5 VLAN, návrh podnikové sítě

Wednesday, 19 January 2022 09:08

Koncepce VLAN, výhody nasazení VLAN, access VLAN, trunk VLAN, IEEE802.1Q, native VLAN, management VLAN, voice VLAN.
Tři způsoby pro nasazení, porovnání metod z hlediska efektivity.
Nastavení směrovače pro propojení VLAN (legacy, Router-on-a-Stick)
Nastavení přepínače L3 pro Inter-VLAN, možnost směrování přepínače L3
Návrh podnikové sítě s např. 6 sekcemi – VLAN, podsíťování, propojování VLAN

- VLAN (virtuální LAN)
  - logicky nezávislá síť v rámci jednoho a více zařízení
  - obvykle realizována na switchích
  - snižuje se díky nim počet broadcastů v síti
  - pracuje na 2. vrstvě OSI/ISO
    - podsítě pracují na 3. vrstvě
  - rozdělení podle:
    i. portu
      - statická VLAN
      - port switche ručně přiřazen

    ii. MAC adresy
      - dynamická VLAN
      - VLAN se přiřadí podle MAC adresy v MAC tabulce

    iii. protokolu
      - dynamická VLAN
      - podle protokolu přenášeného paketu

    iv. autentizace
      - dynamická VLAN
      - po 802.1X autentizaci se uživatel přiřadí do VLAN

  - typy:
    - access
      - defaultní mód
      - přijímá pouze netagované packety
    - IEEE 802.1Q
      - uchovává informaci o VLAN při cestování paketu celou sítí
      - přidává informaci o VLAN jen pokud komunikace probíhá mimo jeden switch
      - odchozí komunikace se taguje na trunk portu
    - native
      - spojená s protokolem 802.1Q
      - nastavuje se na trunk portu
      - chodí sem netagované packety, které přijdou na trunk port
    - management
      - pro správu switche a ze vzdálených míst pomocí Telnetu nebo SSH
      - obvykle VLAN1, ale z bezpečnostních důvodů se mění
      - nutné nastavit IP adresu a default gateway
    - voice
      - pro VoIP
      - nastavuje se většinou nejvyšší priorita, aby byla nízká latence
  - protokoly:
    i. VTP (*VLAN Trunking Protocol*)
      - proprietární Cisco protokol
      - přenášení informace o VLAN mezi switchi
      - správa přidávání, mazání a přejmenovávání VLAN
      - switch módy:
        - server
          - defaultní
          - spravuje seznam VLAN
          - může vytvářet a mazat VLAN
        - klient
          - přijímá konfiguraci ze serveru
          - lokální kopie VLAN (není uložena v NVRAM)
        - transparentní
          - neúčastní se VTP
          - pracuje samostatně (změny VLAN lokální)
          - lze vytvářet *extended* a *private* VLAN

    ii. DTP (*Dynamic Trunk Protocol*)
      - slouží pro automatické vyjednávání, jestli je port trunk
      - nedoporučuje se používat
        - port by mohl vyjednat, že je trunk
  - Inter-VLAN
    - komunikace mezi VLAN
    - musí se mezi nimi routovat
    - zapojení
      1) legacy
         - každá VLAN má jeden fyzický port
      2) router on a stick
         - trunk mezi switchem a routerem
         - tagování pomocí 802.1Q
         - každá VLAN má subinterface (doporučeno zachovat číslo subinterface a VLAN stejné)
      3) L3 switch
         - trunk mezi switchem a L3 switchem
         - rychlé směrování díky HW směrování
         - problémy s připojením do internetu, protože L3 nemá NAT