

# STP (Spanning Tree Protocol)

**STP** je síťový protokol na 2. vrstvě OSI modelu (Data Link Layer). Jeho hlavním úkolem je zajistit topologii sítě bez smyček (loop-free) v prostředí s redundantními cestami mezi switchi. V naší **digitální architektuře** je STP nezbytnou pojistkou proti zahlcení sítě tzv. všesměrovými bouřemi (broadcast storms).

Standardně je STP definován normou IEEE 802.1D, v naší síti však preferujeme modernější a rychlejší varianty jako RSTP (Rapid STP) nebo MSTP (Multiple STP).

## Proč STP potřebujeme?

V rámci zajištění vysoké dostupnosti v našem **VPC** propojujeme switche redundantně. Pokud by nebyl aktivní STP, došlo by k:

- **Broadcast Storms:** Pakety by nekonečně kroužily v síti a během sekund by vyčerpaly veškerou šířku pásma.
- **Instabilitě MAC tabulek:** Switche by neustále měnily záznamy o tom, na kterém portu se nachází konkrétní zařízení, což by znemožnilo doručování dat.

## Jak STP funguje? (Logika algoritmu)

Proces výběru cest probíhá v několika krocích:

1. **\*\*Výběr Root Bridge:\*\*** Všechny switche si vymění zprávy (BPDU). Switch s nejnižším ID se stane "kořenem" sítě.
2. **\*\*Výpočet nejkratších cest:\*\*** Ostatní switche určí porty s nejnižší "cenou" (cost) směrem k Root Bridge.
3. **\*\*Blokování portů:\*\*** Nadbytečné cesty, které by vytvořily smyčku, jsou logicky zablokovány (stav Blocking).

## Využití a správa v naší síti

### 1. Redundance v datových centrech

Naše **IT Podpora** konfiguruje STP na všech switchích, které obsluhují **VPS** hostitele. Pokud dojde k fyzickému přerušení kabelu v naší síti **WAN**, STP automaticky během zlomku sekundy (u RSTP) aktivuje dříve zablokovanou záložní cestu.

### 2. Ochrana před chybným zapojením

STP chrání síť v případech, kdy uživatel v kanceláři neúmyslně propojí dvě zásuvky kabelem „do

smyčky“. Funkce **BPDU Guard** na koncových portech v takovém případě port okamžitě vypne, aby ochránila zbytek **ZIF**.

## Srovnání variant STP

Protokol	Norma	Rychlost konvergence	Využití v naší síti
<b>STP</b>	802.1D	Pomalá (30-50 s)	Již nepoužíváme (legacy)
<b>RSTP</b>	802.1w	Velmi rychlá (< 2 s)	Standard pro běžné pobočky
<b>MSTP</b>	802.1s	Velmi rychlá	Komplexní síť s mnoha VLANy

## Bezpečnostní rizika

V rámci **kybernetické bezpečnosti** musíme STP chránit:

- **STP Spoofing:** Útočník může do sítě poslat BPDU s nízkou prioritou a stát se Root Bridgem, čímž by mohl odposlouchávat veškerý provoz.
- **Opatření:** Naše brány **UTM** a switche mají aktivní funkci **Root Guard**, která zabraňuje neautorizovaným zařízením převzít roli kořenového prvku.

**Upozornění pro techniky:** Při provádění změn v topologii sítě v systému **Jira** vždy počítejte s krátkým výpadkem konektivity během přepočtu STP stromu. U kritických systémů doporučujeme provádět změny mimo pracovní dobu.

— **Související stránky:** [ZIF](#), [VPC](#), [WAN](#), [IT Podpora](#), [VPS](#), [Kybernetická bezpečnost](#), [UTM](#), [Jira](#)

From:  
<https://serviceit.cz/> - **IT ENCYKLOPEDIE**

Permanent link:  
<https://serviceit.cz/doku.php?id=stp>

Last update: **2026/01/01 17:14**

