6.

Přepínače, architektura sítí LAN, segmentace a mikrosegmentace sítí, kolizní a broadcast doména, redundance v síťovém provozu, STP, Etherchannell, VRRP (HSRP)

Pozn. Tato otázka je trošku obsáhlejší a může se neustále rozvádět, proto i tento dokument je obsáhlejší. Témata, která nejsou k této otázce nutná jsem označil jako navíc, ovšem zařadil jsem je sem, protože zkoušející se k nim může dostat. Na konci je ještě zkrácená verze.

Přepínač (switch)

Switch je aktivní prvek druhé vrstvy (linkové) ISO/OSI modelu, který přepíná rámce podle MAC adresy v jejich hlavičce. Přepíná je na správné odchozí porty dle své MAC adress tabulky. Mikrosegmentují sítě (to znamená, že síť dělí na co nejmenší kousky, aby nedocházelo ke kolizím)

MAC adresa (navíc)

MAC adresa je fyzická adresa daného síťového rozhraní. Je unikátní a má 48 bitů. Zapisuje se jako 12 hexadecimálních číslic. První polovina je identifikuje výrobce (Realtek, Asus, ...) (tzv. OUI), druhá polovina identifikuje síťové rozhraní.

ISO/OSI model (navíc)

Je teoretický model vypracovaný ISO v 80. letech. Snažil se vycházet z telefonních linek, takže přenos dat byl spojovaný a co nejvíce spolehlivý. Kvůli své robustnosti neuspěl a nahradil ho model rodiny protokolů TCP/IP. Má sedm vrstev – aplikační, prezentační, relační, transportní, síťová, linková (switch), fyzická (hub)

Přepínání

Switch má dva základní módy:

1. Ulož a pošli (store and forward)
   - Rámce se načtou a uloží. Switch zjistí jejich výstupní port (dle MAC address tabulky) a pošle.
   - Důležité: tento mód kontroluje kontrolní součet v patičce rámce, pokud se neshoduje s jeho provedeným součtem rámec zahodí a nepošle ICMP zprávu (jsme na linkové vrstvě, ICMP je na síťové)
   - Nižší výkon (kvůli větší režii)
   - Defaultní konfigurace, výkon natolik pokročil, že změnu přenosové rychlosti nepoznáme.

2. On the fly (cut through, průběžné zpracování)
   - průběžné přepínání na výstupní port aniž by skončil jeho příjem
   - přepnutí po zjištění cílové MAC a výstupního portu dle tabulky adres

- efektivní
- použití ve spolehlivých sítích

3. Režim nestandardního zpracování (tenhle jsme se neučili, zmínil bych se jenom, že existuje)

Vlastnosti

Přepínání

Každý port může mít jinou přenosovou rychlost (asymetrické přepínání, porty s větší rychlostí dám třeba serveru), nebo každý port má stejnou symetrickou rychlost (symetrické).

Vyrovnávací paměť (navíc)

1. Port-based Memory Buffering
   - Každý port má svojí paměť, kde se ukládají rámce.
   - Rámec je poslán na odchozí port pouze tehdy, když už byly rámce před ním vyslány.

2. Shared Memory Buffering
   - Jedna sdílená paměť.
   - Rámce se při posílání nemusí přesouvat mezi paměťmi.

MAC address table

- Je uložena na switchi.
- Nachází se v ní MAC adresa port adrese odpovídající, číslo VLAN a způsob získání záznamu.
- Příkaz: Switch#show mac-address-table

Získávání záznamů do MAC table

1. Staticky
   - Síťař přidává záznamy do tabulky manuálně.

2. Dynamicky
   - Switch učí z provozu. To znamená, že když přijde rámec s neznámou MAC adresou pošle ho na všechny porty kromě příchozího. Z odpovědi následně zjistí, kde se MAC adresa nachází. Pokud přijme rámec od MAC adresy, kterou nemá, zaznamená si port a tuto MAC adresu so své tabulky.

Problém, který řeší switch (navíc)

Historicky switch vylepšuje funkcionalitu hubu, který rámce vzal a poslal je na všechny porty, kromě příchozího portu (zařízení první vrstvy), což vedlo ke kolizím. Switch tento problém řeší tím, že síť mikrosegmentuje –> rámce se posílají po jedné určité cestě, která vede k cíli.

Architektura sítí

Využívá se hierarchický síťový model. Rozděluje logicky síť na oddělené vrstvy (přístupová, distribuční, páteřní)

1. Přístupová
   - Sdružuje data z přepínačů na přístupové vrstvě. Předává je páteřní vrstvě, kde jsou směrována do cílových sítí.
   - Propojuje vyšší vrstvy s koncovými zařízeními (PC, ...)

2. Distribuční
   - Sdružuje data z přepínačů na přístupové vrstvě. Předává je páteřní vrstvě, kde jsou směrována do cílových sítí.
   - Řídí síťový provoz, vymezuje broadcast domény.
   - Zajišťuje směrování mezi VLANy.

3. Páteřní
   - Představuje vysokorychlostní páteř pro přeposílání dat mezi sítěmi.
   - Zde budou ty nejrychlejší přepínače.

Výhody architektonického rozdělení (navíc)

- Scalability – můžeme je rozšiřovat
- Redudance – v páteřní a distribuční sítí je mnoho nadbytečných linek, kvůli spolehlivosti. O vyřazení smyček se stará STP.
- Performance – díky agregaci linek máme vysokou výkonnost. O to aby linky vypadaly jako jedna se stará etherchannel.
- Maintainability – udržovatelnost, modulární a hierarchická struktura umožňuje snadnou.
- Rozšiřitelnost sítě

Segmentace mikrosegmentace

Segmentace

Myšleno rozdělování sítě na menší části. Síť můžeme segmentovat pomocí VLAN. Tedy virtuální lany, které dělí koncová zařízení podle určité logické příslušnosti. Například chceme mít oddělené učitelský a studentský provoz.

Zkraceně VLAN

Virtuální LAN; pomocí VLAN můžeme síť dělit podle použití, cílových skupin atd.; typy vlan: Data (datová), Default (standardně nastavená), Native (přirozená), Management (řídící), Voice (hlasové služby); portu na přepínači může být přiřazena pouze jedna VLANA -> pro spoje mezi přepínačí se používá mód trunk; broadcast se šíří pouze v rámci VLAN.

Mikrosegmentace

Znamená to, že síť dělím na co nejmenší (atomické) části. Každé koncové zařízení má svoji linku do přepínače. Linka je full-duplex, a tedy mezi koncovým zařízením a přepínačem je bezkolizní mikrosegment.

Kolizní doména

Je to ta část sítě, kde může vznikat kolize. Ethernet má nedeterministickou přístupovou metodu (CSMA/CD), a tudíž nelze předcházet kolizím, když vysílají dvě stanice najednou. Je to zejména

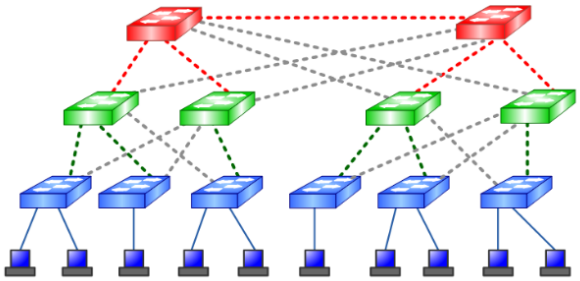
historicky problém, jelikož nyní kolizní doménu změnšuje switch, kdy mikrosegmentuje síť (viz výše)

Broadcast doména

Je segment sítě kde se šíří broadcast vysílání (broadcast -> všesměrové, multicast –> skupina příjemců, unicast –> cílová jedna stanice). Typické broadcast vysílání má poslední platnou adresu sítě a MAC FF:FF:FF:FF:FF:FF. Broadcast doménu zastaví router, vysílání nepřesměruje, naopak switch broadcast doménu zvětšuje.

Redundance

Znamená nadbytečnost. V kontextu přepínačů to znamená, že do určitého cíle se dá dostat více způsoby. Vytváříme smyčky mezi přepínači nadbytečnými linkami, abychom zajistili spolehlivost, kdyby některá z nich přestala fungovat.



STP (spanning tree protocol, protokol přemosťovacího stromu)

Redundance vytváří smyčky. Rámce nemají TTL (time to live), takže teoreticky mohou v smyčce běhat do nekonečna. Tento problém řečí STP, který vytváří bezsmyčkovou logickou topologii.

Problémy sítí se smyčkami

- Rámce se budou donekonečna ve smyčkách množit.
- Špatné doplňování MAC adres table – rámce přichází z různých segmentů.
- Rámce přijdou cíli dvakrát.

Algoritmus STP

Přepínače si zvolí Root Bridge (podle BID -> switch má z výroby, pokud mají dva přepínače stejný BID, volí se bridge s nižší MAC adresou), od RB se rozbíhají všechny cesty.

STP uvede porty na přepínačích do stavu:

- Root Ports – porty nejblíže RB
- Designated Ports – porty na RB; funkční porty, protože jejich cest k RB je kratší
- Non-designated Ports – odstavené porty

Pro předávání informací k vytvoření bezsmyčkové topologie se používají BPDU rámce.

Postup vytvoření bezsmyčkové topologie

Root Bridge se volí podle BID, přepínače si BID vyměňují pomocí BPDU na začátku. RB nastaví své porty na designated. Pak se vybírají root porty, ty jsou vybrány na základě ceny cesty k RB. Následuje nastavení designated a non-designated portů na odstavených linkách. Switch s nižším Bridge ID nastaví porty na designated.

Stavy portů (navíc)

- Blocking – non-designated port
- Listening – poslouchá provoz a zda se nebude moci stát root bridgem.
- Learning – nepřeposílá rámce, pouze se učí provoz
- Forwarding – zcela funkční port
- Disabled – administrativně odstavený

Etherchannel

- Technika, kdy z vice fyzických spojů mezi přepínači vytváříme jeden logický spoj.
- Oba konce EtherChannel musí být konfigurovány do stejného módu (např. LACP).
- Používá load balancing k balancování zátěže na linkách.
- Provoz je rozložen rovnoměrně podle zdrojových nebo cílových MAC nebo IP (dle
- nastavení).
- Funkce etherchannel se využívá, pokud chceme zvětšit přenosovu kapacitu mezi
- přepínači, popř. mezi přepínačem a koncovým zařízením.

VRRP (Virtual Router Redundancy protocol)

- Technika, kdy lze přenést virtuální IP adresu gateway na jiný záložní router.
- Brána má jednu IP adresu a nastaví ne rothraních směrovaču.
- VRRP zvolí master router (podle priority 0 – 255 -> při stejné hodnotě se volí podle IP
- adresy), ostatní jsou zálohy. Při výpadku routeru se IP adresa převede na zálohu.
- Cisco alternativa je HSRP, který používá místo pojmů master a backup pojmy active
- a standby.
- Parametr „preempt“ umožňuje po zresetování návrat k původnímu fyzickému master
- routeru

Zkrácená verze

Přepínač (Switch)

- Aktivní prvek 2. vrstvy ISO/OSI (linková vrstva).
- Přepíná rámce podle MAC adresy.
- Mikrosegmentace – rozdělení sítě pro minimalizaci kolizí.
- **Režimy přepínání:**

    - Store and Forward – ukládá celé rámce a kontroluje chybové rámce.
    - Cut Through – okamžité přepnutí rámců bez kontroly chyb.

Architektura sítí

- Hierarchický model s vrstvami:
    - **Přístupová vrstva** – propojuje koncová zařízení s vrstvami nahoře.
    - **Distribuční vrstva** – agregace provozu, směrování mezi VLANy, přepínání mezí přístupovou a páteřní.
    - **Páteřní vrstva** – vysokorychlostní propojení mezi sítěmi
- **Výhody hierarchické architektury:**
    - Škálovatelnost
    - Redundance
    - Výkonnost
    - Udržovatelnost

Segmentace a Mikrosegmentace

- **Segmentace:** Rozdělení sítě na VLAN, oddělení provozu.
- **Mikrosegmentace:** Bezkolizní propojení každého zařízení s přepínačem, full-duplexní provoz.

Kolizní a Broadcast doména

- **Kolizní doména:** Část sítě, kde může dojít ke kolizím; switch kolizní domény omezuje
- **Broadcast doména:** Oblast, kde se šíří broadcastové zprávy; omezována routery

Redundance a STP (Spanning Tree Protocol)

- **Redundance:** Více fyzických cest pro zajištění spolehlivosti
- **STP:**
    - Volba hlavního přepínače (Root Bridge).
    - Zamezení smyček v síti.
    - **Stavy portů:**
        - Root Port
        - Designated Port
        - Non-Designated Port

EtherChannel

- Spojení několika fyzických spojů do jednoho logického kanálu.
- Zvýšení propustnosti, load balancing.

- LACP pro konfiguraci.

VRRP (Virtual Router Redundancy Protocol)

- Zajištění dostupnosti brány na více směrovačích.
- Volba hlavního routeru (master), záložní routery (backup).
- Preempt pro návrat hlavního routeru po obnovení.