení nebo identifikaci přístupu k nějakému objektu. Nejčastější použití je pro řízení (omezování) síťového provozu, tedy pro filtrování paketů.

Hlavní dělení je tedy podle typu adres, které používáme v pravidlech. Nejčastější jsou   
**IP, MAC a IPv6 ACL**, která mohou být port nebo Router. V konfiguraci se používají prefixy místo Wildcard masky.

**ACL slouží**

* jako základní síťová bezpečnost k blokování nebo povolení (routovaného) provozu
* ke kontrole šířky pásma
* vynucení síťových politik
* identifikaci nebo klasifikaci provozu (pro QoS, NAT apod.)

## Příkazy pro nastavení Cisco switche

copy running-config startup-config (uložit aktuální konfiguraci)

show mac-address-table (ukáže MAC tabulku)

show running-config (ukáže aktuální konfiguraci)

switchport port-security (nastavení port security)

clock set hh:mm:ss day:month:year (nastavení času)

banner motd …… (banner se ukáže při zapnutí sw)

enable password …… (nastavení hesla)

enable secret …… (zašifrované heslo)

**VLAN**

show vlan brief (ukáže správu VLAN)

vlan 10 (vytvoření VLAN)

int vlan 10 (vstup na rozhraní VLAN)

no vlan 10 (zruší VLAN)

switchport mode trunk/access

no switchport mode trunk/access (zruší switchport mode…)