6. Segmentace a mikrosegmentace sítí, kolizní a broadcast doména, přepínače, architektura sítí LAN, redundance v síťovém provozu, STP, Etherchannell, VRRP

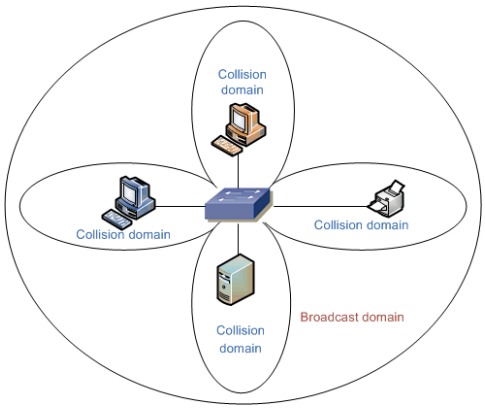
Segmentace a mikrosegmentace sítí

- Obvyklou technikou implementace zabezpečení sítě je segmentace sítě organizace do samostatných zón, které lze samostatně řídit, sledovat a chránit.
- Mikrosegmentace je výsledkem postupného rozdělování segmentů na menší a menší až na jednouzlové. Přenos v takovém segmentu je už omezen pouze propustností a s nikým jiným médium nesdílí.

Kolizní a broadcast doména

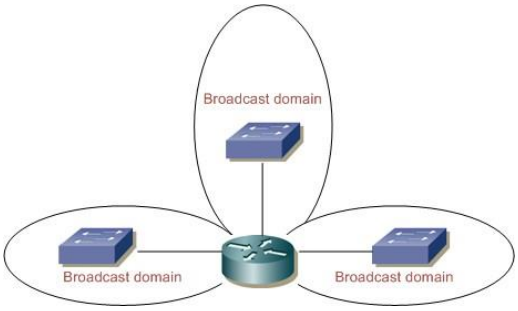
Kolizní doména

- Jedná se o segment sítě, ve kterém se šíří kolize.
- Tyto segmenty lze oddělit zařízením pracující na 2. linkové vrstvě ISO/OSI modelu (switchem).
- Pokud začne zároveň vysílat více rozhraní, dojde ke kolizi a znehodnocení signálu, zařízení musí vysílání opakovat, k tomu slouží protokoly CSMA (Carrier Sense Multiple Access).



Broadcastová doména

- Část sítě, ve které může na linkové vrstvě každý uzel komunikovat s každým pomocí broadcastu.
- Broadcastovou doménu odděluje router nebo brána (gateway) = zařízení na síťové vrstvě.
- VLANy dělí také broadcastové domény.
- Kolizní domény jsou menší a jsou součástí broadcastových domén.



Přepínače

- Síťový přepínač je aktivní prvek v počítačové síti, který propojuje jednotlivé prvky do hvězdicové topologie.
- Přepínače (Switche) přepínají rámce na základě MAC adresy v hlavičce rámce.
- Rámec přepíná na port podle MAC adress table, pokud MAC adresu nemá v tabulce, vyšle rámec broadcastem.
- MAC adress table si tvoří pomocí ARP protokolu.
- Pracuje na 2. vrstvě ISO/OSI modelu.
- Podporuje VLAN.

Segmentuje sítě:

- Kolizní domény
- Všeobecné vysílání
- Vyhrazené spojení

Princip

- Po přijetí rámce si přečte MAC adresu, a do paměti si uloží port a k ní příslušnou MAC adresu.
- Cíl hledá v uložené tabulce MAC adres.
    - Pokud najde pošle rámec na daný port.
    - Pokud nenajde, odešle rámec na všechny porty, kromě od kterého rámec přijal.

Metody přepínání rámců

1. **Store and forward (Ulož a pošli)**
    - Rámce se celé načtou a uloží do vyrovnávací paměti, zjistí se výstupní port podle MAC adresy a MAC adress table.
    - Před odesláním ověřuje integritu dat, chybné rámce zahazuje.
    - Nižší výkon vnitřního přepínánívhodné pro sítě s vysokou chybovostí.
2. **Cut-trough switching/On the fly (Průběžné zpracování)**

    Režim průběžného zpracování
    - Průběžně přepíná na výstupní port, aniž by skončil příjem rámce.
    - Přepnutí rámce ihned po zjištění cílové MAC adresy.

    Režim nestandartního zpracování
    - Načítání prvních 64 bitů pro zjištění kolizních rámců.
    - Neprovádí fragmentaci rámců.
    - Neověřuje kontrolní součet.
3. **Rychlé hardwarové přepínání**
    - Použití v prostředích stejných lokálních sítí.
    - Možná odlišná rychlost na portech.
4. **Symetrické a asymetrické přepínání**

    Asymetrické přepínání
    - Přepínač má porty s různými rychlostmi.

    Symetrické přepínání
    - Všechny porty mají stejnou rychlost (šířku pásma).

Vyrovnávací paměť

- Pokud je nutné rámec před odesláním zkontrolovat je potřeba ho někam uložit -> k tomu slouží vyrovnávací paměť (cache nebo buffer).

Port-based Memory Buffering (Vyrovnávací paměť portu)

- Rámce jsou ukládány v pořadí ve frontách, jak přicházejí z příchozích portů.
- Na výchozí port rámce odeslány pouze tedy, když všechny předchozí rámce byly odeslány (zpoždění).

Shared Memory Buffering

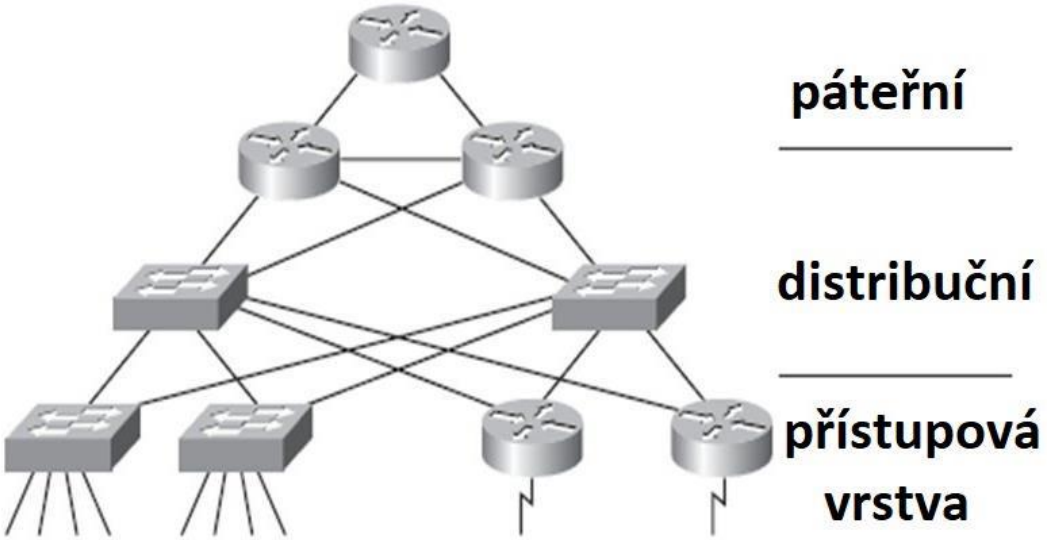
- Všechny rámce jsou uchovávány ve společné vyrovnávací paměti, která je sdílena všemi porty současně.

ARP (Adress Resolution Protocol)

- Získává linkovou fyzickou adresu síťového rozhraní protistrany na stejné podsíti.
- Nalezne vazbu mezi IP a MAC adresou a zachová mapovaní v paměti cache.

Architektura sítí LAN

- Hierarchický síťový model



Páteřní vrstva

- Vysokorychlostní páteř pro přeposílání dat mezi sítěmi.

Distribuční vrstva

- Sdružuje data přijatá z přepínačů na přístupové vrstvě.
- Data předává páteřní vrstvě, kde jsou směrována do cíle.
- Vymezuje broadcastové domény, zajišťuje směrování mezi VLANy.

Přístupová vrstva

- Propojení vyšších vrstev sítě s koncovými zařízeními.
- Může obsahovat směrovače, přepínače, bridge nebo AP (přístupové body bezdrátové sítě).

Typy vysílání

- Unicast – jeden odesílatel, jeden příjemce
- Multicast – jeden odesílatel, příjemcem je skupina zařízení
- Broadcast – jeden odesílatel, příjemcem jsou všechny ostatní adresy

MAC adresa

- 48bitové číslo, které je vyjádřené 12 hexadecimálními číslici (0-F).
- Prvních 24 bitů je dáno od výrobce a zbylých 24 bitů slouží k jednoznačné identifikaci.
- Fyzická adresa zaznamenána v ROM paměti NIC (Network Interface Card).

Redundance v síťovém provozu

- Redundance je klíčovým prvkem veškerých průmyslových sítí a aplikací.
- Cílem síťové redundance, která funguje jako rychle reagující zálohovací systém, je zmírnit riziko neplánovaných výpadků a zajistit kontinuitu provozu pomocí okamžité reakce a omezení vlivů místa selhání kdekoli po kritické datové cestě.
- Pokud by přepínač selhal nebo se kabel přerušil, redundantní systém zajišťuje kontinuitu a zamezuje přerušení kriticky významné komunikace a datového toku.

STP

- Odstraňuje smyčky (redundantní spoje) v sítích, které způsobují množení broadcastů.
- Redundantní spoj v případě výpadku aktivního spoje automaticky aktivuje.
- Rámce nemají TTL, proto rámce mohou ve smyčkách obíhat donekonečna.
- Obsahuje algoritmy, pomocí kterých tvoří bezsmyčkovou topologii (redundantní vyblokuje).
- Root bridge (kořenový přepínač) má nejnižší ID (hodnota v násobcích 4096), v případě shodné hodnoty se vybere přepínač na základě MAC adresy, opět nižší hodnota bude zvolena jako root bridge.
- BDPU (Bridge Protocol Data Units) – zprávy, které si vyměňují switche, aby vytvořili bezsmyčkovou topologii.
- STP využívá BDPU pro zasílání o změně topologie sítě nebo jiné informace o STP
- Cost of Path – cena cesty k root bridge.

Možné problémy

- Broadcast storms – při broadcastu se rámce ve smyčkách množí, až dojde k zahlcení sítě.
- Špatně naučené polohy účastníků – obdrží rámec ze správné strany a potom ještě smyčkou z druhé.
- Dvakrát doručené rámce – Switch nezná MAC adresu koncového PC, a proto rámec pošle jako broadcast a rámec může ke koncovému zařízení dorazit dvakrát.

Porty

- Root ports – porty, které jsou na přepínači nejblíže k root bridge
- Designated ports – porty, které zůstaly funkční, protože jejich cesta je výhodnější
- Non-designated ports – porty, které byly odstaveny, protože jejich cesta je delší

Stavy portů

Blocking

- Non-designated port, nepřeposílá rámce, poslouchá BPDU a je připraven změnit stav, pokud to bude potřeba.
- V tomto stavu je po zapnutí switche.

Listening

- STP umožňuje tento port využít pro přeposílání rámců.
- Poslouchá provoz, přijímá BPDU a zjišťuje, zda může nabídnout lepší cestu k root bridge.
- Pokud jeho cesta není výhodnější, vrátí se do stavu Blocking.

Learning

- Jako Listening, ale učí se MAC adresy rámců, které přes něj přejdou, protože určitě přejde do stavu Forwarding.

Forwarding

- Běžná funkce, učí se MAC adresy a posílá rámce.
- Poslouchá provoz, zpracovává BPDU a zjišťuje, jestli jeho cesta k root brige nebyla překonána nějakou lepší cestou, pokud ano, vrací se do stavu Blocking.

Disable

- Odstavený port, nedělá vůbec nic..

Etherchannell

- Technologie sloučení fyzických linek do jedné logické (lze spojit až 8 fyzických linek).
- Účelem je poskytnutí odolnosti proti chybám a vysokorychlostního propojení.
- Používán primárně v páteřní síti.

Protokoly

- PAgP (Port Aggregation Protocol) – Cisco, mody desirable/auto
- LACP (Link Aggregation Control Protocol) – obecné řešení, mody active/passive

Výhody

- Šířka pásma
- Hashovací algoritmus, který zajišťuje vyvážené zatížení linek
- Odolnost proti poruchám

VRRP

- Virtual Router Redundancy Protocol
- Sloučí více fyzických do jedné virtuální brány.
- Router s označením „Master“ slouží jako primární brána, ostatní jsou „Backup“ a budou využity v případě výpadku hlavního routeru.
- Lze využít i pro rozložení zátěže, kde část koncových zařízení má jako master Router1 a backup Router2 a jiná část koncových zařízení má Router2 jako master a Router1 jako backup.