05 - VLAN, podniková síť

Koncept VLAN

- logické rozdělení sítě na části, bez změny fyzické struktury
- obvykle napojena na switch
  - rozdělení portů switche na několik částí
- mezi VLAN sítěmi lze routovat jako s ostatními sítěmi
- díky VLAN se snižuje počet broadcastů v síti
- díky VLAN se seskupují uživatelé dle skupin/služeb, které jim přísluší
- dokáže izolovat účastníky sítě nezávisle na ostatních prvkách sítě

Výhody

- menší dosah broadcastu
- jednodušší správa sítě
- lepší zabezpečení
- nižší množství HW

Komunikace v rámci VLAN

- při komunikace v rámci jednoho switche / při komunikaci mezi několika switchi

access VLAN

- defaultní mód portu switche
- přijímá pouze packety bez tagovaného rámce (tagované zahazuje)
- může být členem pouze jedné VLAN

```
SWITCH(config-if)# switchport access vlan 100
```

trunk VLAN

- umožňuje skrz něj propojit jiný switch, se zachováním VLAN skupin
- další využití - propojení serverů, které potřebují komunikovat do více VLAN
- použitím **access portu** by si packet nezachoval VLAN a cestoval by dále po VLAN z cílového switche

```
SWITCH(config-if)# switchport trunk allowed vlan 100,200
```

IEEE802.1Q - dot1Q

- uchová informaci o VLAN při cestování packetu celou sítí
- pokud je aktivní encapsulace dot1q, rámec je rozšířen o 4 bity informací
  - značka protokolu 802.1Q
  - priorita
  - příznak, zda je MAC adresa kanonická
  - číslo VLAN

```
SWITCH(config-if)# switchport trunk encapsulation dot1q
```

native VLAN

- "záložní nastaveni"
- používá se v případě, že stanice nepodporuje trunk, ovšem switch má nastaven trunk
- musí být nastavena shodně na obou stranách komunikace
- packety bez tagu, co přijdou do trunk portu, jsou přesměrovány na native VLAN

```
SWITCH(config-if)# switchport trunk native vlan 1
```

management VLAN

- defaultně VLAN 1, doporučeno změnit
- používání pro správu switche
- komunikace přes Telnet, SSH, HTTP…
- nutné nastavit IP adresu a defaultní bránu

voice VLAN

- IP hlasový provoz z IP telefonu - na access portu
- telefon obsahuje malý switch, do něj je připojen PC

VTP

- VLAN Trunking Protocol
- protokol, který přenáší informace o VLAN mezi switchi
- spravuje přidávání, mazání a přejmenování VLAN
- každý switch má jeden z módů:
  - **server** - spravuje seznam VLAN, může je mazat a vytvářet
  - **klient** - přijímá konfiguraci ze serveru, udržuje lokální kopii seznamu
  - **transparentní** - neúčastní se VTP a pracuje samostatně

DTP

- Dynamic Trunk Protocol
- protokol, který automaticky zjistí, zda je daný port trunk
  - poté vyjedná přepnutí druhé strany do trunk režimu
- doporučeno nepoužívat kvůli bezpečnosti

Port security

- zabezpečuje přístup do sítě, jednoduchá
- kontroluje, zda packety přichází z povolené MAC adresy
- port musí být access/trunk (statický mód)

Protected port

- na tento port se nezasílá broadcast/multicast/unicast
- zasílá se pouze komunikace na L3 vrstvě - routování

STP

- Spanning Tree Protocol
- odstraňuje závady v síti
- smyčka = broadcast packet dorazí do cíle a znovu vyšle broadcast
- když vznikne smyčka, STP ji odstraní pomocí blokace portu
- nalézá nejkratší cestu pro packet

EtherChannel

- propojení síťových zařízení více rozhraními
- zvyšuje propustnost
- nabízí alternativní trasu v případě výpadku jedné z linek
- STP neblokuje ostatní cesty, protože svazek EtherChannel je jeden virtuální port