13. VLAN a VTP, nativní a tagované pakety, směrování mezi VLANy.

POČÍTAČOVÉ SÍTĚ A PROGRAMOVÁNÍ

VLAN (Virtual LAN)

- Slouží k logickému rozdělení sítě nezávisle na fyzickém uspořádání.
- Toto dělení šetří čas (manuální přepojení sítě) i peníze (samostatné switche pro každou síť).
  Fyzické umístění počítačů není omezené prostorem.
  - Bez VLAN bychom umístili počítače, například ze stejného oddělení, blízko sebe.
- Každá VLANa je samostatná podsíť.
  - Zařízení z různých VLAN spolu nemohou komunikovat, i když jsou připojeny ke stejnému switchi.
  - Zmenšujeme tím broadcast doménu.
- Vždy existuje alespoň jedna VLANa → defaultní (označena 1).
- Zvýšená bezpečnost oddělením komunikace.

Přiřazení do VLAN

1. **Podle portu**
   - Port na switchi je staticky přiřazen k VLANě
   - Veškerá komunikace přicházející z tohoto portu spadá do dané VLANy.
   - Nejpoužívanější metoda.
   - **Výhody:**
     - Jednoduchá správa
     - Rychlé nasazení
     - Přehledné
2. **Podle MAC adresy**
   - Rámec se zařadí do VLANy podle zdrojové MAC adresy.
   - Potřebujeme tabulku MAC adres.
   - Jedná se o dynamický způsob.
   - **Realizace:**
     - Port se přiřadí do VLANy podle prvního přijatého rámce (do vypnutí portu).
     - Každý rámec se řadí do VLANy samostatně (náročné na výkon).
3. **Podle protokolu**
   - Například oddělení IP od AppleTalk či dělení dle IP adresy.
   - V praxi se moc nepoužívá.
   - Zařízení musí mít pevně definovanou IP adresu a switch musí pracovat i na 3. vrstvě.
4. **Podle autentizace**
   - Uživatel nebo zařízení se ověří pomocí protokolu IEEE 802.1X a podle informací se automaticky zařadí do VLAN.
   - Bezpečnostní metoda
   - Velmi univerzální

Druhy portů

Access port

- Má přiřazenou jednu VLANu.
- Je k němu připojeno zařízení a rámcům říkáme nativní.
- Switch nepřepíná rámce mezi dvěma access porty z různých VLAN.

Trunk Port

- „Teče“ přes něj komunikace z několika VLAN.
- Využívá protokol IEEE 802.1q, kterým značkuje rámce → tagovaný rámec.
- K označení dojde až v době potřeby (rámec se má poslat přes trunk port).

VTP (VLAN Trunking Protocol)

Proprietární síťový protokol firmy Cisco.

Zajišťuje přenášení čísel a názvů VLAN mezi přepínači (usnadňuje nám jejich správu).

Dostupný na většině přepínačů Cisco.

Princip

Druhy přepínačů

- Server
  - Má informace o VLANách a distribuuje je při změně klientům.
- Client
  - Přijímá změny ze serveru.
- Transparent
  - Změny si neukládají, ale jen je posílají dál.
- Přepínače jsou přiřazeny do domény (označené textovým řetězcem).
- Synchronizace je zajištěna číslem revize (32bitové číslo), které vytváří server a s každou revizí ho inkrementuje o jedničku.
- Komunikace probíhá přes multicast MAC adresu a má tři typy paketů:
  - **Summary advertisement**
    - Vysílán každých 5 minut a obsahuje jméno domény, číslo revize a čas poslední změny.
    - Klient po obdržení zkontroluje doménu a jestli je číslo revize vyšší než poslední uložené (pokud ano, tak vyšle Advertisement request).
  - **Subset advertisement**
    - Vysílán serverem v případě změny nastavení.
    - Obsahuje název domény, číslo revize a informace o jedné nebo více VLAN – číslo, stav (aktivní/neaktivní), jméno a velikost MTU (Maximum transmission unit).
  - **Advertisement request**
    - Posílá klient v případě resetu, změny domény, či jako odpověď na Summary advertisement, který měl vyšší číslo revize.

VTP Pruning

- Zabraňuje zbytečnému odesílání všesměrových (broadcast) packetů z určité VLAN na přepínače, které nemají aktivní žádné zařízení na této VLAN.
- Nastaví se na serveru a klienti ho převezmou automaticky.

Nativní a tagované pakety

Nativní pakety

- Jedná se o tu (jedinou) konkrétní VLAN, jejíž rámce na trunk linkách nejsou „taggovány“.

Tagované pakety

- Rámce na trunk linkách jsou označeny („taggovány“).

Směrování mezi VLANy

- Defaultně switch pracuje na vrstvě L2.
- Chceme-li používat L3 IP routing, musíme ho zapnout.
- Směrování probíhá na jednom zařízení, a proto není potřeba směrovací protokol (přímo připojená rozhraní jsou automaticky zapsána do směrovací tabulky).

Routované a neroutované VLANy

- Routování VLAN – umožňujeme jí komunikaci s ostatními VLANy
- Neroutovaná VLAN – izolovaná od ostatních VLAN
- Omezeně routovaná – může komunikovat pouze s některými VLANy (zajištěno pomocí ACL)