13 - VLAN a VTP, nativní a tagované rámce, směrování mezi VLANy

VLAN

- virtuální LAN
- umožňuje užití jednoho switche pro více sítí
- lze dělit síť podle funkce, uživatelů, atd.
- výhody:
    - bezpečnost – skupiny jsou odděleny, lze oddělit skupiny s citlivými daty od zbytku sítě
    - snížení nákladů – není potřeba užívat více switchů, sníží se tak pořizovací i provozní náklady
    - vyšší výkon – rozdělení sítě do několika skupin sníží zbytečný provoz (třeba z broadcastů) a zvýší výkon
- Typy:
    - Data VLAN
        - určena pro přenos dat uživatelů
        - neobsahuje hlasové služby a data pro řízení a správu sítě
    - Default VLAN
        - výchozí VLAN switche, po prvním zapnutí (nebo když není vytvořen/upraven startup-config)
        - všechny porty jsou v jedné síti, a tudíž v jedné broadcast doméně
    - Management VLAN
        - má IP adresu a může řídit switch, IP lze použít pro připojení přes http, SSH, Telnet
    - Voice VLAN
        - pro VoIP (Voice over IP)
- Konfigurace:
    - Statická VLAN
        - porty se přiřadí ručně
        - nejčastější
    - Dynamická VLAN
        - porty přiřazuje VLAN server dynamicky podle MAC adresy
        - když se stanice přestěhuje na jiný port nebo switch, server přiřadí port správné VLAN
    - Hlasová VLAN
        - konfigurace portu pro podporu IP telefonu
        - je nutno vytvořit jedu VLAN pro hlas a jednu pro data
        - hlasový přenos musí mít přednost
- broadcast domána je bez VLAN jednotná pro všechna připojená zařízení, s VLAN se broadcast šíří jen v rámci dané VLAN
- VLAN trunking
    - umožňuje použít jeden spoj pro více VLAN
    - bez trunk spoje by bylo nutné použít spoj pro každou VLAN
    - PC vyšle rámec, ten je označen VLAN ID (určuje které VLAN rámec náleží), poslední switch na cestě VLAN ID odstraní
    - DTP (Dynamic Trunking Protokol) – Cisco
        - switchport mode trunk

                - switch periodicky vysílá své DTP informace
                - zůstává v nakofigurovaném trunking módu
            - switchport mode dynamic auto
                - switch periodicky vysílá své DTP informace
                - přejde do trunking módu jen pokud je na druhé straně rovněž trunk, jinak zůstává v módu access
- Nativní VLAN
    - přiřazena 802.1Q trunk portu, který podporuje provoz přicházející z mnoha VLAN (tagované rámce) a provoz nepocházející z VLAN (netagované rámce), který přiřadí do nativní VLAN

VTP

- VLAN Trunking Protocol
- umožňuje správu všech VLAN ze serveru VTP pomocí:
    - VTP Summary Advertisment Packet
    - VTP Subset Advertisements
    - VTP Advertisement Requests
        - vysílá se:
            - po restartu
            - při změně doménového jména
            - přijímač přijme VTP Summary s vyšším číslem revize, než jeho vlastní
- VTP doména
    - skládá se z několika switchů, kterým bylo přiděleno stejné jméno domény
    - usnadnění správy – chyby se šíří jen po hranice domény
    - nové VLAN na VTP lze vytvářet až po přidělení jména domény
    - konfigurace jsou automaticky číslovány – switche podle toho ví, která je aktuální
- Oznámení
    - souhrná
        - vysílaná pravidelně každých 5 minut, nebo při změně konfigurace
        - číslo současné verze konfigurace
    - dílčí
        - vysílaná, když se vytvoří, smaže, přejmenuje, zakáže nebo aktivuje VLAN, nebo když se změní velikost MTU pro VLAN
    - požadavky
        - posílají se, když se změní jméno domény, přijde číslo vyšší verze, nedorazilo dílčí oznámení, nebo byl switch resetován
- Konfigurace VTP
    - Server
        - na všech switchích používaných pro VTP smaže konfiguraci
        - v každé síti by měl být navíc i záložní server
        - na serveru nakonfigurujeme doménu, ostatní switche ji obdrží po síti
        - při použití hesla pro VTP musí použít všechny switche stejné, jinak nebudou spolupracovat
        - na všech switchích musí být stejná verze VTP
        - VLAN se konfigurují až po spuštění VTP, jinak se smažou
        - musí být nakonfigurované trunk porty, VTP informace se mimo trunk nešíří
    - Klient
        - Default konfigurace viz server

        - Nakonfigurujeme client mode (není default)
        - Nakonfigurujeme trunky
        - Připojíme k VTP serveru
        - Zkontrolujeme stav a funkčnost VTP
        - Nakonfigurujeme přístupové porty
- Verze VTP
    - 1 – zastaralá
    - 2 – výchozí, podporuje Token Ring VLAN
    - 3 - nekomunikuje přímo s procesem spravujícím VLANy (na rozdíl od předchozích), zpětně kompatibilní s v2

Inter VLNA routing

- umožňuje komunikaci mezi zařízeními na různých VLAN
- Tradiční směrování mezi VLAN:
    - Směrovače vyžadují více fyzických rozhraní.
    - Každé fyzické rozhraní je připojeno k jedinečné VLAN.
    - Každé rozhraní má IP adresu pro příslušnou VLAN.
    - Zařízení používají směrovač jako bránu pro komunikaci mezi VLANami.
- Proces směrování:
    - Zdrojové zařízení porovná adresy podle masky podsítě.
    - Pokud je cílová adresa mimo místní síť, zařízení použije výchozí bránu.
    - Směrovač na lokální podsíti slouží jako výchozí brána.
    - ARP a směrování:
    - Zdrojové zařízení pošle ARP požadavek pro MAC adresu směrovače.
    - Směrovač odpoví a zařízení použije tuto MAC adresu v Ethernet rámci.
    - Rámec je přeposlán na správný port přepínače.
- Inter-VLAN komunikace:
    - Směrovač odpoví na ARP požadavek svou MAC adresou (default gateway).
    - Když směrovač dostane paket, rozešle ARP požadavek do cílové VLAN pro zjištění MAC adresy cílového zařízení.
    - Směrovač poté pošle rámec s paketem na přepínač.
    - Omezení tradičního inter-VLAN směrování:
    - Omezený počet fyzických rozhraní na směrovači.
    - Nutnost použití VLAN trunkingu pro více VLAN na jednom rozhraní.
- Virtuální podrozhraní a trunking:
    - Podrozhraní jsou virtuální rozhraní přiřazená fyzickému rozhraní.
    - Každé podrozhraní má vlastní IP adresu, masku podsítě a VLAN.
    - Inter-VLAN směrování se provádí pomocí modelu "router-on-a-stick".
- Router-on-a-stick:
    - Fyzické rozhraní směrovače je připojeno k trunk lince přepínače.
    - Podrozhraní jsou vytvořena pro každou VLAN.
    - Každé podrozhraní má IP adresu specifickou pro danou podsíť.
    - Směrování probíhá přes trunk linku zpět k přepínači.