**17. Protokol STP a EtherChannel**

**1. Redundantní síť a možné problémy**

**1.1 Redundance a smyčky v přepínaných sítích**

V **ethernetových LAN sítích** se redundantní topologie používá zejména proto, aby se eliminoval **jediný bod selhání** (Single Point of Failure) a zajistila se **vysoká dostupnost**. Redundance tedy znamená mít více vzájemně propojených přepínačů (switchů) a více cest (fyzických linek) mezi nimi, než je nezbytně nutné pro samotné propojení.

Nicméně přidání většího počtu spojů mezi přepínači může způsobit **vznik smyček** na 2. vrstvě (spojové vrstvě). Tyto smyčky (loop) vedou k nechtěným jevům:

1. **Broadcast storm** (bouře broadcastů)
   * Pokud v síti existuje smyčka, broadcastové rámce se mohou neustále šířit dokola a **exponenciálně** navyšovat provoz.
2. **Duální zpracování rámců (duplication)**
   * Rámce se mohou doručovat vícekrát, protože switch může rámec přijmout na více portech.
3. **Nestabilita MAC tabulek**
   * Přepínače mohou být zmateny, protože dostávají stejné MAC adresy na různých portech, a neustále přepisují záznamy v CAM/FDB tabulce.

Tyto problémy mohou způsobit **kolaps sítě** (trafika naroste do té míry, že se síť stane nepoužitelnou).

**1.2 Řešení: Spanning Tree Protocol**

Aby se zabránilo vzniku smyček v přepínaných sítích, byl vyvinut **Spanning Tree Protocol (STP)**. Ten logicky **deaktivuje** (blokuje) některé redundantní spoje, čímž vytváří **bezesmyčkovou stromovou topologii** (spanning tree). Po selhání některé aktivní cesty se blokované linky mohou **automaticky aktivovat**.

**2. Koncepce a použití STP**

**2.1 Základní princip STP**

* STP pracuje na **2. (spojové) vrstvě modelu OSI**.
* Všechny přepínače si mezi sebou vyměňují **BPDU** (Bridge Protocol Data Units) – rámce s informacemi o prioritách, MAC adresách, cestovních nákladech atd.
* Na základě výměny BPDU se v síti zvolí:
  1. **Kořenový přepínač (Root Bridge)** – ten s nejnižší prioritou (a případně nejnižší MAC adresou).
  2. Pro každý segment (vztah mezi dvěma switche nebo switchem a rozhraním) se zvolí **Root port** (port na switchi, kterým vede nejkratší cesta k Root Bridge).
  3. **Designated port** na druhé straně segmentu (port, který funguje jako „vítězný“ pro přeposílání rámců z daného segmentu do stromu).
  4. Ostatní porty, které nejsou ani root port, ani designated port, přejdou do blokujícího stavu (**alternate** **porty**), aby nevznikla smyčka.

Výsledkem je **spanning tree** – tedy síťová topologie bez smyček.

**STA — Spanning-tree Algorithm**

* Označí vždy jeden switch jako tzv. root bridge
  + Tento switch se použije jako referenční bod pro výpočty cest rámců v síti
* Switche v síti komunikují pomocí BPDU rámců

<aside> 💡 Jsou zasílány každé 2 sekundy

* + Pomocí těchto rámců se zjistí, kdo má v síti nejmenší Bridge ID - BID

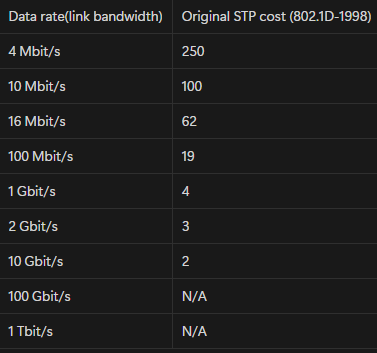
**Bridge ID**

* Unikátní identifikátor switche, Je tvořený z…
  + Priority — Skáče po 4096, od 0 → 65535
    - Defaultně 32768
  + MAC adresy switche
  + Extended system ID (v sítích s více VLAN)

**Určení Root Bridge**

* Všechny switche posílají BPDU rámce sousedům v broadcastové doméně
* Každý switch kontroluje u přijatých BPDU rámců, zda jeho vlastní Bridge ID je vyšší než v přijatém rámci
  + Jestli přijaté BID je nižší — Nastaví si switch jako root ID hodnotu BID z přijatého rámce → ví, kdo je Root Bridge a tuto informaci propaguje v BPDU sousedním switchům
* Pro každou VLAN je vlastní root bridge - **Záleží na implementovaném standardu a verzi STP**

**Určení ceny cesty**

* Po určení Root Bridge, se spočítají nejlepší cestu k Root Bridge — Cena cesty je určena vzdáleností a rychlostí linek mezi switchemi — ze všech míst v broadcastové doméně
  + Výchozí cena cesty je rychlost portu — dá se to změnit
* Během výpočtu je normální komunikace zakázána — aby nedošlo k smyčkám
* Sčítají se ceny cest přes všechny porty všech switchů
  + Cena cesty v BPDU rámci se při každém průchodu portu navyšuje, a tak se na konci zjistí celková cena

**Role portů detailněji**

**Root port**

* Nejblíže k root bridge
* Jsou určeny na každém switchy
* Umožňuje běžnou komunikaci

Zda se port stane root portem závisí na:

1. Nejnižší BID souseda
2. S nižší port priority souseda

<aside> 💡 Port priority = 128 (default) a přidává se k tomu číslo portu, např. 128.2

1. S nižším číslem portu souseda

**Designated port**

* Ostatní povolené trunky porty
* Je vždy na druhé straně root portu
  + Root port ↔ Designated port
* Umožňuje běžnou komunikaci

Specifické vlastnosti

* Všechny porty na switchy jsou designated porty (pokud nejsou root port či alternate port)
* Switch si zaznamená pro tento typ portu tzv. **internal root path cost**
  + Při propojení dvou switchů, kdy žádný z nich není root bridge, zvolí se jako designated port ta strana trunku, která má nižší internal root path cost → má krátší cestu k root bridge
    - Pokud je internal root path cost stejná, použijí se další podmínky jako:
      * Nejnižší BID souseda
      * Nižší port priority souseda
      * Nižší číslo portu souseda
  + Je rovna sumě všech cen po cestě k root bridge

**Alternate port**

* Neumožňují běžnou komunikaci (zabraňuje smyčkám)
* Propouští BPDU rámce
* Do tohoto stavu se port dostane pokud:
  + **Není designated port / root port**
  + **A naproti sobě má designated port**

**Disabled port**

**2.2 Fáze protokolu STP**

Původní STP (IEEE 802.1D) definuje pro porty několik stavů:

1. **Blocking** – port přijímá jen BPDU, nepropouští data. (stav pro Alternate porty)
2. **Listening** – switch poslouchá a posílá BPDU a připravuje se na změnu stavu, ale ještě neposílá data. (Zjišťuje cenu k Root Bridge)
3. **Learning** – switch si začíná vytvářet MAC tabulku, ale ještě nepropouští uživatelská data.
4. **Forwarding** – port už plně propouští uživatelský provoz.
5. **Disabled** – port je administrativně vypnut.

Celý proces konvergence (při změně topologie) může v původním 802.1D trvat až desítky sekund (běžně 30–50 s).

**2.3 Druhy STP protokolů**

V průběhu času vzniklo několik variant STP, aby se řešily různé potřeby, především **rychlejší konvergence** a **podpora VLAN**:

1. **STP (IEEE 802.1D)**
   * Původní verze s pomalejší konvergencí.
2. **RSTP (Rapid STP, IEEE 802.1w)**
   * Vylepšená a rychlejší konvergence (řádově v sekundách).
   * Zjednodušuje stavy portů: Learning, Forwarding, Discarding.
   * Pomocí tzv. edge portů a handshake mechanizmů dosahuje rychlejší stabilizace.
3. **PVST+ (Per-VLAN Spanning Tree Plus)**
   * Cisco proprietární řešení. Umožňuje **samostatný spanning-tree** pro každou VLAN.
   * Využívá STP 802.1D ve spojení s Cisco mechanismy. (cisco proprietary)
   * Rozšiřuje možnosti load-balancingu, protože root bridge může být odlišný v každé VLAN.
4. **Rapid PVST+**
   * Kombinace RSTP a per-VLAN topologie (Cisco proprietární).
   * Rychlá konvergence pro každou VLAN zvlášť.
5. **MST / MSTP (Multiple Spanning Tree, IEEE 802.1s)**
   * Pro velké sítě s mnoha VLAN. VLANy se mohou **seskupit** do tzv. instance MST, každá instance MST má svůj spanning tree.
   * Šetří zdroje (nemusí se vytvářet STP pro každou VLAN zvlášť jako u PVST+).

V praxi se často používá **RSTP (802.1w)** nebo **Rapid PVST+** (v Cisco prostředí) pro rychlou konvergenci.

**3. EtherChannel – popis a využití**

**3.1 Co je EtherChannel**

**EtherChannel** (někdy označovaný jako Port-Channel) je technologie, která umožňuje **spojit (agregovat) více fyzických linek** (typicky 2 až 8 ethernet portů) **do jednoho logického svazku**. Z pohledu vyšších vrstev (včetně STP) se pak tato skupina fyzických spojů jeví jako **jediný logický link**.

* Zvyšuje šířku pásma, zlepšuje redundanci
  + Pokud vypadne jeden kabel – neva, stále běží! Není to skvělé, Horste?
* Poskytuje rovnoměrné rozdělení zátěže
* Všechny fyzické připojení musí mít **stejnou rychlost** a **duplexitu spoje**
  + Nezle mýchat FastEthernet a GigabitEthernet
    - Pokud bychom snížili GigabitEthernet rychlost na FastEthernet, tak ano

**Hlavní přínosy EtherChannel**

1. **Zvýšení propustnosti**
   * Např. pokud sloučíme 4 linky o rychlosti 1 Gb/s, můžeme teoreticky dosáhnout agregované kapacity 4 Gb/s.
2. **Redundance**
   * Pokud jeden fyzický kabel (v rámci EtherChannelu) selže, provoz se přesměruje na zbývající funkční linky. Z logického hlediska zůstává Port-Channel aktivní.
3. **STP transparentnost**
   * STP vidí EtherChannel jako **jednu linku**, takže se **neblokuje** každá fyzická linka zvlášť. Tím lze efektivně využít kapacitu bez rizika smyček.

**3.2 Provoz a nastavení EtherChannel**

EtherChannel lze konfigurovat **staticky** anebo pomocí **dynamických protokolů**:

* **PAgP (Port Aggregation Protocol)** – Cisco proprietární.
* **LACP (Link Aggregation Control Protocol, IEEE 802.3ad)** – standardní protokol, široce podporovaný.

Pro EtherChannel je důležité:

* Všechny porty ve svazku musí pracovat **stejně** (stejná rychlost, duplex, VLAN nastavení apod.).
* Nastavení stran (mode) protokolů musí souhlasit (např. LACP active/passive, PAgP desirable/auto).
* EtherChannel se obvykle konfiguruje příkazem channel-group <x> mode <mode> (v Cisco IOS).

**3.3 Load Balancing v EtherChannelu**

K rozdělování zátěže (load balancing) mezi fyzické linky se používají různé metody založené na:

* Zdrojové a/nebo cílové **MAC adrese**.
* Zdrojové a/nebo cílové **IP adrese**.
* V některých případech i TCP/UDP porty.

Cílem je rozložit provoz tak, aby jednotlivé fyzické spoje byly zatěžovány co nejrovnoměrněji. Zároveň je zajištěno, že rámce daného toku (stejné adresy) putují stejnou linkou, čímž se vyhýbá problémům se sekvenčním doručením.

**LACP**

Stavy:

1. on — Spojí svazek připojení a vyměňuje LACP pakety s druhou stranou spoje
2. active — Aktivně se snaží vytvořit propojení s druhou stranou (na druhé straně musí být active či passive)
3. passive — Pokud je druhá strana aktive, vytvoří LACP propojení

**PAgP**

Stavy:

1. on — Spojí svatek připojení a vyměňuje PAgP pakety s druhou stranou spoje
2. off — Opak on
3. Auto — Snaží se vytvořit propojení s druhou stranou (na druhé straně musí být auto či desirable)
4. Desirable — Pokud je druhá strana auto, vytvoří PAgP připojení

**Shrnutí**

1. **Redundantní síť** přináší výhodu lepší dostupnosti, ale zároveň hrozí vytvoření **smyček** na 2. vrstvě. To způsobuje jevy jako broadcast storms a nestabilitu MAC tabulek.
2. **STP (Spanning Tree Protocol)** je mechanismus, který automaticky **blokuje redundantní cesty** a udržuje bezesmyčkovou stromovou topologii. Při výpadku linky dokáže síť **rekonfigurovat** a zablokovanou cestu aktivovat.
3. Existuje více **druhů STP** – původní 802.1D, rychlejší RSTP 802.1w, Cisco PVST+ a Rapid PVST+, případně MST (802.1s). Hlavním cílem novějších verzí je **rychlejší konvergence** a podpora VLAN.
4. **EtherChannel** umožňuje **agregaci** více fyzických spojů do jednoho logického kanálu. Poskytuje **vyšší propustnost**, **redundanci** a zjednodušené chování pro STP, které tak vidí jen jediný logický link. Pro dynamické vyjednávání EtherChannelu se používají protokoly **PAgP** (Cisco) nebo **LACP** (IEEE 802.3ad).